Ius Comparatum – Global Studies in Comparative Law

Dário Moura Vicente
Sofia de Vasconcelos Casimiro *Editors*

Data Protection in the Internet

Springer

hoeren@uni-muenster.de

Ius Comparatum – Global Studies in Comparative Law

Volume 38

Series Editors
Katharina Boele-Woelki, Bucerius Law School, Hamburg, Germany
Diego P. Fernández Arroyo, Institut d'Études Politiques de Paris (Sciences Po), Paris, France

Founding Editors
Jürgen Basedow, Max Planck Institute for Comparative and International Private Law, Hamburg, Germany
George A. Bermann, Columbia University, New York, USA

Editorial Board Members
Joost Blom, University of British Columbia, Vancouver, Canada
Vivian Curran, University of Pittsburgh, USA
Giuseppe Franco Ferrari, Università Bocconi, Milan, Italy
Makane Moïse Mbengue, Université de Genève, Switzerland
Marilda Rosado de Sá Ribeiro, Universidade do Estado do Rio de Janeiro, Brazil
Ulrich Sieber, Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
Dan Wei, University of Macau, China

hoeren@uni-muenster.de

As globalization proceeds, the significance of the comparative approach in legal scholarship increases. The IACL / AIDC with almost 800 members is the major universal organization promoting comparative research in law and organizing congresses with hundreds of participants in all parts of the world. The results of those congresses should be disseminated and be available for legal scholars in a single book series which would make both the Academy and its contribution to comparative law more visible. The series aims to publish the scholarship emerging from the congresses of IACL / AIDC, including: 1. of the General Congresses of Comparative Law, which take place every 4 years (Brisbane 2002; Utrecht 2006, Washington 2010, Vienna 2014, Fukuoka 2018 etc.) and which generate (a) one volume of General Reports edited by the local organizers of the Congress; (b) up to 30 volumes of selected thematic reports dealing with the topics of the single sections of the congress and containing the General Report as well as the National Reports of that section; these volumes would be edited by the General Reporters of the respective sections; 2. the volumes containing selected contributions to the smaller (2-3 days) thematic congresses which take place between the International Congresses (Mexico 2008; Taipei 2012; Montevideo 2016 etc.); these congresses have a general theme such as "Codification" or "The Enforcement of Law" and will be edited by the local organizers of the respective Congress. All publications may contain contributions in English and French, the official languages of the Academy.

More information about this series at http://www.springer.com/series/11943

Académie internationale de droit comparé
International Academy of Comparative Law

hoeren@uni-muenster.de

Dário Moura Vicente •
Sofia de Vasconcelos Casimiro
Editors

Data Protection in the Internet

Springer

hoeren@uni-muenster.de

Editors
Dário Moura Vicente
Law School
University of Lisbon
Lisbon, Portugal

Sofia de Vasconcelos Casimiro
Law School
University of Lisbon
Lisbon, Portugal

ISSN 2214-6881 ISSN 2214-689X (electronic)
Ius Comparatum – Global Studies in Comparative Law
ISBN 978-3-030-28048-2 ISBN 978-3-030-28049-9 (eBook)
https://doi.org/10.1007/978-3-030-28049-9

© Springer Nature Switzerland AG 2020
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

hoeren@uni-muenster.de

Contents

hoeren@uni-muenster.de

hoeren@uni-muenster.de

Contributors

Lukman Adebisi Abdulrauf Department of Public Law, South African Research Chair in International Constitutional Law, University of Pretoria, Pretoria, South Africa

Shawn Marie Boyne Indiana University, Robert H. McKinney School of Law, Indianapolis, IN, USA

Christina Breunig University of Bayreuth, Centre for Consumer Law, Bayreuth, Germany

Felisa-María Corvo López University of Salamanca, Salamanca, Spain

José Augusto Fontoura Costa University of São Paulo, Law Faculty, São Paulo, Brazil

Dragos Nicolae Costescu University of Bucharest, Bucharest, Romania

Pedro A. de Miguel Asensio Complutense University of Madrid, Madrid, Spain

Sofia de Vasconcelos Casimiro University of Lisbon and Portuguese Military Academy, Lisboa, Portugal

Thomas Hoeren University of Münster, Münster, Germany

František Kasl Masaryk University, Faculty of Law, Institute of Law and Technology, Brno, Czech Republic

Taro Komukai Nihon University, College of Risk Management, Tokyo, Japan

Vassilios Kourtis Aristotle University of Thessaloniki, Salonika, Greece

Elena Lazar University of Bucharest, Bucharest, Romania

Jakub Míšek Masaryk University, Faculty of Law, Institute of Law and Technology, Brno, Czech Republic

Dário Moura Vicente University of Lisbon, Lisboa, Portugal

hoeren@uni-muenster.de

Laurence Nicolas-Vullierme Centre de Droit Européen, Université Panthéon-Assas (Paris 2), Paris, France

Ee-Ing Ong Singapore Management University School of Law, Singapore, Singapore

José Pina-Delgado Instituto Superior de Ciências Jurídicas & Sociais of Praia, Praia, Cape Verde
Constitutional Court of the Republic of Cabe Verde, Praia, Cape Verde

Alexandre Sousa Pinheiro University of Lisbon, Lisboa, Portugal

Radim Polčák Masaryk University, Faculty of Law, Institute of Law and Technology, Brno, Czech Republic

Teresa Scassa University of Ottawa, Faculty of Law, Ottawa, ON, Canada

Martin Schmidt-Kessel University of Bayreuth, Bayreuth, Germany

Anderson Schreiber Rio de Janeiro State University, Rio de Janeiro, Brazil

Dominic N. Staiger University of Zurich, Zurich, Switzerland

Vincenzo Zeno-Zencovich Università degli Studi Roma Tre, Rome, Italy

hoeren@uni-muenster.de

Data Protection in the Internet: General Report

Dário Moura Vicente and Sofia de Vasconcelos Casimiro

1 Introduction

1.1 Subject-Matter, Purpose and Scope of the Present Report

In recent years, data protection, i.e., the legal regulation of the collection, storage, transmission and use of information concerning identified or identifiable individuals, has become a major concern in most countries, as well as at the supranational and international levels.

In fact, the emergence of computing technologies that allow, at ever lower costs, the processing of increasing amounts of information, associated with the advent and exponential use of the Internet and other communication networks and the widespread liberalization of the trans-border flow of information, have allowed the large-scale collection and treatment of individual data, not only for scientific or commercial, but also for political uses.

A growing number of governmental and private organizations now possess and currently use data processing in order to determine, predict and influence individual behavior in all fields of human activity.

This inevitably entails new risks, not only from the perspective of individual privacy, but also from those of other fundamental rights, such as the right not to be discriminated, as well as of the fair competition between commercial enterprises and of the proper functioning of democratic institutions.

D. Moura Vicente (✉)
University of Lisbon, Lisboa, Portugal
e-mail: dmouravicente@fd.ul.pt

S. de Vasconcelos Casimiro (✉)
University of Lisbon, Lisboa, Portugal

Portuguese Military Academy, Lisboa, Portugal
e-mail: svc@fd.ulisboa.pt

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_1

hoeren@uni-muenster.de

The abovementioned phenomena have not remained ignored from a legal point of view: both at the national, supranational and international levels, an increasing number of regulatory instruments—among which the European Union's General Data Protection Regulation applicable as of 25 May 2018[1]—have been adopted with the purpose of preventing and sanctioning personal data misuse.

Nevertheless, distinct national approaches still prevail in this domain, notably those that separate the highly comprehensive, detailed and protective rules adopted in Europe since the 1995 Directive on the protection of individuals with regard to the processing of personal data was enacted[2] from the more fragmented and liberal attitude of American courts and legislators in this respect.

In a globalized world, in which personal data can instantly circulate and be used simultaneously in communications networks that are ubiquitous by nature, these different national and regional approaches are a major source of conflicts of laws. These, in turn, are also the object of divergent solutions, ranging from the application of data protection rules on a purely territorial basis to extra-territorial choice of law regimes, according to which data protection laws may also apply to the processing of personal data undertaken by entities established outside the jurisdiction of the data subject's place of habitual residence.

Ultimately, those different approaches may lead to judicial or administrative decisions preventing the transfer of personal data to third countries that do not provide a degree of protection deemed equivalent to that of the *forum* State, as has recently occurred in the European Union.[3] The main purpose of this report is to identify and explain these different national approaches and to determine the extent to which they may be overcome or harmonized in the near future.

A number of national and special reports, drafted in response to a questionnaire prepared by the authors of this general report, have been instrumental for this purpose. Those reports provide a wealth of information regarding the legal systems of fifteen jurisdictions from four continents, as well as those of the European Union, the United Nations and of International Trade Law.[4]

[1] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, 4.5.2016, pp. 1 ff.

[2] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31 ff.

[3] See the judgment of the CJEU of 6 October 2015, C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650.

[4] The abovementioned reports will be cited hereafter in an abbreviated manner, according to their denominations in the appended list.

hoeren@uni-muenster.de

1.2 Organization of the Report

This report is divided into five sections.

After the introduction provided in Sect. 1, Sect. 2 will give an overview of the general data protection framework in the legal systems covered by the report. For this purpose, that section will examine the applicable rules in the relevant jurisdictions, the notion of personal data prevailing in those rules, the existing supervision authorities and the extent to which the subject matter of the report is also governed by self-regulation instruments.

Section 3 will analyze, from a comparative perspective, a number of critical issues concerning data protection in the Internet, in particular those related to data processed by electronic means, data protection in the electronic communications sector, data protection and digital forensics, data protection and electronic surveillance for security and defense purposes and the remedies and sanctions available for the breach of the applicable rules.

Section 4 will address the international dimension of data protection. Notably, it will seek to determine the extent to which national or supranational rules on data protection are applied on a territorial or an extraterritorial basis, the specific conditions applicable to the transfer of personal data to foreign jurisdictions and the law applicable to liability for damages caused by the unlawful processing of personal data.

Finally, Sect. 5 will identify the basic approaches to regulation of data protection in the Internet that flow from the preceding sections and will endeavor to make a general assessment thereof.

2 The General Data Protection Framework

2.1 The Applicable Rules

The first issue raised by a comparative study on the subject-matter of this report is the extent to which personal data protection is covered by specific legislation or case law and the nature and scope of that legislation or case law.

The protection of privacy has been a relevant concern in Western legal systems for more than a century[5] and has found expression as a personality right in several European codifications,[6] as well as a human right in international covenants.[7] The adoption of specific rules governing the collection, storage, transmission and use of

[5] See the seminal article by Warren and Brandeis (1890). For an overview of the law of privacy in Western legal systems, see Strömholm (1967).

[6] See, for example, article 80 of the Portuguese Civil Code. On the genealogy of this provision, see Mota Pinto (2018), pp. 475 ff.; and Menezes Cordeiro (2011), pp 259 ff.

[7] See, *e.g.,* article 12 of the Universal Declaration of Human Rights.

hoeren@uni-muenster.de

personal data is, however, a much more recent phenomenon, which is closely linked to the technological developments (occurred mostly in the 1980s and 1990s) that have made those operations possible on a large scale, namely the digitization of information, the integration of the processing functions of computers onto low-cost microprocessors and the advent of the Internet as a global network of computer networks.[8]

Since then, data protection statutes have experienced a dramatic increase in number and scope, and have been extended to most countries. After the adoption of Directive 95/46/EC, virtually all European Union Member States have enacted legislation on this topic seeking to transpose that Directive or to adapt pre-existing statutes to it.[9] That legislation has, in turn, had a considerable influence over the law of other regions of the world.[10]

The European tendency to enact comprehensive laws on data protection has been further enhanced by the adoption in 2016 of the General Regulation on Data Protection (hereafter GDPR), which has replaced the 1995 Directive and is directly applicable in all EU Member States. It contains a detailed regime, which aims at codifying the law in this field. Notwithstanding some relevant exclusions, the Regulation covers all fundamental topics of data protection, notably: (1) the general principles governing this matter; (2) the rights of the data subject; (3) the status of the data controller and processor; (4) the transfer of personal data to third countries; (5) the supervision authorities and their reciprocal cooperation; and (6) the applicable remedies, liabilities and penalties.[11]

It is important to note, however, that the adoption of the GDPR has not excluded the relevance of the significant body of case law emanating from the Court of Justice of the European Union (hereafter CJEU) on the interpretation of the 1995 Directive, nor the Guidelines adopted by the so-called *Article 29 Data Protection Working Party* set up under that Directive (which will become the European Data Protection Board under articles 68 *et seq.* of the GDPR).[12]

The GDPR will be complemented by other European legal acts concerning the protection of personal data, among which a Regulation concerning privacy in the electronic communications sector.[13]

[8]See, for recent overviews of this matter, de Miguel Asensio (2015), pp 291 ff.; Hoeren (2018), pp 445 ff.

[9]See, as examples thereof, the statutes cited in the German National Report, Sect. 1.1; the French National Report, Sect. 1; the Greek National Report, Sect. 1.1; the Italian National Report, Sect. 1; the Portuguese National Report, Sect. 1; the Romanian National Report, Sect. 2.1; and the Spanish National Report, Sect. 1.1.

[10]As was the case, *e.g.,* of Cape Verde: see Cape Verdean National Report, Sects. 2 and 5.2.

[11]See, for a comprehensive description of this Regulation, the European Union Special Report.

[12]See *ibidem*, Sect. 1.1.

[13]See the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM (2017) 10 final.

hoeren@uni-muenster.de

In several European countries, personal data protection, or *informational self-determination*, is a fundamental right, either derived from the Constitution's general rules, such as article 2(1) of the German Basic Law, which enshrines a "right to the free development of one's personality",[14] and article 2 of the Italian Constitution, which establishes that "the Republic recognizes and guarantees the inviolable rights of the person, both as an individual and in the social groups where human personality is expressed"[15]; or contained in specific provisions, such as article 35 of the Portuguese Constitution,[16] and article 9A of the Greek Constitution.[17]

Informational self-determination comprises, according to an authoritative definition in German literature:

> the right of a person to decide for herself on whether, when, the contents of, as well as the form of the use and disclosure of her personal data.[18]

Some countries have, however, refrained from adopting European-style comprehensive data protection rules and follow instead a *sector-specific* approach: such is the case of the United States of America, the law of which relies in this respect on a combination of federal and state-level legislation, administrative regulations and self-regulation instruments.[19]

Although the *Privacy Act* was adopted in the U.S. in 1974, it only applies to the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. For their most part, data protection rules in force in this country are contained in a myriad of consumer protection regulations. The right to privacy is, to be sure, protected under the Constitution of the United States,[20] but so is free speech, to which the First Amendment expressly refers and on which data protection laws potentially impinge. Unsurprisingly, no constitutional right to personal data protection is enshrined in the American Constitution.[21]

[14] See the German National Report, Sect. 1.1.

[15] See the Italian National Report, Sect. 2.1.

[16] See the Portuguese National Report, Sect. 1.

[17] See the Greek National Report, Sect. 1.1.

[18] See Larenz and Wolf (2004), p. 137: "Die informationelle Selbstbestimmung umfasst das Recht der Person, selbst über das Ob, die Zeit, den Inhalt sowie die Art und Weise der Verwendung und Preisgabe ihrer persönlichen Daten zu entscheiden". For a more recent analysis of this theme, see Sousa Pinheiro (2015) and van der Sloot (2017).

[19] See, for a detailed description of those sources, the United States of America's National Report, Sect. 1.

[20] Although the exact extent to which it is so is far from settled in case-law and legal literature: see, on this, Prosser (1960); Fried (1968); Rubenfeld (1989); and Post (2001).

[21] See, however, arguing for the constitutional recognition of a right to information self-determination, as part of the substantive due process liberty elaborated on by the U.S. Supreme Court, Eberle (2001).

hoeren@uni-muenster.de

A "light touch" regime, which establishes a minimum data protection standard, has been adopted in Singapore.[22] Other countries, such as South Africa, are still in the process of adopting general data protection legislation.[23]

Data protection rules, contained in the abovementioned legislative instruments, mostly have a mixed nature, covering both Public and Private Law issues. In fact, as noted earlier, a fundamental right to data protection has been enshrined in several countries, which enjoys the corresponding constitutional status. The enforcement of that right, and the overall supervision of the application of data protection rules, is entrusted not only to judicial, but also to administrative authorities; as a consequence thereof, a considerable number of Administrative Law rules on this topic have emerged. Liability for the breach of data protection rules, however, is to a large extent still governed by Tort Law rules. And the territorial scope of application of data protection rules is a matter essentially pertaining to the realm of Private International Law.

At the international level, a number of relevant multilateral initiatives aiming at the protection of personal data have also been undertaken by several organizations, among which the Council of Europe,[24] the United Nations,[25] and the OECD.[26] The subject is also addressed in several bilateral trade agreements.[27]

The most accomplished international instrument providing for a right to personal data protection is, however, the *Charter of Fundamental Rights* of the European Union, Article 8 of which provides, under the heading "protection of personal data", that:

(1) Everyone has the right to the protection of personal data concerning him or her.
(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
(3) Compliance with these rules shall be subject to control by an independent authority.

Three major trends can be inferred from the existing data protection legal framework, as described above: (1) the trend to adopt *specialized legislation* covering several areas of the law; (2) the trend to *constitutionalize* rules on data protection; and (3) the trend to *internationally harmonize* its regime.

The first of these trends has, however, different expressions across the world. In fact, European legal systems, as well as those more closely influenced by them,

[22]See the Singaporean National Report, Sect. 1.

[23]See the South African National Report, Sect. 2.

[24]See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg, on 28 January 1981.

[25]See Guidelines for the Regulation of Computerized Personal Data Files, adopted by the Resolution of the General Assembly 45/95 of 14 December 1990; and the Policy on the Protection of Personal Data of Persons of Concern to UNHCR, of 27 November 2015.

[26]See OECD Privacy Guidelines (revised in 2013).

[27]See the International Trade Law Special Report.

hoeren@uni-muenster.de

adopt a *systematic approach* to the regulation of data protection, consisting of legislation that comprises most, if not all, aspects of this topic, including data collection and treatment both by public and private entities: such is clearly the vision underlying the GDPR. The United States instead favors a more *topical approach*, which restricts data protection laws to specific aspects, notably the collection and treatment of personal data by public agencies, and leaves broad areas of potential conflict between data subjects and data controllers or processors to case law or self-regulation.

As for the second trend, it has also known different expressions: while a number of countries, notably in Europe, has indeed enshrined a new fundamental right to personal data protection, or at least derived it from other constitutionally recognized rights, and certain international instruments have even elevated it to the status of a human right, other countries, such as the U.S., where privacy is still essentially regarded as the "right to be left alone", have not taken this step.

Likewise, the third trend has experienced different degrees of accomplishment: whilst at the worldwide level data protection rules have so far been restricted to a limited number of highly general and abstract principles, such as quality of data, exclusion of processing of sensitive data, data security and right of access by the data subject, in the European Union a much more intense and detailed harmonization has taken place, the enforcement of which is ensured through the applicability of administrative fines to their infringement. As noted by the special rapporteur on United Nations Law, "*a single international data privacy regulatory framework is yet to be seen*".[28]

2.2 The Notion of Personal Data

The second issue to be addressed in this report concerns the notion of personal data.

In the European Union, a very broad notion of personal data has been adopted, most recently in article 4(1) of the GDPR, which comprises:

> Any information relating to an identified or identifiable natural person (data subject).

Personal data concerning legal persons are, accordingly, not included in the notion of personal data relevant for the purposes of the said Regulation.

An identifiable natural person is, for the purposes of the abovementioned provision, "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

[28] See the United Nations Special Report, Sect. 1.1.

hoeren@uni-muenster.de

IP addresses are included in the notion of personal data, according to the case-law of the CJEU.[29]

The broad European notion of personal data has been replicated in several non-EU countries.[30]

As already mentioned, in the EU the right to personal data protection is recognized as a specific fundamental right, which is distinct from privacy, although closely related to it, as is clear from the comparison of articles 7 and 8 of the Charter of Fundamental Rights.[31]

This is not the case of other legal systems, in which the right to personal data is not seen as an independent right, but rather as a derivative of the right to privacy: such is the case, *inter alia*, of South Africa[32] and the U.S.[33]

Within the notion of personal data, a distinct category is established in the European GDPR concerning particularly *sensitive data*, which are subject to special, more protective rules. Such data are defined by article 9(1) of the Regulation as:

> personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The concern with sensitive data is equally present in other jurisdictions, the law of which evidences the European influence.[34]

European legislation regarding personal data protection is in principle equally applicable to their processing by public and private entities. However, "public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing" (article 4(9) of the GDPR). Furthermore, special rules apply to the processing of personal data by European Union institutions and in criminal matters.[35]

The opposite view has prevailed in the U.S., where personal data protection rules are primarily aimed at federal agencies. This difference in part reflects, according to the American national reporter, a divergence in citizens' sources of distrust: while, to her mind, Europeans particularly distrust private corporations, Americans are apparently more concerned with their Government's attempts to invade their privacy.[36]

---

[29] See judgment of 19 October 2016, case C-581/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779.

[30] See, for instance, the Cape-Verdean National Report, Sect. 2.1; Swiss National Report, Sect. 1.1.

[31] See, on this European Union Special Report, Sect. 1.2.

[32] See the South African National Report, Sect. 2.2.

[33] See the United States of America's National Report, Sects. 1.1 and 1.2.

[34] See, for instance, the Cape-Verdean National Report, Sect. 2.2.5, and the Swiss National Report, Sect. 1.1.

[35] See, on this, the European Union Special Report, Sect. 1.3.

[36] See the United States of America's National Report, Sect. 8.

hoeren@uni-muenster.de

2.3 The Supervision Authorities

The role and nature of entities that supervise and control the processing of personal data also differ considerably across the globe.

In Europe, such entities (as is the case of, e.g., in France, the *Commission Nationale Informatique et Libertés*; in Greece, the *Hellenic Personal Data Authority*; in Italy, the *Garante per la protezione dei dati personali*; in Portugal, the *Comissão Nacional de Proteção de Dados*; in Spain, the *Agencia Española de Protección de Datos*; and, in Switzerland, the *Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte*) play an essential role in this field.

According to the GDPR, each Member State shall provide, in accordance with its constitutional organization, for the existence of one or more independent public authorities, which shall be responsible for monitoring the application of the Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. Such authorities shall act with complete independence in performing their tasks and exercising their powers.

Supervising authorities' tasks under the GDPR are manifold and include, *inter alia*: (1) the monitoring and enforcement of the application of the Regulation; (2) the promotion of public awareness and understanding of the risks, rules, safeguards and rights in relation to processing; (3) advising public institutions on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing; (4) handling complaints lodged by data subjects; and (5) conducting investigations on the application of the Regulation.

In order to perform such tasks, supervisory authorities in EU Member States are entrusted with a wide range of investigative, corrective, authorization and advisory powers. The exercise of such powers is nevertheless subject to appropriate safeguards, including effective judicial remedy and due process.[37]

Other countries have followed the European model of concentrating the supervision of data protection legislation in a single administrative body: such is the case of Japan, which has created a Personal Information Protection Commission; of Singapore, where a Personal Data Protection Commission has been set up; and of South Africa, where an Information Regulator was instituted. The legal status of these bodies—notably their independence *vis-à-vis* constitutional powers—is however extremely varied: in Singapore, for example, the said Authority is under the purview of the Info-Communications Media Development Authority, which is itself under the Ministry of Communications and Information[38]; and in South Africa the Regulator is appointed by the President of the Republic.[39]

A considerably different approach has prevailed in the U.S., where a public agency specifically devoted to personal data protection does not exist. Instead, it is

[37] See, on this, the European Union Special Report, Sect. 1.4.

[38] See the Singaporean National Report, Sect. 2.3.

[39] See the South African National Report, Sect. 3.

hoeren@uni-muenster.de

the Federal Trade Commission (FTC)—which was created in 1914 and is entrusted *inter alia* with the protection of consumers—that has become the primary privacy enforcement agency in that country.[40] Although it is an independent law enforcement agency, the FCT's jurisdiction is limited to challenging privacy violations through information practices that are deemed to be deceptive or unfair.

In Brazil, a specific data protection agency is also hitherto non-existent. Some of the tasks typically entrusted to such agencies in other countries are incumbent upon the so-called "Internet Steering Committee" (*Comité Gestor da Internet*), which was created in 1995 with the purpose of coordinating and integrating all Internet service initiatives in Brazil. Law no. 13.709, of 13 August 2018, on the protection of personal data, provided for the setting up of a National Personal Data Protection Authority (*Autoridade Nacional de Proteção de Dados*) and a National Council for Personal Data and Privacy Protection (*Conselho Nacional de Proteção de Dados Pessoais e da Privacidade*). However, the President of the Republic vetoed that Law's provisions on these institutions. Subsequently, Provisional Measure no. 869/2018 created these entities, but their setting up is still impending.[41]

2.4 The Self-Regulation Instruments

Similar conclusions may be reached in respect of the relevance of self-regulation instruments on data protection in the different jurisdictions covered by this report, which has been encouraged *inter alia* by the *OECD Guidelines governing the protection of privacy and transborder flows of personal data*, "whether in the form of codes of conduct or otherwise".[42]

Such instruments are particularly relevant, given the lack of public regulation of the sector, in the United States of America, where the Network Advertising Initiative (NAI), comprised exclusively of digital advertising companies, has adopted a *Code of Conduct*, last updated in 2017,[43] requiring transparency, an opt-in choice before sensitive information may be used for behavioral advertising and reasonable security provisions. The breach of the Code's provisions may be publicized by the NAI and reported to the FCT. Another organization, the Digital Advertising Alliance (DAA), also seeks to establish and enforce privacy practices for digital advertising through a set of *Principles of Transparency and Control to Data Used Across Devices* that apply to Multi-Site Data and Cross-App Data gathered in either desktop or mobile environments.[44] These instruments have, however, so far only obtained limited results in preserving consumer privacy.[45]

[40] See the United States of America's National Report, Sect. 1.4.

[41] See the Brazilian National Report, Sect. 2.5.

[42] See section 19d), of the *Guidelines* as amended in 2013.

[43] Available at https://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf.

[44] Available at http://digitaladvertisingalliance.org/principles.

[45] See the United States of America's National Report, Sect. 1.5.

hoeren@uni-muenster.de

In Europe, the GDPR also encourages the drawing up of codes of conduct by associations and other bodies representing categories of controllers or processors and intended to contribute to the proper application of the Regulation, which take account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises. However, such codes are subject to approval by national supervising authorities, which must assess whether they provide sufficient appropriate safeguards and, in the affirmative case, shall also register and publish them. Compliance with approved codes of conduct is to be monitored by independent bodies with an appropriate level of expertise in relation to the subject-matter of the code and accredited for that purpose by the competent supervisory authority.[46] Self-regulation by data controllers or processors is thus much more strictly allowed and controlled in the EU than in the U.S. Unsurprisingly, self-regulation instruments are considerably less developed in Europe than in the U.S.[47]

In some non-European countries, supervising authorities have taken upon themselves the task of issuing guidelines or codes of conduct concerning personal data protection: such is the case, e.g., of Singapore,[48] and of South Africa.[49] Whether binding or not, and even when issued in consultation with the industry, such instruments do not seem to qualify as self-regulation initiatives. Other non-European countries simply lack any self-regulation instruments in this area: thus far, that's, for example, the case of Brazil[50] and Cape Verde.[51]

3 Specific Problems Concerning Data Protection in the Internet

3.1 Personal Data Processed by Electronic Means

Personal data protection or, as it is more commonly referred to in Anglo-Saxon countries, *data privacy*, has become an increasingly central topic in the last two or three decades due to the rapid development of information processing technologies.

These technologies, which are closely related to the so-called Information Society, are essentially aimed at optimizing information, making it available through electronic means where and when it is necessary. The term "information" is used in this context in a very broad sense, and comprises all types of data, independently from its purposes, forms, contents or other criteria.

[46] See the European Union Special Report, Sect. 2.6.

[47] See, for instance the French National Report, Sect. 5.

[48] See the Singaporean National Report, Sect. 2.4.

[49] See the South African National Report, Sect. 3.3.

[50] See the Brazilian National Report, Sects. 1–5.

[51] See the Cape-Verdean National Report, Sect. 2.4.

hoeren@uni-muenster.de

The possibilities that information-processing technologies offer in terms of speed, ease and quantity of data processing intensify the potential harm caused by its unauthorized use. These possibilities have caused alarm in relation to certain types of data, leading several countries to react through the enactment of specific legislation or, whenever specific legislation is absent, giving rise to significant, and often controversial, case law. Personal data has been in the center of these concerns.

It isn't possible to address in detail all topics related to personal data processed by electronic means, as there are countless relevant ones in this regard. The exact configuration of the right to be forgotten in the electronic context, the process for obtaining a valid consent for personal data processing online, the operation of the information right by electronic means, the meaning of the "privacy by design" and the "privacy by default" concepts in this same context, profiling and portability, are just some of those topics. Some decisions had to be taken in order to select the topics which are addressed in more detail. The selected topics are, thus, those with a wider scope, which comprise many of the other topics,[52] as well as those which have been in the spotlight of important case law or new legislation. In this regard, topics such as portability or profiling aren't dealt with, autonomously, in a separate section.

Some brief lines should be dedicated, though, to the challenge of data portability and its potential impact in the economy and in the protection of the data subjects. Data portability grants the data subject a right to have the personal data transmitted directly to him or to another entity, through electronic means. Data portability, inasmuch as it requires the adoption of technical standards to ensure interoperability between the different entities that process those data, promotes the free movement of personal data and, consequently, works as an inducement or a driving force to the economy. The easiness of personal data transfer may promote competition, improving innovation and service variety. Although there is sectorial legislation granting data portability, dating back from the 1990s,[53] the general right to data portability provided by the GDPR, which is applicable in all contexts, with minor exceptions, is noteworthy.[54]

Also noteworthy are the GDPR provisions on profiling. The ability to build a very complete psychological profile of the data subject has been made possible by current technologies,[55] and the possibilities keep evolving. Taking into account the particular risks posed to the data subjects by profiling, some legal systems have adopted specific rules to deal with these risks. Swiss law is one of those legal systems, since it requires the controller to conduct an impact assessment in case of profiling, given the fact that this form of data processing may pose a threat to the data subject's privacy.[56] The GDPR also addresses profiling. Besides setting out particular

[52]Security obligations, for example, cover concepts such as "privacy by design", which represents a deepening and an extension of those obligations. On privacy by design, see Orrù (2017).

[53]See, for instance, the United States of America's Health Insurance Portability and Accountability Act of 1996.

[54]See article 20 of the GDPR.

[55]See the International Trade Law Special Report, Sect. 4.

[56]See the Swiss National Report, Sect. 2.8.

hoeren@uni-muenster.de

requirements for authorizing the profiling, it grants the data subject the right not to be subject to a decision based solely on automated processing, including profiling.[57]

In France, the constitutionality of legislation enacted to adapt domestic law to the GDPR has been challenged in respect of this particular topic. The *Conseil Constitutionnel* held that a decision based on automated processing is possible, as long as it obeys to certain conditions, such as the fact that it does not involve the processing of sensitive data and it is subject to an administrative appeal.[58]

Some other aspects of data protection though electronic means are separately dealt with in the following pages in a more detailed way. First, national legal systems will be compared in respect of the existence of legislation or relevant case law covering the protection of personal data in the context of services provided at a distance, by electronic means, at the individual request of a recipient of services. Subsequently, specific aspects of data protection in this context will be compared in the jurisdictions covered by this report, such as electronic communications for marketing purposes, protection of minors, the existence of a right to be forgotten, the processing of employees' data and security obligations and data breach notifications.

3.1.1 Processing of Personal Data in the Context of Services Provided at a Distance by Electronic Means

Even before the adoption of the GDPR, the European Union had set out a considerable number of rules, both through the Directive on electronic commerce[59] and through the Directive on privacy and electronic communications,[60] which are applicable to services provided at a distance, by electronic means, at the individual request of their recipient. These rules reinforce the protection of data subjects whenever their personal data are processed in the context of electronic communications.

The European Union's Directive on electronic commerce, expressing consumer protection concerns, addresses the requirements for the conclusion of contracts by electronic means by imposing that certain information be mandatorily provided in a durable medium, such that the recipient of the services may store and reproduce it. When combined with the obligation to provide certain minimum information to data subjects relating to personal data processing, set forth in the GDPR,[61] this

[57] See article 22 of the GDPR.

[58] See the French National Report, Sect. 2.

[59] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), OJ L 178, 17.07.2000, pp. 1 ff.

[60] See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Directive on privacy and electronic communications"), OJ L 201, 31.7.2002, pp. 37 ff.

[61] See article 13 of the GDPR.

hoeren@uni-muenster.de

requirement means that the information provided in a durable medium must include the mandatory privacy policy terms.

Furthermore, the Directive provides that service providers that send unsolicited commercial communications by electronic mail should consult regularly and respect the existing opt-out registers, containing the identification of data subjects that did not give their consent to receive those communications. The legislation of EU Member States reflects the transposition of these provisions.[62]

The legal framework for unsolicited commercial communications and for managing personal databases for that specific purpose is further detailed in the Directive on privacy and electronic communications. Although primarily designed to regulate privacy in the electronic communications sector, notably the processing of personal data in connection with the provision of publicly available electronic communications services and public communications networks, including public communications networks supporting data collection and identification devices, this Directive includes several provisions applicable to the processing of personal data by electronic means, in general, whether by a provider of a publicly available electronic communications service or networks or by any other entity. This Directive establishes, as a rule, an opt-in system for unsolicited commercial communications, requiring the prior consent of the data subject, except for certain specific scenarios, such as in the context of the sale of a product or a service. Moreover, this Directive addresses the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user of an electronic service. According to the Directive, this specific data processing, such as the one that takes place with the use of cookies in certain websites, shall only be permitted on the condition that the subscriber or user concerned has given his or her consent, which must be preceded by clear and comprehensive information on the conditions of the corresponding processing of personal data.[63]

The abovementioned legal framework, contained in the European Union's directives, has been transposed to the Member States' domestic laws.[64] In certain circumstances, though, the conformity of national legislation with the European

[62]See, for example, Spanish National Report, Sects. 2.1.1 and 2.1.2.

[63]The Directive on privacy and electronic communications also covers obligations to protect personal data conveyed and stored through electronic means, as well as obligations to inform third parties about data breaches. Nevertheless, and contrarily to the previous provisions, these obligations are set out only for providers of publicly available electronic communications services and or for providers of public communications networks and, consequently, should be addressed in the following topic, regarding data protection in the electronic communications sector.

[64]See, for instance, the opt-in system referred to in the German National Report, Sect. 2.1.4, the Portuguese National Report, Sect. 2, the Greek National Report, Sect. 2.1.1, the French National Report, Sect. 2, and the Spanish National Report, Sects. 2.1.1 and 2.1.2. The national provisions on the storing of information, and access to information already stored, in the terminal equipment, are also included, for example, in the Czech Republic National Report, Sect. 2.1, the Portuguese National Report, Sect. 2, the Greek National Report, Sect. 2.1.1, the French National Report, Sect. 2, and the Spanish National Report, Sect. 2.1.2.

hoeren@uni-muenster.de

Union's legal framework has been challenged, as was the case of the transposition of the opt-in system in the Czech Republic.[65]

The gap that divides the European Union Member States' legal systems and the United States' legal system is rather evident in respect of this first set of statutory provisions.

Contrasting with the increasing consumer protection concerns in the European Union, the United States of America has no federal legislation that grants a private right of action to consumers based on unsolicited commercial communications by electronic mail. Although there is a federal law that applies to all commercial emails[66] and gives their recipients the right to prohibit marketers from continuing to send commercial communications by electronic mail, through an opt-out system, this law is primarily enforced by the FTC. Instead of setting up clear rules for companies on how personal data should be processed, the FTC has focused mainly in raising awareness about the issues that companies should consider when collecting data.[67] At the state level, the small number of laws that regulate electronic marketing has a very narrow scope and is applied to very specific sectors of activity.

It is noteworthy that the other legal systems comprised in the scope of this study that have legal provisions on this particular topic bear a greater resemblance to that of the European Union,[68] which widens the gap between the United States and other parts of the world. This can be explained by several factors, including those legal systems' cultural or geographical proximity with the European Union, their historical tradition of protecting personality rights, or, more interestingly, the convenience to adapt themselves to the most demanding legislation in order to provide legal certainty to international transactions. Switzerland has an opt-in-system.[69] Japan has two laws that regulate unsolicited commercial communications by electronic means, both of them setting an opt-in system.[70] The recent general data protection law enacted in South Africa, although not yet fully in force, provides for an opt-in system, which will repeal the existing opt-out system currently laid down by specific legislation on electronic communications and transactions.[71]

In the United States, the most important federal legislation applicable to services provided at a distance and designed to protect personal data is the Fair and Accurate Credit Transactions Act (hereinafter FACTA).[72] In the specific context of online

[65] See the Czech National Report, Sect. 2.1.

[66] Controlling the Assault of Non-Solicited Pornography and Marketing of 2003 (CAN-SPAM Act).

[67] See the United States of America's National Report, Sect. 2.2.

[68] See the South African National Report, Sect. 4.1.2, the Swiss National Report, Sect. 9, the Japanese National Report, Sect. 3.1.1, the Canadian National Report, Sect. 2.3 and the Singaporean Report, Sect. 3.7.1. Other non-European countries don't have any relevant provisions on this subject (see the Cape Verdean National Report, Sect. 3.1, according to which Cape Verde' provisions on this topic concern exclusively the electronic communications sector, and the Brazilian National Report, Sect. 3.1).

[69] See the Swiss National Report, Sect. 3.

[70] See the Japanese National Report, Sect. 3.1.1.

[71] See the South African National Report, Sect. 4.1.2.

[72] See the United States of America's National Report, Sect. 2.1.

hoeren@uni-muenster.de

transactions, FACTA protects consumers from identity theft and ensures that consumers' credit information is accurate. FACTA includes provisions on security of card-related data and the ability to place fraud alerts. This Act grants consumers the right to request and obtain a free credit report per year from the three main consumer credit reporting companies in the United States. Notwithstanding the fact that FACTA does protect personal data processed by electronic means, this Act is designed to reduce credit fraud and improve confidence in online transactions. Its rules are, thus, primarily aimed at protecting electronic commerce, rather than personal data.

It is also relevant to highlight the fact that whenever regional trade agreements contain provisions on electronic commerce, they frequently include personal data protection rules.[73] Although these rules differ in their extent and effectiveness,[74] some of those agreements encourage the enactment of data protection rules by their Member States. The fact that these may be required to adopt certain minimum data protection rules in order to be able to conclude such trade agreements naturally contributes to the expansion and enhancement of personal data protection and encourages harmonization in this area.

As already mentioned, international organizations, such as the United Nations, also play a significant role in setting common rules on personal data protection in the context of services provided at a distance by electronic means.[75]

3.1.2 Protection of Minors' Personal Data Processed by Electronic Means

In the European Union, the GDPR sets forth additional relevant rules for personal data processing by electronic means, such as restrictions on profiling, which is defined as a form of automated processing of personal data,[76] data breaches notification procedures, protection of minors in relation to information society services and the right to be forgotten, among many others.[77]

The protection of minors in relation to information society services is regulated by specific provisions in several countries and, in some of them, such as the United States, through specific laws.

In this respect, the GDPR's main concern is to set special requirements regarding a child's consent in relation to information society services. Where personal data processing is based on the consent given by the data subject, the GDPR has given Member States the possibility to choose the age limit above which a child may give a valid consent to operators of information society services, without the intervention of

[73] See the Data Protection in International Trade Law Special Report, Sect. 8.1.

[74] See the Data Protection in International Trade Law Special Report, Sects. 8.1 and 9.

[75] See *supra,* Sect. 2.1, and the instruments mentioned therein.

[76] See article 4(4) of the GDPR.

[77] See the European Union Special Report, Sect. 2.

hoeren@uni-muenster.de

the holder of the corresponding parental responsibilities.[78] Nevertheless, that age limit cannot be set below 13 years. In the event that a Member State chooses not to regulate this topic, the processing of data of children below the age of 16 years in that context is only deemed lawful to the extent that consent is given or authorized by the holder of the parental responsibility over the child.

The United States has a specific law for regulating the processing of personal data of children under the age of 13 by operators of websites or online services.[79] The Children's Online Privacy Protection Act of 1998 (hereinafter COPPA) imposes certain specific requirements for the processing of data on operators of websites or online services directed to children under 13 years of age and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. COPPA has assigned the enforcement of its provisions to the FTC, at the federal level, and has given this agency the power to promulgate rules to guide the interpretation and enforcement of this Act. Taking into account that COPPA was enacted in 1998, and technology and the risks that it poses to children have evolved radically since then, the FTC has updated and expanded the focus of the COPPA regulations and has issued additional guidance. Although the COPPA Act itself does not provide for specific penalties, courts have determined damages pursuant to the Federal Trade Commission Act, because COPPA infringements are considered to be unfair or deceptive trade practices under that Act. Nevertheless, there is no private cause of action for COPPA infringement, so states have to file civil actions to obtain injunctions and damages in the interest of their citizens.[80]

With regard to the consent of the minor when using the services regulated under the COPPA, which consists in the single topic specifically regulated under the GDPR regarding minors, COPPA determines, as a rule of thumb, that prior to any collection, use, and or disclosure of personal information from a child under 13, the respective operator must obtain verifiable parental consent. Furthermore, COPPA regulates in detail the requirements for obtaining a verifiable parental consent, defining admissible methods for this purpose.

Therefore, with respect to minors' personal data protection, when using online services and or websites, the United States of America has more detailed and restrictive legislation than the European Union.

Other countries covered by this report do not have specific provisions on the protection of minors' personal data processed by electronic means.[81] In the absence

[78]See the European Union Special Report, Sect. 2.2. Some European Union Member States have already set their age limit under this GDPR provision. By way of example, after the full implementation of the GDPR, on the 25th of May 2018, France has set that age limit at 15 years through its Law of 20 June 2018.

[79]See the United States of America's National Report, Sect. 2.3.

[80]Important case law on this subject has been further developing processes for determining damages. See the United States of America's National Report, Sect. 2.3, referring to the case law United States v. Boston Scientific Corp., 253 F. Supp. 2d 85, 98 (D. Mass. 2003).

[81]See, for example, the Canadian National Report, Sect. 2.1.

hoeren@uni-muenster.de

of specific provisions, the consent given by children is regulated by common law or general statutory rules on whether and to what extent minors may personally exercise their rights and conclude contracts.[82]

In this regard, it is important to highlight the fact that France is the only European Union country included in the scope of this report which, previously to the GDPR, had specific provisions on the protection of personal data of minors processed by electronic means.[83] According to the French legal framework applicable before the GDPR, minors had a specific right to obtain the erasure of personal data collected online concerning him or her. This right, which may also be denominated as a right to be forgotten, or a right to the erasure of personal data, according to the terminology of the GDPR, is now extended to all data subjects comprised in the scope of application of the GDPR.

3.1.3 The Right to the Erasure of Personal Data Processed by Electronic Means

This leads us to another relevant provision of the GDPR related to the protection of personal data processed by electronic means: the "*right to be forgotten*", enshrined in the GDPR and recognized, long before it came into force, in the CJUE's judgment on the *Costeja* case.[84]

Under the GDPR, the data subject, besides having the right to obtain the erasure of its personal data directly by the data controller, whenever one of the grounds provided for in article 17 applies, also has the right to have its personal data erased by other entities which may have linked, copied or, in any other way, disseminated those data, particularly when they were made public.[85] The said provision was

[82]See, for instance, the Singaporean National Report, Sect. 3.3. Advisory guidelines from the Singaporean administrative body also comprise guidelines on the treatment of minors, including how consent to obtaining and using their data should be obtained. The South African National Report, Sect. 4.1.3, refers to specific provisions for the protection of minors, included in a data protection law. These provisions determine the conditions under which minors personal data may be processed. Albeit relevant, these are general provisions, applicable to all types of personal data processing related to minors, regardless of the means used. Therefore, these provisions aren't specific for the processing of personal data by electronic means.

[83]See the French National Report, Sect. 2.

[84]See the judgment of the CJEU of 13 May 2014, rendered in case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317. In this case, the CJEU held that an electronic search engine operator is the controller of the processing of personal data available on the websites, run by third parties, which appear on its search results lists. Consequently, the respective data subject may approach that operator directly in order to obtain the removal of a hyperlink to a certain website from the search results list, as long as this website contains his or her personal data and even if this data is accurate and doesn't have to be removed from the website where it is made available. On this case, see de Vasconcelos Casimiro (2014).

[85]See the European Union Special Report, Sect. 2.3.

hoeren@uni-muenster.de

clearly designed for the online environment,[86] as it is stated in the corresponding recital of the GDPR.[87]

A right with such an extensive scope has no equivalent in the other jurisdictions covered by the present study.[88] However, in most countries, as is the case of South Africa[89] and Brazil,[90] there is a general right to obtain the erasure of personal data whenever their processing is no longer authorized, similar to that which was already set out in Directive 95/46/EC.[91] Japan stands out in this respect, for its restrictive understanding of the right to erasure of personal data processed by electronic means. In Japan, there are no statutory laws or administrative guidelines regulating a right to the erasure of personal data comparable to that of the GDPR. Additionally, court cases in that country have emphasized the importance of other legal interests whenever there is a request to remove contents from search results. In particular, the Japanese Supreme Court has held that a search engine service provider is under the obligation to delete search results only in the event that the legal interests involved in the deletion are clearly superior to the legal interests involved in providing the search results. This court has stressed the social importance of the search engine in the Internet era.[92] Nevertheless, case law in Japan confirms that search engines are obliged to erase results containing infringements, including, thus, infringements to data protection legislation.

It can therefore be concluded that although most jurisdictions covered by this report recognize a right to the erasure of personal data, currently the broadest and most detailed provisions in this respect are set forth in the GDPR.

In this respect, the United States also differ from most countries for not having a provision or relevant case law related to a general right to delete personal data, particularly in the online context.

[86]Following the CJEU decision in the Google Spain case, there are some relevant case law and administrative decisions relating to this topic. The Portuguese data protection authority, for example, issued a decision (section 536/2016, not publicly available) imposing on a search engine operator the removal of search results relating to a public figure that was under the suspicion of having committed a crime 8 years earlier. See the Portuguese National Report, Sect. 2.

[87]See the GDPR, recital 66.

[88]See, for example, the Canadian National Report, Sect. 2.2.

[89]See the South African National Report, Sect. 4.1.4.

[90]See the Brazilian National Report, Sect. 3.3.

[91]The Law section 13.709, of 13 August 2018, on the protection of personal data introduce this right. See the Brazilian National Report, Sect. 3.3.

[92]See the Japanese National Report, Sect. 3.1.3.

hoeren@uni-muenster.de

3.1.4 Protection of Employees' Personal Data Processed by Electronic Means

Another topic which accentuates differences between the European and the United States' legal framework on personal data processed by electronic means is the processing of employees' personal data.

Employees enjoy few privacy rights in their workplace in the United States.[93] At the federal level, the Electronic Communications Privacy Act of 1986 (hereinafter ECPA) is the law that primarily governs the monitoring of electronic communications in the workplace. The ECPA prohibits individuals and companies from intercepting electronic communications. However, there are two exceptions to this prohibition that apply to the workplace. One of the exceptions allows interception for monitoring purposes of employees' electronic communications by the employer as long as the interception is done in the "ordinary course of business" and the employer uses certain limited types of equipment to monitor those communications. Based on this exception, many employers use electronic mail systems that automatically copy all messages that pass through their system in order to monitor their employees' productivity and illegal conduct. The other exception gives employers the right to track the websites visited by their employees. In addition to the interception of electronic communications without the consent of the employee, under the referred exceptions, the employer may monitor other electronic communications, including personal messages of the employee, as long as the employer can demonstrate the employee's consent for that monitoring. Some courts have held that this consent may be a tacit one. It is also important to highlight the fact that the definition of electronic communications for interception purposes does not include communications held in electronic storage and that, for that reason, courts have been granting the possibility to read the private electronic messages of employees stored in electronic systems.[94]

Although the Fourth Amendment to the Constitution of the United States grants employees who work for public employers a specific right against "unreasonable government searches", this right has been interpreted in a very restrictive sense in the context of personal data processed by electronic means. The Supreme Court of the United States, in particular, has adopted a very restrictive interpretation of this constitutional right, by requiring an adequate balance between the protection of the public employee and the government's need for an adequate supervision control and for an efficient operation of the workplace.[95]

The monitoring of an employee's activity on electronic social networks is prohibited under the Stored Communications Act (hereinafter SCA), although this prohibition is easily circumvented in the event that the electronic communication made available in those networks is readily available to the public or is disclosed by

[93] See the United States of America's National Report, Sect. 2.5.

[94] See the United States of America's National Report, Sect. 2.5.

[95] See the United States of America's National Report, Sect. 2.5.1.

hoeren@uni-muenster.de

an authorized receiver of the communication. There are several cases denying relief to employees fired on the grounds of the content of communications made available on electronic social networks.[96]

Sectoral legislation may, however, offer some protection to employees in certain specific areas and under specific statutes, such as the protection of their credit card information, under the FACTA, medical records, genetic information and disabilities.[97]

At the state level, there are no significant additional protections for employees in the context of personal data processed by electronic means. It is, therefore, a fact that the United States' legal framework, both at the federal level and at the state level, does not grant employees significant protection in that context.

In contrast with the United States, the European Union Member States have developed a very strict legal framework that affords employees a considerable level of protection to their personal data, whenever processed by electronic means.[98] While in the United States there are many exceptions to the protection of the personal data of employees, processed by electronic means, in the European Union such exceptions are much less extensive and numerous, and they are mainly justified by the legitimate interests of the employer.

Although the GDPR does not contain specific rules concerning this topic,[99] Member States have a considerable level of freedom to accommodate their own solutions and, in particular, they may provide protections beyond the minimum requirements set forth in that legal instrument.[100] This is true in general and specifically in this case, since the GDPR contains a general clause allowing Member States to provide for specific rules to ensure the protection of rights and freedoms in respect of the processing of personal data of employees in the employment context.[101] Additionally, collective agreements may provide for specific rules for personal data processing in the employment context, including the conditions for processing based on the consent of the employee.[102]

The exercise of the right to exceed the minimum requirements set forth in the European Union's legal framework is particularly noticeable in what concerns the processing of personal data of employees through electronic means. Member States have specific legislation, administrative guidance and, in some cases, abundant case law on this subject.

---

[96]It is noteworthy that, since 2012, 25 states have enacted legislation preventing employers from forcing their employees to disclose the respective passwords. See the United States of America's National Report, Sect. 2.5.3.

[97]See the United States of America's National Report, Sect. 2.5.

[98]See van der Sype et al. (2017).

[99]See the European Union Special Report, Sect. 2.4.

[100]See, for instance, article 5 of the GDPR, which sets out the main principles applicable to the processing of personal data, such as lawfulness, fairness and transparency, purpose limitation, minimization, accuracy, storage limitation, integrity, confidentiality and accountability.

[101]See article 88(1) of the GDPR.

[102]See recital 155 of the GDPR.

hoeren@uni-muenster.de

This is the case of Spain,[103] Portugal,[104] Germany,[105] Italy,[106] Czech Republic,[107] Romania,[108] France[109] and Greece.[110] All these countries have specific statutory provisions on the protection of employee's personal data, including personal data processed by electronic means.[111]

Portugal is illustrative in this regard. The Portuguese Labor Code (approved by Law no. 7/2009, of 12 February 2009, as amended), provides that employees have the right to privacy in the workplace.[112] Among other rules, it states that the employer may not use distance surveillance means at the workplace through the use of technological equipment, such as closed-circuit television, in order to control the professional performance of the employee. The use of such monitoring equipment may only serve specific purposes, notably to ensure the safety of people or goods, or to meet particular demands arising from the specific activity involved. Furthermore, the data collected by these means are considered sensitive data.[113] There is also extensive Portuguese case law and administrative guidance on topics related to the processing of employees' data by electronic means, such as geolocation of vehicles used by employees, the use of electronic equipment at the workplace, access control management systems and biometric systems, among many others.

It should be noted that these domestic law provisions are intended to grant additional protection to employees or to clarify the legal regime already applicable under the GDPR or other general provisions on data protection. This means that, besides these specific provisions, employees enjoy the protection provided by the general personal data legal framework. The main reason why the European Union countries have enacted specific legislation or issued guidance in this regard relates to the fact that an employee is particularly vulnerable at the workplace and in the employment context in general, given its subordination to the employer, and may feel pressed to accept restrictions to its privacy rights.

Nevertheless, under certain conditions, the employer may legitimately access electronic communications of an employee. Such is the case, for example, when the rules adopted by the latter include that possibility and are notified in advance to

[103] See the Spanish National Report, Sect. 2.1.6.

[104] See the Portuguese National Report, Sect. 2.

[105] See the German National Report, Sects. 2.1.5–2.1.7.

[106] See the Italian National Report, Sect. 2.3.

[107] See the Czech National Report, Sect. 2.2.

[108] See the Romanian National Report, Sect. 3.2.

[109] See the French National Report, Sect. 2.

[110] See the Greek National Report, Sect. 2.1.4.

[111] Some non-European countries, such as Singapore, also cover the protection of personal data of employees, although there are no specific statutory provisions for these data subjects. See the Singaporean Report, Sect. 3.5.

[112] See article 16 of the Code.

[113] See the Portuguese National Report, Sect. 2.

hoeren@uni-muenster.de

the former. In any event, an employer should not have access to an employee's private communications. As a rule, tracking websites visited by employees is not allowed. Nevertheless, the employee's activity in electronic social networks may be used to justify dismissals, insofar as the information at stake is publicly accessible.[114]

3.1.5 Security Obligations and Data Breach Notifications Concerning Data Processed by Electronic Means

The GDPR has also introduced stricter provisions regarding the notification of security and data breaches. According to these provisions, the data controller and the data processor are obliged to implement technical and organizational measures, such as encryption, in order to ensure a level of security that is appropriate to the risks inherent to the processing. The obligation to implement security measures was already provided for in the Directive 95/46/EC.[115] The main novelty lies in the provisions on data breach contained in the GPDR.

Data breach is defined in a very broad sense and there are specific obligations on data controllers to notify a personal data breach to the supervisory authority and, under certain circumstances, to the data subject.[116]

In the United States, neither of these two topics, *i.e.*, security obligations and data breach notification obligations are regulated in a general federal law, despite efforts to pass federal legislation in this respect. Security provisions and notification obligations are therefore disseminated in various sector-specific legislative enactments. Notification provisions usually require the implementation of a notification policy, including procedures for incident reporting, incident handling and data breach notification requirements.[117]

In the remaining legal systems, solutions differ. In certain countries, such as Japan although there are provisions on security measures, there is no general obligation to notify an authority or data subject of a data breach.[118] However, certain practices have been implemented and guidelines were adopted in this respect.[119] In Canada, there are data breach notification provisions.[120]

It is expected that in the coming years more and more countries will implement security obligations, as well as data breach notification obligations. This is a trend that has started at the beginning of the twenty-first century and that has been steadily

[114] See, for example, the French National Report, Sect. 2.

[115] See the European Union Special Report, Sect. 2.5.

[116] See the European Union Special Report, Sect. 2.5.

[117] See the United States of America's National Report, Sect. 2.7.

[118] Except for the My Number Act, which set forth the obligation to report data breaches, for certain relevant institutions. See the Japanese National Report, Sect. 3.1.5.

[119] See the Japanese National Report, Sect. 3.1.5.

[120] See the Canadian National Report, Sect. 2.5.

hoeren@uni-muenster.de

expanding across the globe. Singapore is a good example of this trend. It started by adopting, in 2012, a statutory rule imposing a general obligation to protect personal data from unauthorized use. This rule was complemented with detailed guidelines issued by the Personal Data Protection Commission and developed by case law. Further laws and regulations on this subject, comprising a mandatory data breach notification regime, are intended to be tabled in Parliament in the near future.[121]

3.2 Data Protection in the Electronic Communications Sector

The electronic communications sector—which is a new term for the telecommunications sector—and the legislation governing it have been developing for more than a century.

Communications often have a transnational character, since they take place without consideration of national borders. This transnational character, combined with the fact that the International Telecommunications Union (hereinafter ITU)[122] is the oldest international organization, explains the existence of a relatively large set of harmonized rules applicable to electronic communications at the international level.

Given this international context, data protection in the electronic communications sector benefits from a certain level of harmonization within the geographical scope of the present study.

For this reason, all jurisdictions covered by this report have adequate and very comprehensive legislation, regulation and supervisory systems concerning the electronic communications sector, which, given the international context in which they were adopted, are extremely similar. In each country, there are specific statutes that regulate the electronic communications sector, which comprise provisions on data protection in this sector.[123] The prohibition of the interception of communication data and, in general, the obligation to guarantee the confidentiality of communications are enshrined in international instruments such as the Universal Declaration of Human Rights of 1948, the European Convention on Human Rights of 1950 or the European Union Charter of Fundamental Rights of 2000. Several countries have transposed the provisions of these international instruments into their national legal systems.

[121] See the Singaporean National Report, Sect. 3.6.

[122] The ITU, originally the International Telegraph Union, was created in 1865 and is, since 1947, a United Nations specialized agency. ITU is an international body that promotes the development of telecommunication networks and access to telecommunication services by fostering cooperation among governments and standardizing technologies and protocols, among many other undertakings. See http://www.itu.int.

[123] See, for example, the United States of America's National Report, Sect. 3, the European Union Special Report, Sect. 3, the Cape Verdean National Report, Sect. 3.2, and the Japanese National Report, Sect. 3.2.

hoeren@uni-muenster.de

Furthermore, different categories of communications data are subject to different confidentiality levels of protection. The protection of confidentiality in communications entails the implementation of security measures, as well as of notifications obligations, including security breaches or data breaches notification obligations, which are provided for in the legislation of all analyzed legal systems. In all these systems, there is also a national independent authority with supervisory powers in the electronic communications sector.[124]

3.3 Data Protection and Digital Forensics

Security concerns and the need to collect, preserve, analyze and transmit factual evidence in criminal investigations, as well as in civil procedures, in the specific context of data processed by electronic means, have determined the establishment of a legal framework allowing, under certain conditions, restrictions to personal data protection for these specific purposes.

That legal framework—which, in the context of electronic communications, is designed as an exception to the confidentiality of communications—exists in all countries comprised in the scope of this study.[125]

Nevertheless, the extent those the restrictions on personal data protection and, most importantly, the conditions under which they operate, differ significantly.

Again, the United States of America stands out in this respect among other countries.[126] The ECPA is the primary federal legislation that regulates privacy on electronic communications. This Act regulates the interception and collection of electronic communications, not only when in transit but also when stored on an equipment.

The particularity of the United States' legal framework stems from the fact that the ECPA has been amended several times and that some of these amendments, most notably the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (hereinafter USA PATRIOT Act), have greatly facilitated the access to personal data processed by electronic means.

There is case law holding that the USA PATRIOT Act violates the First Amendment to the United States' Constitution, as it allows the Federal Bureau of Investigation to resort to certain mechanisms in order to obtain electronic communication service providers' customer records without giving them the possibility of

[124]See, for example, the Portuguese National Report, Sect. 3, the Cape Verdean National Report, Sect. 3.2, and the Spanish National Report, Sect. 2.2.

[125]See the United States of America's National Report, Sect. 4, the European Union Special Report, Sect. 3.4, the Cape Verdean National Report, Sects. 20–21, and the Singaporean National Report, Sect. 3.8.

[126]See the United States of America's National Report, Sect. 4.

hoeren@uni-muenster.de

challenging such requests.[127] Nevertheless, the ECPA is still in force and allows the Government to routinely access personal data processed by electronic means, such as data held by search engines, social networks and providers of electronic communication services.

In addition to ECPA, the Communications Assistance for Law Enforcement Act of 1994 (hereinafter CALEA), as well as the SCA contribute to a legal framework that facilitates the access of government to personal data processed by electronic means. The CALEA, for example, requires electronic communication network providers to redesign their network architectures to make it easier for the government to wiretap digital telephone calls. Data retention is also facilitated and even stimulated under the United States' federal legislation.

The European Union's legal framework embodies a totally different approach. The protection of personal data is a fundamental right, enshrined in a comprehensive general regulation. Consequently, all restrictions to this right must be applied to the minimum possible extent.

In the context of criminal proceedings and forensics,[128] the most important instrument providing common rules for the processing of the personal data of individuals involved in criminal proceedings is Directive (EU) 2016/680.[129] This European act grants a high level of protection to the personal data of natural persons while facilitating the cooperation between competent authorities of Members States. Furthermore, article 15(1) of the Directive on privacy and electronic communications, which establishes, among other important provisions, the confidentiality of electronic communications, provides, under the heading "Application of certain provisions of Directive 95/46/EC":

> Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

[127] See the United States of America's National Report, Sect. 4.1.

[128] See the European Union Special Report, Sect. 3.4.

[129] See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

hoeren@uni-muenster.de

This provision is one of the most controversial ones in the European Union's data protection legal framework. It led to the approval of the Data Retention Directive,[130] which was considered invalid by the CJEU.[131] The Court decided that the Directive did not strike an adequate balance between personal data protection and the public interests underlying criminal investigations. The Data Retention Directive provided that Member States should impose electronic communications service providers the obligation to retain certain communications data, such as traffic data, for a certain period of time. If necessary, these communications data could be used in the investigation of serious crimes. Among other aspects stressed by the Court, this Directive did not define precise boundaries or adequate safeguards concerning the period of time during which data retention could take place or concerning the entities which could access those data. This judgment is illustrative of the position of the European Union regarding restrictions to personal data protection, since it establishes a very demanding level of requirements for the lawfulness of these restrictions, and highlights the fact that the EU and the US are evolving in opposite directions.

A brief reference to another topic that may raise an interesting debate in respect of digital forensics, particularly with regard to its limits, is in order. As cyberspace challenges existing State borders, digital forensics rules aimed at extracting evidence from computer systems should take into account the sovereignty of States and create limits whenever a computer system spreads throughout several States. Some of the legal systems comprised in this study seem to have a very broad understanding of these limits, at least in specific circumstances. According to recent amendments to the Singaporean Criminal Procedure Code, investigators located in Singapore may inspect and search, in or from Singapore, any data stored on or available to a computer implicated in the investigation, regardless of whether the computer is located inside or outside Singapore.[132] While the stated intent is to enable access to data on web-based email accounts or web storage accounts residing in computers outside Singapore, the wording remains fairly broad.[133] In Portugal, the Cybercrime Law also has a controversial provision on computer data searching, providing that whenever, in the course of a search, there are reasons to believe that the data sought are found elsewhere in the system, this search may be extended to other parts of that system. This provision raises several doubts as to its exact territorial scope.[134]

[130]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006 OJ L 105, 13.04.2006, p. 54.

[131]See the judgment of the CJEU of 8 April 2014, joined cases C-293/12 and C-594/12, *Digital Rights Ireland v Seitlinger*, ECLI:EU:C:2014:238. In a similar vein, although relating to national legislation which had transposed the data Retention Directive, see the judgment of the CJEU of 21 December 2016, joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

[132]See the Singaporean National Report, Sect. 3.2.

[133]See the Singaporean National Report, Sect. 3.2.

[134]See article 15(5) of the Portuguese Cybercrime Law (Law section 109/2009, of 15 September 2009).

hoeren@uni-muenster.de

In the United States, a recently approved federal law also raises interesting questions concerning sovereignty in cyberspace. In 2018, the Clarifying Lawful Overseas Use of Data Act (hereinafter CLOUD Act) was enacted in order to amend the SCA. The Cloud Act allows federal law enforcement agencies to issue a warrant to electronic communications service providers based in the United States in order to demand the provision of data stored in any server they own and operate, regardless of whether the data are stored in the United States or on foreign soil. In the event that these service providers believe that the request violates the laws of the foreign country where the data are stored, the Cloud Act provides for a mechanism to facilitate the interaction with the foreign country, through executive agreements, as an alternative to the usually slow process followed under a mutual assistance, treaty (hereinafter MLAT). The standard mechanism used in a context of cross-border law enforcement, in order to request data or aid in data discovery in a foreign country, consists in resorting to informal mutual legal assistance or to formal MLAT, which requires the consent, on equal terms, of the countries involved. Under the Cloud Act, even if the electronic communications service provider considers that the request of the federal law enforcement agency violates the law of the country where the data is stored, the alternative mechanisms should consist of those set forth in the United States' law.

3.4 Data Protection and Electronic Surveillance for Security and Defense Purposes

Restrictions to personal data protection for security and defense purposes are one of the most complex topics in this field. The difficulties in determining the proper balance between the values at stake have given rise to intensive debate.

The European Union's legislation does not provide guidance on this subject, since it falls outside its jurisdiction.[135] It is up to each Member State to enact its national legislation in this respect, without an obligation to reach harmonization in the Union. For this reason, national legislation differs also in this part of the globe.

In the Czech Republic, for example, a bill is pending to amend the Act on Military Intelligence, which, if approved, shall allow the military intelligence to access traffic data, upon previous authorization from the court.[136]

In Portugal, the Security Information Service and the Strategic Defense Information Service may, under determined circumstances, gain access to banking and tax data, data on communication traffic, locality or other data connected with communications.[137]

[135] See the European Union Special Report, Sect. 3.4.

[136] See the Czech Republic National Report, Sect. 5.

[137] See the Portuguese National Report, Sect. 3.

hoeren@uni-muenster.de

In South Africa there are specific provisions allowing the electronic surveillance in the event that there are grounds to believe that there is a potential threat to national security.[138]

In France, there is a specific law on electronic surveillance of international electronic communications.[139] Additionally, the French Code of Internal Security provides for the electronic surveillance of individuals who may represent a serious threat to public order. The French Code of Defense also has provisions which ensure the security of national information systems. The French Criminal Procedures Code provides for specific provisions regarding the implementation of electronic surveillance mechanisms. This implementation is subject to the approval of the Minister of Justice.

In the United States, the Foreign Intelligence Surveillance Act (hereinafter FISA) provides for the legal framework for conducting foreign intelligence gathering for national security threats, while maintaining the secrecy of the respective investigations.[140] After the National Security Agency's programs on data collection became public on 2013, the USA Freedom Act of 2015 was enacted in order to set out some limits to the collection of data permitted under the USA PATRIOT Act, prohibiting the bulk collection of US call metadata and telephonic records.[141]

The restrictions to personal data protection for security and defense purposes vary significantly in all the analyzed legal systems, either in terms of the type of restrictions allowed, the requirements to implement them, the extent of those restrictions, or the competent authorities to supervise their implementation.

[138] See the South African National Report, Sect. 4.4.

[139] See the French National Report, Sect. 5.

[140] See the United States of America's National Report, Sect. 5. The federal legislation on intelligence gathering for security and defense purposes has been highly criticized, both at a national level and at an international level. In the recent history of the United States of America, there have been several cases in which the means and methods used by the Government in this context were questioned. The Echelon case, involving authorities of several other countries as data controllers, is one such case, which determined a strong reaction from the European Parliament—see the Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)). More recently, the Prism case has reignited the debate on the topic. It has also resulted in a strong reaction from the European Parliament—see the Report on the US NSA surveillance program, the surveillance bodies of various EU Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in the areas of Justice and Home Affairs (2013/2188(INI)). The *Article 29 Data Protection Working Party* has also issued an opinion on this topic—see the Opinion 04/2014 on the surveillance of electronic communications for intelligence and national security purposes, adopted on 10 April 2014. On this, see Edgar (2017).

[141] See the United States of America's National Report, Sects. 5.1 and 5.2.

hoeren@uni-muenster.de

3.5 Remedies and Sanctions

In the European Union, supervisory authorities have significant corrective powers, including those to issue warnings and reprimands, impose temporary or definitive limitations on processing, and impose administrative fines. These administrative fines may amount to up to 20 million euros or four percent of the annual worldwide turnover of an undertaking in the preceding financial year, whichever is higher.[142]

Data subjects are granted several remedies under the GDPR in case of infringement to their rights. The main ones consist of the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy, either against the supervisory authority or against a third party, such as the data controller or the data processor. Data subjects have the right to receive compensation for damages suffered by any infringement.

Additionally, Member States may set forth national rules for criminal responsibility. The infringer may, thus, be subject to civil liability, criminal and administrative responsibility.

In the United States, the fact that data protection legislation is essentially of a sectoral nature determines that rules on remedies and sanctions, as well as the jurisdiction to enforce them, are equally sectoral in nature. As in Europe, sanctions for infringements of data protection rules in the United States may be administrative, civil or criminal, but the amounts of the applicable penalties are far lower.[143]

Other legal systems included in the scope of this study also have rules on remedies and sanctions for breaching data protection rules, such as the Singaporean legal system.[144]

4 The International Dimension of Data Protection

4.1 The Territorial Scope of Rules on Data Protection

We now turn to the issues raised by the international dimension of personal data protection.

Due to, on the one hand, the global reach of the communications networks through which personal data are currently collected, transmitted, and used—and, hence, the *ubiquitous nature* that their processing typically takes on—and, on the other hand, the different approaches that, as seen in the previous sections, are adopted by several jurisdictions in respect of certain key aspects of their protection, these issues are now of paramount significance.

[142] See the European Union Special Report, Sect. 4.1.

[143] See the United States of America's National Report, Sect. 6.

[144] See the Singaporean Report, Sect. 3.10.

hoeren@uni-muenster.de

One may therefore ask, primarily, how is the territorial scope of application of data protection rules, including those on electronic data processing, defined in the jurisdictions covered by the present study.

In this respect, the GDPR sets out a basic rule in article 3(1), according to which:

> This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

The *place of establishment* of the personal data controller or processor is, thus, the primarily relevant connecting factor to determine the applicability of the Regulation's provisions.

In the abovementioned *Costeja* case,[145] the CJEU has clarified, in respect of the corresponding provision of Directive 95/46, that:

> processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

The processing of personal data through a search engine such as *Google Search*, which was operated by Google Inc. (a company incorporated in the U.S. but with an establishment in Spain, Google Spain SL), was thus deemed to be carried out "in the context of the activities" of that establishment, since the latter was "intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable".[146]

In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned were, as the Court held, "inextricably linked", since the activities relating to the advertising space "constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed".[147]

This broad definition of the notion of establishment of the data controller or processor, which the CJUE has reaffirmed in the *Weltimmo* case,[148] is now reflected in recital 22 of the GDPR, which states that:

> Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

The European approach in respect of the scope of application of personal data protection rules, centered on the *place of establishment* or the domicile of the data

[145] See, *supra,* para 7.3.

[146] See CJEU of 13 May 2014, rendered in case C-131/12, Google Spain SL and Google Inc., ECLI:EU:C:2014:317, para. 56.

[147] See *ibidem*, para. 57.

[148] See the judgment rendered on 1 October 2015 in case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639.

hoeren@uni-muenster.de

controller or processor, instead of the *geographical location* of the personal data at stake, is also to be found in some non-European jurisdictions. Such is the case of Cape Verde,[149] and South Africa.[150]

A more markedly territorial approach, based on the place of processing of the personal data, is preferred by Brazil, which adopts it in its Civil Framework of the Internet ("*Marco Civil da Internet*"),[151] and by Switzerland, where it has been affirmed by the Federal Administrative Court.[152]

4.2 The Applicability of Data Protection Rules to Foreign Entities

A related issue is whether, and to what extent, electronic data processing by entities seated outside a given jurisdiction is comprised in the scope of application of the local rules concerning personal data protection.

Such is the purpose of article 3(2) of the GDPR, which states that:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.

The GDPR hereby seeks to ensure that natural persons who are in the European Union are not deprived of the protection to which they are entitled under the Regulation, when the processing of their personal data is carried out by a controller or processor not established in the Union, if the processing activities are related to the offering goods or services to such persons[153] or to the monitoring of their behavior.[154]

The so-called *market-place principle*, which the previously applicable Directive 95/46/EC did not explicitly enshrine as a criterion for the determination of its spatial scope of application,[155] was thus introduced in the Regulation.[156] By virtue of that principle, European personal data protection rules have gained a certain degree of *extraterritorial applicability.*

[149] See the Cape-Verdean National Report, Sect. 4.1.

[150] See the South-African National Report, Sect. 5.1.

[151] Namely in article 11 thereof, according to which Brazilian law on rights to privacy shall apply to any process of collection, storage, custody or treatment of personal data that occurs in national territory: see the Brazilian National Report, Sect. 4.1.

[152] See the Swiss National Report, Sect. 2.1.

[153] See, on this, recital 23 of the Regulation.

[154] See, on this, recital 24 of the Regulation.

[155] On which see Carrascosa González (2015), pp. 448 ff.

[156] See, in this sense, the German National Report, Sect. 2.7.1.

hoeren@uni-muenster.de

As recital 23 of the Regulation makes it clear, in order to determine whether a controller or processor is offering goods or services to data subjects who are in the Union, one should ascertain whether it is apparent that the controller or processor "envisages offering services to data subjects in one or more Member States in the Union", i.e., that it is *targeting them*.

For this purpose, the recital goes on to say, the *mere accessibility* of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient; instead, "factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union".

In what concerns the issue of whether a processing activity can be considered to "monitor the behavior of data subjects", recital 24 of the Regulation states that one should ascertain whether natural persons are "tracked on the internet". This includes subsequent use of personal data processing techniques such as "profiling a natural person, particularly to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes".

The applicability of domestic rules on data protection to foreign business operators (notably those that process such data in connection with the supply of goods or services to persons located in national territory) is also provided for in article 75 of the Japanese Act on Protection of Personal Information,[157] and in the Singaporean Personal Data Protection Act 2012, which covers, according to section 2(1), companies formed under non-Singapore laws and/or resident outside Singapore.[158]

A particularly difficult issue arises in connection with the applicability of the provisions on the so-called right to be forgotten to search engine service providers established abroad when their listings appear on websites with different domain names: should in those cases the removal of the search results be ordered only in respect of the website identified by a domain name that serves the forum State or should it extend to any other sites?

[157] See the Japanese National Report, Sect. 4.2.

[158] See the Singaporean National Report, Sect. 4.1.

hoeren@uni-muenster.de

This issue motivated a request for a preliminary ruling of the Court of Justice of the European Union from the French *Conseil d'État*,[159] to which the Court replied as follows[160]:

> On a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and of Article 17(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation), where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.

In this landmark judgment, the Court has, in sum, decided that the right to be forgotten does not require search engine operators to de-list search results on a *global basis*, but rather solely within the EU territory.

While acknowledging that the objective of Directive 95/46/EC and the GDPR is to "guarantee a high level of protection of personal data throughout the European Union" (para. 54) and that a de-referencing carried out on all the versions of a search engine "would meet that objective in full" (para. 55), the Court admitted—as this Report shows—that "numerous third States do not recognise the right to de-referencing or have a different approach to that right" (para. 59) and that the right to the protection of personal data is not an absolute right, and must be balanced against other fundamental rights, in accordance with the principle of proportionality (para. 60). Furthermore, the Court stated, "the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world" (*ibidem*).

In particular, the Court noted, it is not apparent from the wording of the Directive or the GDPR that the EU legislature would, for the purposes of ensuring that the said

[159]Case C-507/17, *Google*, OJ C 347, 16.10.2017, p. 22. An opinion was rendered by Advocate General Maciej Szpunar on 10 January 2019 in respect of the issues raised in this request for a preliminary ruling, according to which "the search engine operator is not required, when acceding to a request for de-referencing, to carry out that de-referencing on all the domain names of its search engine in such a way that the links in question no longer appear, irrespective of the location from which the search on the basis of the requesting party's name is performed". Nevertheless, according to the Advocate General "once a right to de-referencing within the EU has been established, the search engine operator must take every measure available to it to ensure full and effective de-referencing within the EU, including by use of the 'geo-blocking' technique, in respect of an IP address deemed to be located in one of the Member States, irrespective of the domain name used by the internet user who performs the search". See, on this, de Miguel Asensio (2019).

[160]Judgment of the Court (Grand Chamber) of 24 September 2019, ECLI:EU:C:2019:772.

hoeren@uni-muenster.de

objective is met, have chosen to confer a scope on the rights enshrined in those provisions which would go beyond the territory of the Member States (para. 62).

From this it follows, according to the Court, that there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject to carry out such a de-referencing on all the versions of its search engine (para. 64).

Nevertheless, the Court added, it is for the search engine operator to take, if necessary, "sufficiently effective measures" to ensure the effective protection of the data subject's fundamental rights (para. 70). Such measures should have the effect of "preventing or seriously discouraging" Internet users in the Member States from accessing the links in question using a search based on that data subject's name (*ibidem*).

4.3 The Specific Conditions Applicable to the Transfer of Personal Data to a Foreign Jurisdiction

Thirdly, one may ask whether the transfer of personal data to a foreign authority is freely allowed or subject to specific conditions and, in the latter case, what they are.

The free flow of data across national borders is, of course, a major concern in a global information society; but the different levels of protection of personal data that still prevail in national legal systems inevitably entail restrictions to their transfer abroad.

The GDPR addresses this issue in chapter V. According to article 45(1), transfer of personal data to a third country or an international organization may, in principle, only take place when the Commission has decided that:

> the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.

When assessing the adequacy of the level of protection in the third country or international organization, the Commission shall, pursuant to article 45(2) of the GDPR, take account in particular of: (1) the rule of law and respect for human rights and fundamental freedoms; (2) the existence and effective functioning of one or more independent supervisory authorities; and (3) the international commitments that the country or organization has entered into in relation to the protection of personal data.

This rule reflects the CJEU's 2015 judgment in the *Schrems* case,[161] in which it held that the notion of an "adequate level of protection" cannot be understood as requiring a level of protection identical to that guaranteed in EU law, but rather as demanding the third country in fact to ensure, by reason of its domestic law or its

[161] On which see CJEU of 6 October 2015, C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650.

hoeren@uni-muenster.de

international commitments, a level of protection of fundamental rights and freedoms that is "*essentially equivalent to that guaranteed within the European Union*".[162]

After having assessed the adequacy of the level of protection, the European Commission may decide, by an implementing act, that a third country, a territory or one or more specified sectors thereof, or an international organization ensures an adequate level of protection (article 45(3)).[163]

A list of the third countries, territories, and specified sectors within third countries and international organizations for which the Commission has decided that an adequate level of protection is or is no longer ensured is to be published in the *Official Journal of the European Union* (article 45(8)).

Absent an adequacy decision, a controller or processor may still transfer personal data to a third country or an international organization, according to article 46 of the GDPR, if it has provided "*appropriate safeguards*", and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards may be provided for, without a specific authorization from a supervisory authority, by: (1) a legally binding and enforceable instrument between public authorities or bodies; (2) binding corporate rules; (3) standard data protection clauses adopted by the Commission; (4) standard data protection clauses adopted by a supervisory authority and approved by the Commission; (5) an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards; or (6) an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In the absence of either an adequacy decision or appropriate safeguards, a transfer of personal data to a third country or an international organization may only occur in one of the cases laid down in article 49 of the GDPR, namely: (1) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers; (2) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; (4) the transfer is necessary for important reasons of public interest; (5) the transfer is necessary for the establishment, exercise or defense of legal claims; (6) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; (7) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation.

[162] See *ibidem*, para. 73.

[163] See, on this, the communication from the Commission to the European Parliament and the Council "Exchanging and Protecting Personal Data in a Globalized World", COM (2017) 7 final, published on 10 January 2017.

hoeren@uni-muenster.de

In the *Schrems* case, Decision 2000/520, adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC, whereby the "*Safe Harbor Privacy Principles*" issued by the U.S. Department of Commerce in 2000 were considered to ensure an adequate level of protection for personal data transferred from the EU to organizations established in the U.S., was held invalid by the CJUE.

Thereafter, a new "*Privacy Shield Framework*",[164] which imposes stronger, self-certified, obligations on American companies, was designed for the transfer of personal data from the EU to the U.S. On July 12, 2016, the European Commission considered that the *Framework* is adequate to enable such data transfers under EU law, which allowed it to enter into force as of 1 August 2016.[165]

Rules similar to those adopted in the EU in respect of the transfer of personal data to third countries have been enacted in Cape-Verde,[166] Japan,[167] Singapore,[168] and South Africa.[169]

4.4 The Law Applicable to Liability for Damages Caused by the Unlawful Processing of Personal Data

Finally, the question should be addressed of what law applies to liability for damages caused by the unlawful processing of personal data in the jurisdictions under analysis in this report.

As the EU Special Report emphasizes, there are no common European conflict of laws rules on this topic, since non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation, are excluded from the scope of application of Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (the "Rome II Regulation") by its article 1(2)(g).[170]

Although the GDPR proclaims in article 82(1) that "[a]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or

[164] Available at https://www.privacyshield.gov.

[165] However, on 3 October 2017 the High Court of Ireland has ruled, in *The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (available at https://www.dataprotection.ie/docimages/documents/Judgement3Oct17.pdf), to make a reference for a preliminary ruling to the CJEU in order to determine, *inter alia,* whether certain features of the *Privacy Shield* constitute an adequate remedy for the protection of the rights to privacy and personal data enshrined in the EU Charter of Fundamental Rights.

[166] See the Cape-Verdean National Report, Sect. 4.3.

[167] See the Japanese National Report, Sect. 4.3.

[168] See the Singaporean National Report, Sect. 4.2.

[169] See the South-African National Report, Sect. 5.2.

[170] See the European Union Special Report, Sect. 4.4.

hoeren@uni-muenster.de

processor for the damage suffered", it is silent on the issue of the law applicable to the ensuing claims.

To be sure, in its Resolution of 10 May 2012 on the amendment of Regulation (EC) No. 864/2007,[171] the European Parliament requested the Commission to submit, on the basis of point (c) of Article 81(2) of the Treaty on the Functioning of the European Union, a proposal designed to add to the Rome II Regulation a provision on the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality, in respect of which it recommended the following text:

> 1. The law applicable to a non-contractual obligation, arising out of a violation of privacy or rights relating to the personality, including defamation, shall be the law of the country in which the most significant element or elements of the loss or damage occur or are likely to occur.
>
> However, the law applicable shall be the law of the country in which the defendant is habitually resident if he or she could not reasonably have foreseen substantial consequences of his or her act occurring in the country designated by paragraph 1.
>
> [. . .].

This recommendation has so far not been enacted. In the EU, the matter is thus left to domestic conflict of laws rules, which differ considerably in this respect.[172]

Although many Civil Law jurisdictions traditionally opt for the applicability of the *lex loci delicti commissi* in respect of tort liability,[173] the issue arises as to where the wrongful act should be held committed whenever—as is often the case in respect of the unlawful processing of personal data through the Internet—the place of the wrongful activity and that of its harmful effect differ.

Portuguese Private International Law[174] provides a solution for this type of situations, according to which:

> If the injurer is considered liable by the law of the State where the injury was inflicted but not by the law of the place where the conduct causing the damage occurred, the former law applies, provided that the injurer should have foreseen the occurrence of an injury in that country as a consequence of his/her act or omission.[175]

[171] Published in the OJEU, C 261, of 10 September 2013, pp. 17 ff.

[172] See, for a comparative analysis, Kuipers (2017), pp. 1350 ff.

[173] Such is the case, *e.g.*, of Greek, Portuguese, and Spanish Private International Law: see, respectively, articles 26, 45(1) and 10(9) of the Civil Codes of those countries.

[174] See article 45(2) of the 1966 Civil Code and, on the applicability of this provision to the situations referred to in the text, Moura Vicente (2005), pp. 307 ff.; Dias Oliveira (2011), pp. 395 ff.; and de Lima Pinheiro (2015), pp. 502 ff.

[175] A similar rule can be found in article 133(2) of the Swiss Private International Law Act 1987, which states: "If the injury occurs in another State than the State, in which the act that caused injury arose, the law of that State shall be applicable if the tortfeasor should have foreseen that the injury would occur there". The same happens with article 17 of the Japanese General Law on the Application of a Law, pursuant to which: "The formation and effect of a claim arising from a tort shall be governed by the law of the place where the result of the wrongful act occurred; provided, however, that if the occurrence of the result at said place was ordinarily unforeseeable, the law of the place where the wrongful act was committed shall govern". See the Japanese National report, Sect. 4.4.

hoeren@uni-muenster.de

Hence, if the data controller or processor has acted in its home country, where its actions were *ex hypothesis* lawful, but should have foreseen the occurrence of an injury to the data subject in a foreign country, as a consequence of the processing of its personal data, *e.g.* because it was offering its goods or services in that country, and this country's law holds the controller or processor liable in tort for the damage thus caused to the data subject, this law shall apply.

Other legal systems, such as the Belgian,[176] German[177] and Italian[178] ones, offer the plaintiff a choice, in what concerns torts committed at a distance, between the law of the place of the harmful event and that where the damage was sustained.

Such a choice is in line with the GDPR's rule on jurisdictional competence contained in article 79(2), which also applies to court proceedings for the exercise of the right to receive compensation by virtue of article 82(6) of the Regulation, according to which:

> Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

A preference for the law of the place of the injury is more openly expressed by several Common Law systems, notably the American and the English ones, which determine its applicability to claims for compensation of personal injury.[179]

---

[176] See article 99, § 2, according to which: "Obligations resulting from a tort are nevertheless governed: 1° in the event of defamation or violation of privacy or personality rights, at the choice of the plaintiff, by the law of the State on the territory of which the act leading to the damage or the damage occurred or is likely to occur, unless the person liable proves that he could not have foreseen the damage to occur in that State [. . .]".

[177] See article 40(1) of the Introductory Act to the German Civil Code, according to which: "Tort claims are governed by the law of the country in which the liable party has acted. The injured party can demand that instead of this law, the law of the country in which the injury occurred is to be applied. The option can be used only in the first instance court until the conclusion of the pre-trial hearing or until the end of the written preliminary procedure".

[178] See article 62(1) of Law of 31 May 1995, section 218, on the Reform of the Italian System of Private International Law, according to which: "The law of the State where the event occurred governs tort liability there for. However, at the request of the injured party, the law of the State where the fact which caused the damage occurred shall apply".

[179] Accordingly the § 146 of the American Restatement 2nd on the Conflict of Laws states that: "In an action for a personal injury, the local law of the state where the injury occurred determines the rights and liabilities of the parties, unless, with respect to the particular issue, some other state has a more significant relationship under the principles stated in § 6 to the occurrence and the parties, in which event the local law of the other state will be applied". Section 11 of the English Private International Law (Miscellaneous Provisions) Act 1995 provides, in turn, that: "(1)The general rule is that the applicable law is the law of the country in which the events constituting the tort or delict in question occur. (2) Where elements of those events occur in different countries, the applicable law under the general rule is to be taken as being (a) for a cause of action in respect of personal injury caused to an individual or death resulting from personal injury, the law of the country where the individual was when he sustained the injury [. . .]".

hoeren@uni-muenster.de

However, the effectiveness of this conflicts rule is somewhat mitigated, on the one hand, by the fact that Common Law jurisdictions may dismiss cases on the basis of the doctrine of *forum non conveniens* if the issues in dispute are subject to a foreign law[180]; and, on the other hand, because the contents of the foreign applicable law are not to be determined *ex officio* by the competent court, but rather pleaded and proven by the party relying on it.[181]

As a result, Common Law jurisdictions will tend to apply more frequently the *lex fori* by default to claims of liability for damages caused by the unlawful processing of personal data. Although this may improve efficiency in international litigation, it may as well, to a certain extent, promote *forum shopping* in respect of such claims.

5 Concluding Remarks

5.1 The Basic Approaches to Regulation of Data Protection in the Internet

In the era of the Internet and of large scale automated processing of information, the protection of personal data has unequivocally become a universal concern.

Although the technological developments occurred in this area over the past four decades have dramatically improved humankind's access to information and knowledge, and opened impressive new perspectives for scientific research and entrepreneurial activities, new and unprecedented risks have also arisen in what regards, for example, the safeguard of informational privacy, off air competition and even—as recent occurrences in Europe and the U.S. with potentially long-lasting effects in public life have shown—of the proper functioning of democratic institutions.

The present report has evidenced that, although these concerns are currently shared by a significant number of countries and supranational organizations, the basic approaches to the regulation of personal data protection still differ widely around the globe.

The major differences identified in the previous sections concern in particular the following areas:

a) The *sources of regulation* of personal data processing, in respect of which the European trend to codify and comprehensively harmonize the law applicable in this field sharply contrasts with the American sector-specific approach to public regulation on data protection, which is largely complemented by self-regulation instruments emanating from the private sector, such as codes of conduct or transparency principles, which enjoy only a limited degree of enforceability;

[180] See Fentiman (2017), pp. 797 ff.

[181] See, for a comparative overview of this matter, see Esplugues et al. (2011).

hoeren@uni-muenster.de

b) The *notion and scope of personal data* covered by the relevant legal sources, which ranges from the very broad concept adopted in European legislation and in several non-European legal systems closely influenced by it, which comprises "any information relating to an identified or identifiable natural person"—the protection of which is regarded as a fundamental, constitutionally protected right—to the much more narrow scope of the personal data that enjoys legal protection currently prevailing in the United States, where data protection rules are primarily aimed at federal agencies;
c) The role and nature of *supervision authorities*, which in the European Union have been entrusted with a wide range of investigative, corrective, authorization and advisory powers, typically concentrated in a single independent public agency, whereas in certain non-European countries such authorities are sometimes put under the control of the executive power (as happens in Singapore and South Africa) or have their attributions dispersed among a number of distinct public agencies, none of which is specifically devoted to data protection (as is the case of the U.S.);
d) The protection specifically awarded to the electronic processing of personal data pertaining to *consumers and workers*, in respect of which the European Union and its Member States have also taken the lead, e.g., through the imposition of strict rules in respect of the collection of data through the use of cookies or other technological devices and the distribution of unsolicited commercial communications, which have no equivalent in the U.S.; and the enactment of special provisions ensuring workers' right to privacy which include, *inter alia,* a general prohibition to use surveillance means at the workplace and to access workers' private electronic communications, in respect of which American law allows a far broader range of exceptions;
e) The enshrinement of the data subject's so-called *right to be forgotten*, which has been recognized in the widest terms by the case-law of the Court of Justice of the European Union (so as to affect also information provided by search engines) and was recently regulated in substantial detail in the GDPR, but which has so far found no acceptance in U.S. federal or state law;
f) The existence of specific *duties to secure personal data* and to *notify data breaches*, which European law now regulates in general terms, but which in other legal systems have been the object of only limited or sector-specific legal provisions;
g) The *exceptions to personal data protection* allowed in respect of criminal investigations, as well as for security and defense purposes, which are considerably more far-reaching in the U.S., particularly in the context of anti-terrorist statutory enactments, than in Europe;
h) The *remedies and sanctions* available for the breach of the applicable personal data protection rules, which, albeit provided for in most legal systems, have recently been considerably aggravated in the European Union, in particular through the power granted to supervisory authorities to impose administrative fines of extremely high values that have no equivalent in other jurisdictions;

hoeren@uni-muenster.de

i) The *territorial scope of application of national rules on personal data protection*, in respect of which the recent European GDPR has made an express option for a mitigated form of extraterritorial applicability—comprising all situations in which the processing of personal data, albeit undertaken by entities not established in the Union, concerns data subjects who are in Europe and takes place in the context of the offering of goods or services to those subjects or in the monitoring of their behavior occurred in the Union—that has no explicit equivalent on the other side of the Atlantic;
j) The conditions applicable to the *transfer of personal data* to foreign jurisdictions, in respect of which the European Union, followed by other countries such as Cape-Verde, Japan, Singapore and South Africa, has established a particular system of control of the adequacy of the level of protection provided by the country of destination as a condition for the lawfulness of such transfer; and
k) The *law applicable to liability for damages* caused by the unlawful processing of personal data in cross-border situations, with regard to which Private International Law rules provide an array of different solutions, even within the European Union, that vary from the (*quasi*) systematic application of the *lex fori* to the optional applicability of the law of the wrongful activity or that of the harmful effect.

5.2 A General Assessment

The comparison conducted above denotes a rather *paradoxical situation*: whilst the Internet is by nature a global computer network and personal data processing conducted through it is largely also a trans-border phenomenon that tends to ignore national frontiers, the regulation of that phenomenon is still—with the notable exception of the European Union—essentially the result of national or even private initiatives.

What's more, the approaches to that regulation differ widely, particularly among the two major Western trading blocks, in what concerns its sources, contents, remedies and scope of application.

The diversity of such approaches does not appear to constitute the mere result of different legislative techniques or historical traditions; it is rather the fruit of deeply-rooted different perceptions of the respective roles of private ordering, the protection of individuals' fundamental rights and the preservation of national security in a market economy.[182]

[182]This was recognized by the Irish High Court in its judgment of 3 October 2017 on *The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (see note 158) where it stated: "A central purpose of the European Union is the promotion of the peace and prosperity of citizens of the European Union through economic and trading activity within the single market and globally. The free transfer of data around the world is now central to economic and social life in the union and elsewhere. The recent history of our continent has shown how

hoeren@uni-muenster.de

The very notion of *privacy*—which, as mentioned above, lies at the root of contemporary rules on individual data protection—is perceived differently in the American and Continental European legal traditions: whilst the former tends to see it essentially as an expression of *individual liberty*, which is primarily threatened by the Government, the latter conceives it basically as a requirement of *personal dignity*, which must be safeguarded above all against the mass media.[183]

As such, the different approaches identified in this study do not seem capable of being easily overcome, as the limited reach of international instruments in this field clearly illustrates.

This is, in reality, a recurring problem in Internet history, which the well-known *UEJF et Licra c. Yahoo! Inc. et Yahoo France* case already illustrated nearly 20 years ago.[184]

Far from being subtracted from State law, the so-called *cyberspace* still reflects the often unsurmountable divergences between national legal systems.

References

Carrascosa González J (2015) The Internet – privacy and rights relating to personality. Recueil des Cours de l'Académie de La Haye de Droit International 378:267 ff.

de Lima Pinheiro L (2015) Direito Internacional Privado, vol II, 4th edn. Almedina Coimbra

de Miguel Asensio P (2015) Derecho Privado de Internet, 5th edn. Madrid

de Miguel Asensio P (2019) Ámbito espacial del derecho al olvido: las conclusiones en el asunto C-507/17, Google. La Ley Unión Europea 67:1

de Vasconcelos Casimiro S (2014) O direito a ser esquecido pelos motores de busca: o Acórdão Costeja. Revista de Direito Intelectual 2:307

Dias Oliveira E (2011) Da responsabilidade civil extracontratual por violação de direitos de personalidade em Direito Internacional Privado. Coimbra

Eberle EJ (2001) The right to information self-determination. Utah Law Rev 965

Edgar TH (2017) Beyond Snowden: privacy, mass surveillance and the struggle to reform the NSA. Washington

Esplugues C, Iglesias JL, Palao G (2011) Application of foreign law. Munich, Sellier

Fentiman R (2017) Forum non conveniens. In: Encyclopedia of private international law, vol 1. Edward Elgar, Cheltenham

crucially important each of these objectives is to the wellbeing of the people of Europe. Damage to the global economy has resulted in very real detriment and hardship to millions of Europeans. International terrorist atrocities have been and continue to be perpetrated in many Member States of the European Union. There are many who experienced the corrosive effects of widespread state surveillance upon their private lives and society in general who regard preservation of the right to privacy, includ[ing] data protection, as fundamental to a democratic society. In a democratic society, a balance must be struck between these competing concerns, interests and values. Not every State will strike the same balance" (see paras. 45–47 of the decision).

[183] See, on this, Whitman (2004).

[184] See the Ordonnance de référé rendered by the Tribunal de Grande Instance de Paris on 22 May 2000, available at http://juriscom.net/2000/05/tgi-paris-refere-22-mai-2000-uejf-et-licra-c-yahoo-inc-et-yahoo-france/.

hoeren@uni-muenster.de

Fried C (1968) Privacy. Yale Law J 77:475
Hoeren T (2018) Internetrecht. De Gruyter, Berlin
Kuipers JJ (2017) Personality rights. In: Encyclopedia of private international law, vol 2. Edward Elgar, Cheltenham
Larenz K, Wolf M (2004) Allgemeiner Teil des Bürgerlichen Rechts, 9th edn. C.H. Beck, Munich
Menezes Cordeiro A (2011) Tratado de Direito Civil, vol IV, Pessoas, 3rd edn
Mota Pinto P (2018) O direito à reserva sobre a intimidade da vida privada. In: eiusdem, Direitos de Personalidade e Direitos Fundamentais. Estudos, Coimbra
Moura Vicente D (2005) Problemática Internacional da Sociedade da Informação. Coimbra
Orrù E (2017) Minimum harm by design: reworking privacy by design to mitigate the risks of surveillance. In: Data protection and privacy: (in) visibilities and infrastructures, Law governance and technology series, vol 36, p 107
Post RC (2001) Three concepts of privacy. Georgetown Law J 89:2087
Prosser WL (1960) Privacy. Calif Law Rev 48:383
Rubenfeld J (1989) Right to privacy. Harv Law Rev 102:737
Sousa Pinheiro A (2015) Privacy e proteção de dados: a construção dogmática do direito à identidade informacional. Lisbon
Strömholm S (1967) Right of privacy and rights of the personality: a comparative survey. Stockholm
van der Sloot B (2017) Legal fundamentalist: is data protection really a fundamental right? In: Data protection and privacy: (in) visibilities and infrastructures, vol 36, Law governance and technology series, p 3
van der Sype YS, Guislan J, Seigneur JM, Titi X (2017) On the road to privacy – and data protection – friendly security technologies in the workplace – a case-study of the MUSES risk and trust analysis engine. In: Data protection and privacy: (in) visibilities and infrastructures, Law governance and technology series, vol 36, p 241
Warren S, Brandeis L (1890) The right to privacy. Harv Law Rev 4:193
Whitman JQ (2004) The two western cultures of privacy: dignity versus liberty. Yale Law J 113:1151

hoeren@uni-muenster.de

Right to Privacy and Personal Data Protection in Brazilian Law

Anderson Schreiber

1 Introduction

Personal data protection is certainly one of the most sensitive challenges faced by contemporary legal science, arising from the extraordinary technological advancement occurred in the last decades. In Brazil, personal data protection arises from the Constitution, which establishes the inviolability of intimacy and private life, in accordance with article 5, item X. Nowadays, both scholars and case law recognize that the right to privacy encompasses not only the protection of individual private life but also the protection of personal data. As a result, personal data can never be seen as an "ownerless information" (*res nullius*) that could be freely collected on the internet. On the contrary, it is a projection of human personality and, as so, requires strong protection from the legal system.

2 General Data Protection Framework in Brazil

2.1 The Applicable Rules

Until the year of 2018, personal data was not solidly protected by Brazilian legislation, being ruled only by sparse laws that were too narrow or generic. For example, article 21 of the Brazilian Civil Code of 2002, which addresses protection of privacy

A. Schreiber (✉)
Rio de Janeiro State University, Rio de Janeiro, Brazil
e-mail: schreiber@sdls.com.br

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_2

hoeren@uni-muenster.de

in general terms,[1] was almost a reproduction of what the Constitution itself provides for, and did not mention the specific problem of personal data protection. The Brazilian Civil Rights Framework for the Internet (Federal Law 12.965/2014) provided for personal data protection as one of its principles in Article 3, item III, but also did not enter into much detail regarding the subject. The Brazilian Consumer Code (Federal Law 8.078/1990) provided for specific rules regarding consumers' data banks in its articles 43 and 44, but did not grant a wide protection to personal data. The *Habeas Data* Law (Federal Law 9.507/1997) provided for a writ for access to information, but dealt more specifically with the procedural rules applicable to that remedy. Additionally, Brazil signed in 2003 the Declaration of Santa Cruz de la Sierra, which encourages personal data protection by its signatory countries.

Due to the notorious insufficiency of these legal provisions, the burden to construct a system of personal data protection in Brazil fell for several years on legal doctrine.[2] Such efforts led to a Bill of Law that was discussed for a long time, finally resulting in the Federal Law 13.079/2018, Brazilian Personal Data Protection Law.

2.2 The Notion of Personal Data

The new Brazilian Personal Data Protection Law recognizes the specific right to personal data protection. Article 5, item I, of this Law defines personal data as "*data related to a natural person identified or identifiable*". The limitation of the protection to *natural person* related data confirms the tight connection between data protection, privacy and human dignity, as advocated by Brazilian legal doctrine.

2.2.1 Sensitive Data

The Brazilian Personal Data Protection Law provides for a special protection of the so-called *sensitive data*, *i.e.* information related to the most intimate aspects of the human person, defined by law as "*personal data concerning racial or ethnic origins, religious beliefs, political opinions, membership of unions or religious, philosophical, and political organizations, data relating to health or sexual life, and genetic or biometric data, when related to a natural person*" (Article 5, item II). The Law conditions the processing of this data to a specific and underlined consent by the holder, linked to specific purposes. Such consent can only be waived in pre-established circumstances listed by the Law, such as when the data is indispensable to "health protection" or to "studies by research institute" (Article 11).

[1] "Article 21. Private life is inviolable, and the judge, at the request of any interested person, will adopt the measures necessary to cease any act contrary to this rule."

[2] Worth to mention the writings of Doneda (2006) and Schertel Mendes (2014).

hoeren@uni-muenster.de

2.2.2 Anonymised Data

The Brazilian Personal Data Protection Law also provides another category of data called *anonymised data*, defined by law as "*data related to an unidentified person, considering the use of reasonable available technical means at the time of its process*" (Article 5, item III). Personal data can become anonymised through data anonymisation, which is described by legislation as "*the use of reasonable available technical means at the time of the processing by which data can no longer be directly or indirectly associated to an individual*" (Article 5, item XI). The Law does not consider anonymised data as personal data, unless it is possible to reverse the data anonymisation (Article 12).

The legislation guarantees the anonymisation of any excessive, unnecessary or inappropriately treated personal data if requested by the holder at any time (Article 18, item IV). Moreover, the Law assures the right to anonymisation on some specific processing, such as studies conducted by research institutes (Article 7, item IV). Anonymisation is also a requirement in case the controller decides to keep personal data after the end of the processing operation (Article 16, item IV).

2.3 Principles of Data Protection

The Brazilian Personal Data Protection Law establishes the following principles on the subject: principles of purpose, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination and accountability (Article 6). In summary, it is required that: (a) data processing always be performed for purposes in accordance with the legal system, (b) that the use of the required data be limited to those purposes, and (c) that the processing is safe and transparent.

2.4 Scope of Protection

The protection of personal data has its scope defined in Article 3 of the Brazilian Personal Data Protection Law, which ensures protection against "*any processing operation carried out by an individual or legal entity of public or private law, independently of the means, the country of its headquarters or the country where the data is located*". It is established that protection against processing of personal data is granted, provided that: (1) processing operations are performed in national territory; (2) treatment activities have the purpose of offering or providing goods or services, or data treatment of individuals located in national territory; (3) the personal data subjected to treatment has been collected in national territory.

Public entities also have a specific applicable law regarding public access to information (Federal Law n° 12.527/2011), which provides guidelines for data

hoeren@uni-muenster.de

storage by entities of Public Administration. The Federal Law n° 12.527/2011 doesn't exclude public entities from following the Brazilian Personal Data Protection Law: both laws are applicable.

2.5 The Supervision Authorities

In 1995, the Brazilian Internet Steering Committee was created with the purpose of coordinating and integrating all internet service initiatives in Brazil. It is composed by representatives from civil society, corporate sector and Federal Government. The mission of the Brazilian Internet Steering Committee involves: proposing policies and procedures regarding the regulation of internet activates and the promotion of studies and technical standards for network and service security in the country. Both of these activities can be generally related to the supervision/controlling of personal data shared on the internet.[3]

In addition, it is important to note that the Brazilian Personal Data Protection Law suffered some vetoes by the Brazilian President. The most significant of them was the veto to (a) the creation of the Personal Data Protection National Authority, a regulatory agency that would have the attribution to assure personal data protection, and (b) the creation of the National Personal Data and Privacy Protection Council, an entity that would be in charge of suggesting data protection policies. Such vetoes were based on alleged unconstitutionality on formal grounds, since the Brazilian Constitution provides that regulatory agencies may only be created by laws proposed by the Federal Government. The law in question was, on the contrary, formally proposed by the National Congress.

In order to solve this legal issue, the president enacted Provisional Measure n° 869/2018, creating both supervisory bodies. The new measure provides attributions almost identical to those of the original Bill of Law. The Personal Data Protection National Authority is responsible not only for monitoring infractions and for applying sanctions, but also for establishing interpretations about data protection legislation, promoting cooperation with national and international authorities, among others (Article 55-J). On the other hand, the National Personal Data and Privacy Protection Council has the power to, for example, provide subsidies for the development of the national policy for personal data and privacy protection, conduct studies and debates about these subjects and prepare annual reports evaluating the implementation of the actions for following the national policy (Article 58-B).

The experience of other countries shows that the autonomy and independence of the supervisory body is essential to personal data protection, because public authorities are often some of the major violators of citizens' privacy. However, the new Brazilian supervisory bodies did not have their full autonomy guaranteed by the

[3]For more information: http://www.cgi.br/about/.

hoeren@uni-muenster.de

Provisional Measure, since the Personal Data Protection National Authority was created as a federal agency integrated to the Office of the President (Article 55-A).

3 Specific Problems Concerning Data Protection in the Internet

3.1 Personal Data Processed by Electronic Means

The Brazilian Personal Data Protection Law can be generally applied for the protection of personal data in the context of services provided at a distance by electronic means. The Brazilian Civil Rights Framework for the Internet (Federal Law n° 12.965/2014) can also be specifically applied in cases involving personal data sharing on the internet. There is also a bill of law (PL n° 281/2012) which deals specifically about the consumer's protection in electronic commerce. This bill of law is currently under examination by the Brazilian Chamber of Deputies (Lower House).[4]

The above-mentioned legislation generally requires previous consent of the data holder to the processing of personal data, including electronic processing. However, in some situations provided in Brazilian law, especially those listed in items II to X of article 7 of the Brazilian Personal Data Protection Law (such as protection of life, physical safety or health), this processing can be done without any consent.

On electronic processing there are no limitations in terms of processing purposes or types of data. On the other hand, in accordance with the Brazilian Civil Rights Framework for Internet (Article 7), personal data shared via internet can only be used for the aims which: (1) justified their collection, (2) are not prohibited by law, and (3) are specified in service agreements or terms of use.

3.2 Protection of Minors' Personal Data

Article 14 of the Brazilian Personal Data Protection Law establishes that the processing of children's and teenagers' personal data must always serve their best interest. The authorization of at least one of the parents or legal guardians of the minor is required if the minor is under 12 years-old, in accordance with Brazilian Statute of the Child and the Adolescent (Federal Law 8.069/1990). Parent's authorization can only be waived if the collection of children's personal data is essential for their own protection or to contact their guardian (Article 14, §3th).

[4]The National Congress is the legislative body of Brazil's federal government. The Brazilian National Congress is bicameral, composed of the Federal Senate (Upper House) and the Chamber of Deputies (Lower House).

hoeren@uni-muenster.de

Moreover, data controllers have some additional obligations when processing children's and teenagers' personal data, such as: (1) keeping public information on the type of data collected, the form of their use and the procedures applied (Article 14, §4th); (2) making all reasonable efforts to verify if the consent has actually been given by the guardian of the child (Article 14, §5th); and (3) adapting information on data processing so its adequate to children's understanding (Article 14, §6th). Lastly, Article 14 prohibits data controllers to condition the participation of children in games, internet applications or other activities to provision of personal information besides the ones strictly necessary.

3.3 *Right to Erase Personal Data* (vs *"Right to Be Forgotten")*

The Brazilian Personal Data Protection Law does not use the expression "right to be forgotten", but does provide for some specific rules regarding the erasure of personal data after the end of its processing. Such right may be exercised when the personal data is no longer necessary or relevant to the achievement of its specific purpose (article 15, item I) or when the consent is revoked by the holder (article 15, item III). These cases, strictly speaking, do not constitute what has been understood as "*right to be forgotten*". The so-called "*right to be forgotten*" should be considered as the right of each human person to stand against oppressive public remembering of certain facts that prevent them from fully developing their personal identity by emphasising to society aspects of their personality that no longer reflect reality.[5] Such right may be exercised, for example, by people who have transitioned from their biological sex and do not want such biological sex to be publicly remembered by newspapers or TV shows. Similarly, former prisoners and former victims of brutal crimes may exercise their right to be forgotten in order to avoid the oppressive public association of their names to the crimes committed, if the remembering of such facts is presenting such people in a way that no longer reflects reality. As occurs in other parts of the world, the right to be forgotten is considered a very subtle and controversial subject in Brazil, which is currently awaiting ruling by the Brazilian Supreme Court.

3.4 *Security Obligations and Data Breach Notifications Concerning Data Processed*

The Brazilian Personal Data Protection Law provides that the data holder must be informed of any security incident that may cause relevant risk or damage to personal

[5] Schreiber (2017), pp. 70–71.

hoeren@uni-muenster.de

data holders and to the national authority. The Law determinates that the notification shall be made in reasonable time and must state details about the incident, for instance the nature of the affected data, risks related to the breach, security measures adopted to protect the data, among others (Article 48).

Legislation provides a relevant role to supervision authorities in cases of security fail. The supervisory board is supposed to verify the severity of the incident, assure data holder rights and determinate measures to allay damages (Article 48, §2nd).

3.5 Data Protection in Electronic Communications Sector

In Brazil, there is no specific legislation regarding the electronic communication sector. Thus, this sector must attend the general rules provided in the Brazilian Civil Rights Framework for the Internet (Federal Law n° 12.965/2014) and in the Brazilian Personal Data Protection Law (Federal Law n° 13.709/2018). Consequently, all the provisions about confidentiality, security measures and obligations in case of a breach of security are also applied to electronic communications.

3.6 Data Protection and Digital Forensics

When it comes to digital forensics, the Brazilian Law provides specific legislation about two main topics: (a) crimes through electronic means and (b) interception of communication data for the purpose of investigation, detection and prosecution of crimes.

Concerning crimes through electronic means, the Brazilian Cybercrimes Law (Federal Law n°12.737/2012) is worth mentioning. This Act typifies crimes such as computing device invasion providing penalties of up to 2 years of detention.

Regarding the interception of communication data for the purpose of the investigation, detection and prosecution of crimes, the relevant legislation is the Federal Law n°9.296/1996. According to this law, interceptions may be determined "*by a judge, ex officio or upon request of: I- the police; and II- the prosecutor*" (Article 3). The Law, however, forbids interceptions when: (1) there is no reasonable indications of authorship or participation in a criminal offence; (2) it is possible to produce probative evidence by other means; and (3) the fact investigated constitutes criminal offence punishable, at most, with a custodial sentence (Article 2).

hoeren@uni-muenster.de

3.7 Data Protection and Electronic Surveillance for Security and Defence Purposes

Currently, in Brazil, there are no specific rules about the electronic processing of personal data for security and national defence purposes. The Brazilian Personal Data Protection Law is not applicable for processing performed for these aims (Article 4, item III). This Law states, nonetheless, that a specific law concerning the processing of personal data for security and national defence purposes will be created (Article 4, §1st).

3.8 Remedies and Sanctions

In Brazil, any breach of an individual's privacy is subject to civil liability under the Brazilian Civil Code. In other words, if an entity or individual uses personal data from another person without consent, this entity or individual must pay compensation for damages, whether moral or material. This remedy is reinforced by the Brazilian Personal Data Protection Law, which imposes joint and several liability between controllers and processors for damages caused by personal data processing (Article 42). The new law does not make it clear whether such liability is based on fault or shall be understood as strict liability. This is one of the main issues that Brazilian legal doctrine is being called to address. The Law also provides administrative penalties to be imposed by the supervision authority (Article 52), such as warnings, fines and elimination of the violated data, among others.

4 International Dimension of Data Protection

4.1 The Territorial Scope of Rules on Data Protection

The Brazilian Data Protection Law is applied to processing operations carried out by any entity provided that: *"I-the processing operation is performed in the national territory; II- the treatment activity has the purpose of offering or providing goods or services, or the treatment of data located in national territory; III- the personal data for data treatment has been collected in Brazil"* (Article 3). In other words, the law is applicable to both national and international entities in the above-mentioned hypotheses, "*independently of the means, the country of its headquarters or the country where the data is located*" (Article 3, *caput*).

Likewise, the Brazilian Civil Rights Framework for the Internet (Federal Law n° 12.965/2014) provides that "a*ny process of collection, storage, custody and treatment of records, personal data or communications by connection providers and*

hoeren@uni-muenster.de

Internet applications providers, in which at least one of these acts occurs in the national territory, shall respect Brazilian law" (Article 11).

4.2 The Specific Conditions Applicable to the Transfer of Personal Data to a Foreign Jurisdiction

The Brazilian Personal Data Protection Law provides specific hypotheses in which international personal data transfers are allowed (Article 33). Some examples of authorized situations are: (1) when the transfer is for countries or international organizations that provide a degree of personal data protection suitable to the provisions of the national legislation; (2) when the holder has provided his specific consent and highlighted the transfer, with prior information on the international character of the operation; or (3) when the transfer is necessary to the execution of public policy or legal attribution of the public service, under the condition of being publicized, among others.

4.3 The Law Applicable to Liability for Damages Caused by the Unlawful Processing of Personal Data

Concerning the law applicable to liability of damages, it is clear that if the damages are caused in Brazil then Brazilian law is applied. Brazilian law, however, does not clarify where damages shall be deemed caused in case of unlawful processing of personal data involving systems located in different jurisdictions. Courts usually apply Brazilian law in these cases whenever the victim is living in Brazil when the damage is caused.

5 Conclusion

The right to privacy was in a sort of hiatus in Brazil. After the promising treatment given by the Constitution of 1988, which established a solid commitment to privacy protection, it ended up being put on hold by the legislator.[6] Meanwhile, the extraordinary technological evolution showed that privacy was under threat. The approval of the Brazilian Personal Data Protection Law in 2018 is good news and emphasises the Brazilian Congress' commitment to carrying out the constitutional project, as well as bringing our country closer to the best international experiences in this matter. Notwithstanding, the creation of an independent agency in charge of personal

[6] Schreiber (2014). p. 186.

hoeren@uni-muenster.de

data protection is urgent. That is the only way to prevent that all efforts applied in the creation of the new law become ineffective in the transformation of Brazilian reality. What we need, after all, is the creation of a true culture of privacy, which may only be achieved if we have independent entities fighting for the protection of personal data.

References

Doneda D (2006) Da Privacidade à Proteção de Dados Pessoais. Renovar, Rio de Janeiro

Schertel Mendes L (2014) Privacidade, Proteção de Dados e Defesa do Consumidor. Editora Saraiva, São Paulo

Schreiber A (2014) Direito à Privacidade no Brasil: avanços e retrocessos em 25 anos de Constituição. In: Clève C (ed) Direitos fundamentais e jurisdição constitucional. Thomson Reuters, São Paulo

Schreiber A (2017) Direito ao Esquecimento. In: Direito Civil: diálogos entre a doutrina e a jurisprudência. Atlas, São Paulo

hoeren@uni-muenster.de

Data Protection and the Internet: Canada

Teresa Scassa

1 General Data Protection Framework in Canada

1.1 Overview

Personal data in Canada is protected by a complex web of laws. The public sector in each province and territory is governed by its own data protection law which is combined with access to information provisions in a single statute.[1] The federal public sector is governed by the *Privacy Act*.[2] Personal health information in the hands of health care 'custodians' is typically the subject of specific legislation in each province or territory.[3] A federal law, the *Personal Information Protection and*

[1]Freedom of Information and Protection of Privacy Act, SA, RSA 2000, c. F-25; Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165; The Freedom of Information and Protection of Privacy Act, SM 1997, c 50; Personal Health Information Privacy and Access Act, SNB 2009, c. P-7.05; Freedom of Information Act, RSN 1990, c F-25; Freedom of Information and Protection of Privacy Act, SNS 1993, c 5; Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31; An Act respecting access to documents held by public bodies and the Protection of personal information, RSQ, c A-2.1; The Freedom of Information and Protection of Privacy Act, SS 1990-1991, c F-22.01; Access to Information and Protection of Privacy Act, SNWT.1994, c 20; Access to Information and Protection of Privacy Act, SNWT 1994, c 20; Access to Information and Protection of Privacy Act, RSY 2002, c 1.

[2]Privacy Act, RSC 1985, c P-21.

[3]See, *e.g.* Personal Health Information Act 2008 SNL c P-7.01; Personal Health Information Protection Act SO 2004, c 3 Sch. A; Health Information Act RSA 2000, c H-5; and Personal Health Information Act CCSM c P33.5; E-Health (Personal Health Information Access and Protection of Privacy) Act, SBC 2008, c 38; Health Information Protection Act, SS 1999 c H-0.021; An Act respecting the sharing of certain health information, SQ 2012, c 23; Personal

T. Scassa (✉)
University of Ottawa, Faculty of Law, Ottawa, ON, Canada
e-mail: tscassa@uottawa.ca

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_3

hoeren@uni-muenster.de

Electronic Documents Act (PIPEDA)[4] addresses the protection of personal information in the hands of private sector organizations. This law applies to all personal information collected, used or disclosed by the federally regulated private sector (*e.g.*, the telecommunications and airline industries) as well as all private sector commercial activity that crosses provincial or national borders. It also applies to any purely intra-provincial collection, use and disclosure of personal information that takes place in a province that has not enacted legislation considered substantially similar to PIPEDA.[5] To date, three provinces have enacted private sector data protection laws that are considered substantially similar. These are Quebec,[6] Alberta,[7] and British Columbia.[8] As a result, personal data collected in the course of commercial activity in each of those provinces is governed by separate provincial legislation. The substantially similar laws of Alberta, BC and Quebec will also apply in some circumstances to non-commercial activities of organizations within those provinces.

PIPEDA is applicable only to personal information that is collected, used and disclosed in the course of *commercial* activity. The patchwork of data protection laws in Canada can lead to somewhat uneven data protection from one province to another. For example, PIPEDA does not apply to political parties in Canada, although B.C.'s *Personal Information Protection Act* applies to political parties in that province.

In addition to specific data protection laws, it is possible to sue for breach of privacy. Such suits are governed by the private law of each province. The *Civil Code of Quebec* provides recourse for breach of privacy rights in that province.[9] In British Columbia, Manitoba, Saskatchewan and Newfoundland specific statutes provide a right of action for breach of privacy.[10] Courts in other provinces have recognized a tort of 'intrusion upon seclusion'.[11] Privacy class action law suits for large scale data breaches have also become more common. These may rely upon causes of action for

Health Information Privacy and Access Act, SNB 2009, c P-7.05; Personal Health Information Act, SNS 2010, c 41; Health Information Act, RSPEI 1988, c H-1.41; Health Information Privacy And Management Act, SY 2013, c 16; Health Information Act, SNWT 2014; Public Health Act, SNu 2016, c 13.

[4]S.C. 2001, c. 5 [PIPEDA].

[5]PIPEDA, s. 26(2)(b).

[6]Act respecting the protection of personal information in the private sector, CQLR c P-39.1.

[7]Personal Information Protection Act, SA 2003, c P-6.5.

[8]Personal Information Protection Act, SBC 2003, c 63.

[9]Civil Code of Québec, CQLR c CCQ-1991, ss. 3, 35–41.

[10]Privacy Act, RSBC 1996, c 373; The Privacy Act, RSM 1987, c P125; The Privacy Act, RSS 1978, c P-24; Privacy Act, RSN 1990, c P-22.

[11]See, *e.g. Jones v. Tsige*, 2012 ONCA 32; *Trout Point Lodge Ltd. v. Handshoe*, 2012 NSSC 245. The threshold for the statutory or common law torts is relatively high. For example, the tort of intrusion upon seclusion requires not only an unjustified intrusion upon someone's seclusion but that it also be of a kind that would be "highly offensive to the reasonable person" (Jones, at para 70).

hoeren@uni-muenster.de

breach of privacy, breach of confidence, negligence, breach of contract or other grounds.

The Quebec *Charter of Human Rights and Freedoms*[12] recognizes a broad right of privacy in that province. The *Canadian Charter of Rights and Freedoms*[13] has been used primarily to provide for privacy rights in the criminal or quasi-criminal contexts. This right is based in section 8, which guarantees a right to be free from unreasonable search and seizure. There has been some discussion in the case law as to whether privacy rights might be implicated in the right to life, liberty and the security of the person in s. 7 of the Charter, although this aspect of privacy jurisprudence is not well developed.[14] The rights under the Canadian Charter are available only with respect to government action. Although the constitutional protection for privacy in Canada tends to be limited to the right to be free from unreasonable search or seizure, Canadian courts have ruled that data protection laws are 'quasi-constitutional' in status.[15] This means that the informational privacy interests they protect must receive a broad interpretation.

1.2 Personal Data

Data protection statutes at the federal and provincial levels use the term "personal information". Each statute contains its own definition, but at the core of each definition is the idea that "personal information" is "information about an identifiable individual". Courts have generally interpreted this to mean that information is personal information if, on its own or when combined with other available information, it can lead to the identification of an individual.[16] The form that the information takes is generally not important. Personal information can be medical or biological data, biometrics, a voiceprint, photographic or video images, data, or other written information.[17]

To qualify as personal information, information must be "about" an individual. Thus it must be capable of being linked to an individual and capable of revealing something about an individual. The Privacy Commissioner of Canada has found, for example, that the selling price of a home is personal information since it can be

[12]Charter of Human Rights and Freedoms, CQLR c C-12.

[13]The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11.

[14]See, *e.g.*; *Cheskes v. Ontario* (Attorney General), 2007 CanLII 38387 (ON SC); *R. v. Hebert*, [1990] 2 S.C.R. 151, and *M. (A). v. Ryan*, [1997] 1 S.C.R. 157.

[15]See, *e.g. Nammo v. TransUnion of Canada Inc.*, 2010 FC 1284; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers*, Local 401, [2013] 3 SCR 733, 2013 SCC 62.

[16]See, *e.g. Gordon v. Canada (Minister of Health)*, 2008 FC 258; *Ontario (Attorney General) v. Pascoe*, (2002) 22 CPR (4th) 447 (Ont CA), aff'g *Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner)* [2001] OJ No 4987, 16 CPR (4th) 460 (OntDiv Ct).

[17]Privacy Commissioner of Canada (2013a) Interpretation Bulletin.

hoeren@uni-muenster.de

linked to the seller and can lead to inferences about their negotiation skills, or the urgency of the sale.[18] The Supreme Court of Canada has ruled that an internet IP address can constitute personal information, as it is capable of revealing a person's internet-based activities.[19]

The protection available to personal information varies depending upon its level of sensitivity. For example, whether consent must be express or can be implied may depend upon the sensitivity of the information at issue.[20] Sensitive information is generally considered to include things such as financial information or health information. However, the Supreme Court of Canada has cautioned that the assessment of sensitivity of information must be contextual.[21] For example, while financial information is generally sensitive, some kinds of financial information may be less so depending on the circumstances.[22] Thus, for example, while a person's income may be financial information and therefore sensitive in nature, in a jurisdiction where the law requires the publication of the salaries of identified public servants, such a person's salary will be considerably less sensitive information.

In addition to sensitivity, new federal guidelines on obtaining meaningful consent to the collection, use and disclosure of personal information under PIPEDA, direct organizations to consider the risk of harm that may flow from the proposed use of personal information. The guidelines indicate that: "Harm should be understood broadly, including material and reputational impacts, restrictions on autonomy, and other factors".[23] The higher the risk of harm, the more necessary is explicit consent.

1.3 Oversight

Oversight of the protection of personal data in Canada tends to follow the jurisdictional lines that define the statutory regimes. The federal Privacy Commissioner has oversight over data protection under both the federal *Privacy Act* and PIPEDA. Each province has an Information and Privacy Commissioner who oversees public sector access to information, protection of privacy, and personal health information

[18]PIPEDA Case Summary #2009-002, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-002/.

[19]*R. v. Spencer*, [2014] 2 SCR 212, 2014 SCC 43.

[20]See, *e.g.* PIPEDA, Schedule I, Clause 4.3.6. New guidelines on consent note that sensitivity can vary depending on the circumstances. See: Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent.

[21]*Royal Bank of Canada v. Trang*, [2016] 2 SCR 412, 2016 SCC 50, at para 36. See also PIPEDA, clause 4.3.4.

[22]See Trang, *Ibid.*, at para 46; *Toronto Real Estate Board v. Commissioner of Competition*, 2017 FCA 236, at para 174.

[23]Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent, "Risk of Harm".

hoeren@uni-muenster.de

protection regimes. Provincial commissioners also oversee provincial private sector data protection laws in the three provinces that have enacted such legislation.

Each data protection statute in Canada provides a complaints mechanism for those who feel that a public sector body, health information custodian, or private sector organization has breached its obligations. Typically the complaints process involves an investigation stage, and commissioners have broad powers to investigate. It is possible for complaints to be resolved between the parties through mediation, but if resolution is not achieved, complaints may proceed to a hearing.

Some provincial commissioners have order-making powers under their enabling legislation which means that a hearing in which a complaint is considered well-founded can lead to a binding order. This is the case in B.C., Alberta and Quebec, where the respective commissioners may make orders that are enforceable at law.[24] The federal Privacy Commissioner, who oversees both the federal public sector's Privacy Act and PIPEDA, has no order making powers and can merely make recommendations regarding compliance.[25] Guidance in combination with audits, investigations and recommendations are all used to achieve soft compliance with legal obligations. The lack of order-making powers has been the subject of considerable criticism, and has led to calls for reform from many, including the former and current privacy commissioners.[26] Those commissioners who do have order-making powers do not have the power to award damages. Their orders are subject to judicial review by the courts.

1.4 Self-Regulation

Canada's federal private sector data protection law, PIPEDA, was built around the *Canadian Standards Association Model Code for the Protection of Personal Information*. This is reproduced in Schedule I of PIPEDA, and provides much of the normative core of the statute. PIPEDA does not preclude the adoption of sectoral codes of practice that can guide organizations within particular sectors in complying with data protection obligations. In fact, in the *2017-2018 Departmental Plan*[27] for the Office of the Privacy Commissioner of Canada, Commissioner Therrien indicated that his office supported the development of sectoral codes.

[24]PIPA (B.C.), ss. 52–53; PIPA (Alberta), ss. 52–54; PPIPS, ss. 55 and 56.

[25]PIPEDA, s. 13.

[26]See, *e.g.* Privacy Commissioner of Canada (2017) Real fears, real solutions, p. 4; Privacy Commissioner of Canada (2013b) The Case for Reforming.

[27]Privacy Commissioner of Canada (2018a) 2017-18 Departmental Plan.

hoeren@uni-muenster.de

2 Personal Data Processed by Electronic Means

Canada has no separate data protection laws to cover the protection of personal data in the online context, nor is there a discrete part of PIPEDA that applies to online activities. Nevertheless, because online activities generally cross provincial or national boundaries, PIPEDA would apply to internet-based commercial activity. There is a growing body of Commissioner Findings that relate to online activities,[28] as well as some case law.[29] The Office of the Privacy Commissioner of Canada (OPC) takes the view that many "free" internet services such as those provided by social networking platforms are engaged in commercial activity.[30]

When PIPEDA took effect in 2001 it did not specifically anticipate digital developments beyond the very early days of electronic commerce. The OPC has issued a considerable number of guidance documents aimed at assisting organizations in complying with their obligations in the digital and mobile contexts. For example, it has provided guidance on good privacy practices for developing mobile apps,[31] and on ways to communicate privacy practices to app users.[32] It has also produced guidelines on online behavioural advertising.[33] More recently, the OPC has been developing new approaches to consent. This process began with a discussion paper,[34] a public consultation, and the issuing of a report on consent.[35] The report has led to the development of *Guidelines for Obtaining Meaningful Consent*.[36] The Guidelines, which are jointly developed with the Privacy Commissioners of British Columbia and Alberta, took effect on January 1, 2019.

Although the *Guidelines for Obtaining Meaningful Consent* are meant to apply to all contexts in which consent is required, they also address online consent. For example, to avoid detail being buried in privacy policies that are never accessed by users, the guidelines specify that for consent to be meaningful, an "organization must

[28]See, *e.g.* PIPEDA Report of Findings #2018-002, "Company's re-use of millions of Canadian Facebook user profiles violated privacy law", https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-002/; PIPEDA Report of Findings #2012-001, "Social networking site for youth, Nexopia, breached Canadian privacy law", https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2012/pipeda-2012-001/; PIPEDA Report of Findings #2018-002, "Company's re-use of millions of Canadian Facebook user profiles violated privacy law", available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-002/.

[29]See, *e.g. A.T. v. Globe24h.com*, 2017 FC 114.

[30]See, *e.g.* PIPEDA Report of Findings #2018-002, at para 12.

[31]Privacy Commissioner of Canada (2012) Seizing Opportunity.

[32]Privacy Commissioner of Canada (2014) Ten Tips for Communicating Privacy Practices to Your App's Users.

[33]Privacy Commissioner of Canada (2011) Guidelines on Privacy and Online Behavioural Advertising.

[34]Privacy Commissioner of Canada (2016) Consent and Privacy.

[35]Privacy Commissioner of Canada (2017) 2016-2017 Annual Report, Report on Consent.

[36]Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent.

hoeren@uni-muenster.de

allow individuals to quickly review key elements impacting their privacy decisions right up front as they are considering using the service or product on offer, making the purchase, or downloading the app, etc."[37] The Guidelines also state that information must be provided in "manageable and easily-accessible ways" that give users some control over the flow of information to them. The Guidelines encourage organizations to "be innovative and creative"[38] in providing notice of collection and in obtaining consent, and suggest using just-in-time notification, interactive tools, and customized mobile interfaces.[39] User-friendly interfaces must be designed with the audience for the particular product or service in mind,[40] and consent should also be part of a "dynamic and ongoing process".[41] In particular, the Guidelines suggest that organizations find ways to periodically remind users about key elements of their privacy policy.

2.1 Children's Privacy

Neither PIPEDA nor any of the three substantially similar provincial private sector data protection laws specifically addresses the privacy rights of minors. The OPC has provided specific guidance for businesses that collect information from children and youth.[42] In its 2017 report on consent it expressed the view that: "in all but exceptional cases, consent for the collection, use and disclosure of personal information of children under the age of 13, must be obtained from their parents or guardians".[43] For minors over the age of 13, the OPC requires organizations to take level of maturity into account in developing consent processes. This position is reflected in the new *Guidelines on Consent*. The issue of children and consent was discussed in the 2018 report of a Parliamentary committee that studied PIPEDA reform. The ETHI committee recommended that the government "consider implementing specific rules of consent for minors, as well as regulations governing the collection, use and disclosure of minors' personal information".[44]

[37]Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent, Clause 1. Additional emphasis on four key elements is prescribed. These elements are: what personal information is collected, with whom the information will be shared, for what purposes the information is collected, used or disclosed, and the risks of harm or other consequences from sharing personal information.

[38]Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent, Clause 4.

[39]Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent, Clause 4.

[40]Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent, Clause 5.

[41]Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent, Clause 6.

[42]Privacy Commissioner of Canada (2015a) Collecting from kids. The topic of consent and children is also addressed in Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent.

[43]Privacy Commissioner of Canada (2017) 2016-2017 Annual Report, Report on Consent.

[44]House of Commons (2018) Towards Privacy by Design, p. 2.

hoeren@uni-muenster.de

2.2 The Right to Be Forgotten

The right to be forgotten (RTBF) raises interesting issues in Canada and its status unclear. In 2018 the OPC took the public position[45] that PIPEDA could be interpreted to provide not just a right of de-indexing but a right of erasure in appropriate circumstances. However, this view has yet to be tested. In *A.T. v. Globe24hr.com*,[46] the Federal Court ordered a Romanian company to remove Canadian court decisions containing the personal information of Canadians from its website. The site operator had been charging fees to anyone seeking to have their information removed. While the outcome sought to protect individuals' reputations and privacy in a manner similar to the RTBF, it is not strictly a RTBF case since the order was premised on a breach of the rules regarding collection, use and disclosure. In RTBF cases, the content at issue may be legitimately posted online and the issue is whether the individual has a right to have it either removed or de-indexed.

On September 27, 2018 the Commissioner announced in the OPC's Annual Report to Parliament that it was referring to Federal Court a complaint raising RTBF issues.[47] This litigation may provide some insight into the extent to which PIPEDA's current provisions support a RTBF.

2.3 Unsolicited Commercial Messages

On July 1, 2014 anti-spam legislation took effect in Canada.[48] The statute, known by the acronym CASL (Canadian anti-spam legislation) amended four federal statutes, including PIPEDA to provide a regime for dealing with unsolicited commercial communications. The regime was further fleshed out with the enactment of the *Electronic Commerce Protection Regulations*.[49] The general purpose of the anti-spam regime is "to encourage the growth of electronic commerce by ensuring confidence and trust in the on-line marketplace".[50] The CASL applies to all

[45]Privacy Commissioner of Canada (2018b) Draft OPC Position on Online Reputation.

[46]2017 FC 114.

[47]Privacy Commissioner of Canada (2018d) Trust but Verify, pp. 13–14.

[48]An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act , S.C. 2010, c. 23. ("Canada's Anti-Spam Legislation" or "CASL"). Note that the law was enacted in 2010, but its coming into effect was delayed in part to ensure that necessary regulations were in place.

[49]SOR/2013-221.

[50]Regulatory Impact Analysis Statement (2013) s. 3.

hoeren@uni-muenster.de

electronic messages[51] that are sent by organizations in the course of "commercial activity". A commercial electronic message is defined in these terms:

> (2) For the purposes of this Act, a commercial electronic message is an electronic message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity [. . .]

The CASL prohibits the sending of unsolicited commercial electronic messages with the consent of the recipient, although consent may be express or implied.[52] In general, express consent requires that individuals be provided with certain information prior to agreeing (orally or through written electronic means). In some cases, express consent may be determined by the conduct of the individual.[53] Consent may only be implied in the circumstances set out in the legislation.[54] These include situations where there is a pre-existing commercial relationship between the parties, or where the person to whom the communication is sent "has conspicuously published, or has caused to be conspicuously published, the electronic address to which the message is sent, the publication is not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at the electronic address and the message is relevant to the person's business, role, functions or duties in a business or official capacity".[55] The legislation establishes a Spam Reporting Centre for individuals to report cases of unsolicited commercial messages. The Canadian Radio-Television Commission, the Competition Bureau and/or the Office of the Privacy Commissioner of Canada are empowered to investigate in appropriate circumstances.

The CASL provides for administrative monetary penalties.[56] Sections 47–51 of the CASL also establish a private right of action for breaches of the CASL. The coming into effect of the right was initially scheduled for July 1, 2017, but it has been indefinitely postponed.

2.4 Employee Personal Information

Employee personal information is treated somewhat differently from other personal information under Canada's private sector data protection laws. PIPEDA applies to

[51] An electronic message is defined as: "a message sent by any means of telecommunication, including a text, sound, voice or image message" CASL, s. 1(1).

[52] CASL, s. 6(1).

[53] CASL, s. 10(8).

[54] CASL, s. 10(9).

[55] CASL, s. 10(9)(b).

[56] CASL, s. 20(1). Penalties for an individual are set at a maximum of $1,000,000 CAD. For an organization, the maximum is $10,000,000 CAD.

hoeren@uni-muenster.de

the personal information of employees in federally regulated industries (such as banking, telecommunications, airlines, etc.). In B.C., Quebec and Alberta, the provincial private sector laws govern the collection, use and disclosure of employee personal information. Employees in the other provinces are not covered by PIPEDA as far as their personal employee information is concerned and have no other statutory protection.

Section 4.01 of PIPEDA provides that the statute does not apply to "business contact information" that an organization "collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession". "Business contact information" is defined to include "the individual's name, position name or title, work address, work telephone number, work fax number or work electronic address".[57] Apart from this exclusion, PIPEDA applies to personal information that "is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business".[58] However, s. 7.3(1) of PIPEDA provides that the collection, use and disclosure of personal employee information can take place without consent if it is "necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual", and the individual has been informed "that the personal information will be or may be collected, used or disclosed for those purposes".

Employee personal information has been interpreted broadly, and includes job performance information,[59] including complaints against an employee.[60] Where video surveillance is carried out in a workplace, video footage may also constitute employee personal information of any employee who is identifiable in the footage.[61] Similarly, GPS location data relating to vehicles driven by employees can constitute employee personal information.[62]

B.C.'s PIPA defines "employee personal information" as "personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal

[57]PIPEDA, s. 2, definition of "business contact information".

[58]PIPEDA, s. 4(1)(b).

[59]PIPEDA Case Summary #2003-198, "Employer accused of wrongful disclosure", https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-198/.

[60]See, *e.g. L'Ecuyer v. Aéroports de Montréal*, 2003 FC 573, aff'd [2004] FCA 237.

[61]*Eastmond v. Canadian Pacific Railway*, 2004 FC 852; PIPEDA Case Summary #2004-264, "Video cameras and swipe cards in the workplace", https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-264/.

[62]PIPEDA Case Summary #2006-351, "Use of personal information collected by Global Positioning System considered", https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-351/.

hoeren@uni-muenster.de

information that is not about an individual's employment".[63] Alberta's PIPA relies upon a similar definition,[64] although it was amended to clarify that employee personal information includes information about a "potential, current or former employee of an organization".[65] Under these statutes, employee personal information may be collected without consent where it is "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual".[66]

The OPC takes the position that an employer's collection of information about an employee from social networking sites amounts to the collection of personal information.[67] However, as noted above, 7.3(1) of PIPEDA permits the collection, use and disclosure of personal employee information without consent if it is "necessary to establish, manage or terminate an employment relationship", and the individual has been informed "that the personal information will be or may be collected, used or disclosed for those purposes". Thus, with appropriate notice, an employer could engage in social media monitoring. Because PIPEDA also applies to applicants for employment, information about prospective employees can be collected from social media sites—with appropriate notice. The OPC advises those employers covered by PIPEDA to have clear policies on social media communications.[68]

2.5 *Data Security Breach Notification*

Data security breach notification requirements were added to PIPEDA in 2015,[69] and took effect on November 1, 2018. The provisions are similar to ones added to Alberta's *Personal Information Protection Act* in 2010. Like the Alberta provisions, PIPEDA's data breach notification requirements set a risk-based threshold for notification. Section 10.1 requires organizations to disclose to the Commissioner any breach of security safeguards for personal information where "it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual". There is also a concurrent obligation for the organization to notify

[63]PIPA (BC), s. 1. Note that some issue may exist as to whether executives can be considered "employees" for the purposes of this legislation. See: Re: Occupational Health and Safety Agency for Healthcare in BC, [2010] B.C.I.P.C.D. No 48, Order No P10-03.

[64]PIPA (Alberta), s. 1(1)(j).

[65]PIPA (Alberta), s. 1(1)(j). Note that the previous definition was interpreted to include information about former employees. See: Re: Clean Harbors Lodging Services, [2010] AIPCD No 57, Order No P2010-011.

[66]PIPA (BC), s. 13(2)(b). A comparable provision can be found in PIPA (Alberta), s. 15(1)(a). Specific provision around the use and disclosure of employee personal information are found in PIPA (BC), ss. 16 and 19; PIPA (Alberta), ss. 18 and 21.

[67]Privacy Commissioner of Canada (2015b) Social Networking in the Workplace.

[68]*Ibid.*

[69]Digital Privacy Act, S.C. 2015, c. 32.

hoeren@uni-muenster.de

affected individuals.[70] Under the Alberta statute, the decision to notify individuals affected by a breach rests with the Commissioner, and not with the organization.[71]

PIPEDA's data breach notification provisions also require organizations to keep a record of every breach of security safeguards—regardless of the degree of risk to individuals. Such records must be made available to the Commissioner on request.[72] Although the obligation is to make information available to the Commissioner, rather than to the public, such records might be capable of being subpoenaed, for example, in cases where there is litigation relating to a data security breach. The data breach notification regulations limit the retention period for such information to two years.[73]

3 Data Protection in the Electronic Communications Sector

Because of the interprovincial and cross-border nature of electronic communications, PIPEDA is the applicable statute. The Privacy Commissioner of Canada has taken the position that Internet Protocol addresses (IP addresses) are personal information so long as they can be linked to an identifiable individual.[74] Electronic communications providers are subject to the same rules as all other organizations under PIPEDA, including the data breach notification requirement provisions.

4 Data Protection and Digital Forensics

PIPEDA and the equivalent provincial private sector data protection laws generally permit the disclosure of personal information without consent when it comes to the investigation, detection and prosecution of crimes. In fact, the legislation is worded broadly enough to include not just crimes, but also "the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law".[75] There is also an exception to the requirement of consent to disclosure of personal information where "disclosure is requested for the purpose of *administering* any law of Canada or a province".[76]

[70] PIPEDA, s. 10.1(3).

[71] PIPA (Alberta), s.37.1(1).

[72] PIPEDA, s. 10.3.

[73] Breach of Security Safeguards Regulations, SOR/2018-64, s. 6.

[74] Privacy Commissioner of Canada (2013a) Interpretation Bulletin.

[75] PIPEDA, s. 7(3)(c.1)(ii).

[76] PIPEDA, s. 7(3)(c.1)(iii).

hoeren@uni-muenster.de

In 2014 a new provision was added to the *Criminal Code* which permits organizations to voluntarily preserve data or to provide it to police so long as they are not prohibited by law from doing so:

> **487.0195** (1) For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving *or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.*
>
> *(2) A person who preserves data or provides a document in those circumstances does not incur any criminal or civil liability for doing so.*[77] [Emphasis added]

As a result, organizations are immunized from civil suit for voluntary disclosures of personal information to law enforcement officials so long as they are not prohibited by law from making these disclosures.

PIPEDA's paragraph 7(3)(*c.1*), which permits the disclosure of personal information without consent to law enforcement and national security authorities, has been the subject of considerable debate and litigation. Any disclosure by an organization under s. 7(3)(c.1) is voluntary—the organization may decline to share the information. In such a case, the agency seeking the information would have to obtain a court order to compel its disclosure.

Reliance by police upon the permissive disclosure provisions of paragraph 7(3)(*c.1*) created uncertainty about the constitutionality of such requests. In particular, issues arose around police requests to telecommunications service providers to link IP addresses with customer name and address information. In *R. v. Spencer*[78] the unanimous Supreme Court of Canada ruled that police requests for such information without a court order violated an accused's constitutional right to be free from unreasonable search and seizure.

The Court also held that the provisions of both PIPEDA and the *Criminal Code* that permit companies to voluntarily disclose personal information to law enforcement officials at their request do not displace any reasonable expectation of privacy. One of the requirements of paragraph 7(3)(*c.1*) of PIPEDA is that police have a *lawful authority* to obtain the information sought. If the information sought is of a kind that triggers a reasonable expectation of privacy, then a warrant is necessary in order to lawfully obtain it. If the circumstances require a warrant, then a request made without a warrant is without lawful authority.

Nevertheless, *Spencer* leaves a considerable grey area when it comes to the voluntary disclosure of personal information by organizations. The Supreme Court of Canada accepted that the reasonableness of a person's expectation of privacy in their ISP subscriber information may depend upon the wording of their ISP's Terms of Service and privacy policy. In other words, if the company's privacy policy states that the organization may hand over customer data to police upon request, the reasonableness of a customer's expectation of privacy in this information would

[77] Protecting Canadians from Online Crime Act, S.C. 2014, c. 31.

[78] *R. v. Spencer*, [2014] 2 SCR 212, 2014 SCC 43.

hoeren@uni-muenster.de

be considerably diminished.[79] This is a troubling result given that most privacy policies and terms of service for telecommunications services are effectively contracts of adhesion.

In addition, *Spencer* addressed only one kind of customer data. The lack of certainty over what customer information attracts a reasonable expectation of privacy—and in what circumstances—means that different organizations may respond to law enforcement requests in different ways, leaving individuals "in the dark about when their personal information may be disclosed to state authorities without their consent or prior judicial authorization".[80]

Under pressure from civil society groups, and as a result of voluntary disclosures made by Telco's in the United States, Canadian Telco's began to make voluntary disclosures in 2013 and 2014 regarding the number of requests they had received from police and their responses to these requests. In 2015, the federal Department of Industry released Voluntary Reporting Guidelines[81] to provide guidance to organizations that chose to report on their disclosures of customer information in response to requests from state authorities. The guidelines, which seek to balance the need for transparency with the public interest in law enforcement and national security,[82] have been welcomed by the OPC as a "good first step".[83]

As noted earlier, where there is a reasonable expectation of privacy in data or information, prior judicial authorization is generally required before law enforcement can rely upon it. The Criminal Code details the different types of warrants that are available depending upon the nature of the information sought. It uses two different judicial standards: reasonable grounds to believe and reasonable grounds to suspect. The former standard is typically applied to information in which there is a higher expectation of privacy.

Under the *Criminal Code*, a court may require those in possession of data hosted on a computer system to preserve it,[84] or to provide it to law enforcement officials.[85] Preservation orders are available where there are "reasonable grounds to suspect" that an offence has been or will be committed. Production orders are also available for data,[86] the tracing of specific communications,[87] or for transmission data.[88] A production order is available for data and documents where there are "reasonable grounds to believe" that an offence has or will be committed. However, a production

[79]See discussion by Penney (2014).

[80]Privacy Commissioner of Canada (2015c) Submission to Standing Committee on Industry.

[81]Innovation, Science and Economic Development Canada (2015) Transparency Reporting Guidelines.

[82]*Ibid.*

[83]*Ibid.* at 3.

[84]Criminal Code, RSC 1985, c C-46, s. 487.013.

[85]Criminal Code, s. 487.014.

[86]Criminal Code, s. 487.014.

[87]Criminal Code, s. 487.015.

[88]Criminal Code, s. 487.016.

hoeren@uni-muenster.de

order for the tracing of communications or for transmission data is available on a "reasonable grounds to suspect" basis. Police may also seek production orders for tracking data,[89] or financial data[90] on a 'reasonable grounds to suspect' basis. A judge may impose any conditions considered appropriate on any of these production orders.[91] A judge may also prohibit the person against whom such an order is made from disclosing the existence, or some or all of the contents of any such order for a period of time specified in the order.[92] Although the *Criminal Code* provides for such orders to be made on an *ex parte* basis, the entity that is ordered to produce data or documents is entitled to ask a court to review, revoke or vary the order within 30 days of its making.[93]

Any data retained by organizations as a result of preservation demands or orders, or production orders, must be destroyed at the expiration of the order if such data would not otherwise be retained in the normal course of business.[94] However, it should be noted that these provisions regarding the destruction of data relate only to the copies preserved by the organizations. Police who obtain data under production orders or warrants are not subject to any specific legislative requirements regarding the retention, destruction, or secure storage of this data.[95]

Warrants are available for the interception of private communications, although the threshold for such warrants is relatively high.[96] It is otherwise an offence to intercept private communications. However, the evolution of contemporary communications technology has eroded the robustness of these protections. The Supreme Court of Canada has found, for example, that accessing historical text message records is not an interception of private communications. In *R. v. Jones*,[97] the majority of the Court noted that the stringent warrant requirements for interception were crafted in light of the potential that police might proactively intercept communications in the hope of detecting criminal conduct.[98] However, according to the majority, once communications have taken place, as is the case with historical text messages, the same privacy concerns are not at play. The majority reached this conclusion in spite of the fact that the production order at issue included text messages sent or received on the date of the authorization.

Warrants for the installation of tracking devices on vehicles or other 'things' are available on a "reasonable grounds to suspect" standard.[99] A warrant to track an

[89]Criminal Code, s. 487.017.
[90]Criminal Code, s. 487.018.
[91]Criminal Code, s. 487.019.
[92]Criminal Code, s. 487.0191.
[93]Criminal Code, s. 487.0193.
[94]Criminal Code, s. 487.0194.
[95]This lack of guidance was criticized in *R. v. Rogers Communication* 2016 ONSC 70.
[96]Criminal Code, ss. 185, 186.
[97][2017] SCJ No 60, 2017 SCC 60 [Jones].
[98]Jones, *ibid.* at para 74.
[99]Criminal Code, s. 492.1(1).

hoeren@uni-muenster.de

individual "by identifying the location of a thing that is usually carried or worn by the individual" is available on the more stringent "reasonable grounds to believe" standard.[100]

In addition to these law enforcement provisions, amendments to PIPEDA in 2015 permit information sharing between private sector organizations where it is "reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation".[101] A further exception deals with information sharing between organizations that is related to "detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud".

5 Data Protection and Electronic Surveillance for Security and Defence Purposes

The collection, use, retention and disclosure of information by the Canadian Security Intelligence Service in relation to national security are governed by the *Canadian Security Intelligence Service Act.*[102] As with criminal investigations, prior judicial authorization is required for investigations that impact a reasonable expectation of privacy. The *CSIS Act* provides for warrants on a "reasonable grounds to believe" standard.[103] The system is one in which oversight is "front-ended"[104] meaning that authorization is required in advance of information collection. Bill C-59, before the Senate at the time of writing, would overhaul the security intelligence system, creating, among other things, new powers for bulk surveillance combined with new oversight mechanisms. The Bill would permit the creation of some bulk data sets with judicial authorization; there are also "judicial controls on retention, exploitation and querying of at least some sorts of information".[105]

The Communications Security Establishment (CSE) which is established by the *National Defence Act*,[106] has intelligence gathering functions although, unlike CSIS, these are aimed outside of the country. The CSE has engaged in bulk metadata collection, which has raised concerns about breach of privacy under the *Canadian*

[100]Criminal Code, s. 492.1(2).
[101]PIPEDA, s. 7(3)(d.1).
[102]RSC 1985, c C-23 [*CSIS Act*].
[103]CSIS Act, s. 21.1(2).
[104]Forcese (2018), p. 3.
[105]Forcese (2018), p. 4.
[106]RSC 1985, c. N-5.

hoeren@uni-muenster.de

Charter of Rights and Freedoms.[107] Bill C-59 would provide additional safeguards with a new system requiring pre-authorization for bulk data collection. However, C-59 will permit the collection of "publicly available" information without authorization, and critics have suggested that the definition of "publicly available" is overly broad.[108] The definition reads:

> "publicly available information" means information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase. It does not include information in respect of which a Canadian or a person in Canada has a reasonable expectation of privacy.[109]

Not only is the definition exceptionally broad, its boundaries are blurred by the fact that it excludes information in relation to which there is a "reasonable expectation of privacy". The existence or reasonableness of an expectation of privacy is often a matter of debate.

Specific criminal activities that may have international and/or organized crime dimensions are governed by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.[110] This statute provides for some information sharing by financial services providers with law enforcement and national security officials.

6 Remedies and Sanctions

PIPEDA's enforcement is largely based upon a soft-compliance ombuds model. For example, the Commissioner has the power to audit the personal information handling practices of an organization if he has reasonable grounds to believe that the organization is not complying with its obligations under PIPEDA. An audit results in a report of findings and recommendations that may be included in the Commissioner's annual report to Parliament.[111]

A person who feels their rights have been breached under PIPEDA can file a complaint with the Privacy Commissioner of Canada.[112] The complaint may lead to an investigation and ultimately to the issuing of a non-binding report by the Privacy Commissioner.[113] If the complaint is considered well-founded, the report will also include recommendations for changes to the organization's practices. Once a report has been issued, a complainant may file an application with the Federal Court of

[107] Austin (2015), p. 107; Forcese (2015).

[108] Forcese (2018), p. 8.

[109] Bill C-59, An Act respecting national security matters, 41st Parl., 1st Sess., Part 3, Communications Security Establishment, s. 2.

[110] SC 2000, c 17.

[111] PIPEDA s. 19.

[112] PIPEDA, s. 11.

[113] PIPEDA, ss. 12, 13.

hoeren@uni-muenster.de

Canada.[114] The Commissioner also has the authority to send a matter on to the Federal Court.[115] Such a proceeding may take into account the Commissioner's report and its conclusions, but it is a *de novo* hearing and the Court is not bound by either the record before the Commissioner or his report. The Federal Court can issue binding orders and can award damages.[116] The Court has taken a very conservative approach to moral damages under PIPEDA, ruling that such damages are only available in "egregious" circumstances.[117] Where damages have been awarded, they have tended to be very low. As a consequence, such applications are almost always brought by unrepresented applicants who may struggle to adduce appropriate evidence of actual and/or moral damage. Under the provincial equivalents to PIPEDA in B.C., Alberta and Quebec, the Commissioners may issue binding orders, but they do not have the power to award damages.

Both the current and former Privacy Commissioners are on record for criticizing the weak enforcement provisions of PIPEDA and have called for a reform of the legislation that would include order-making powers and other enforcement mechanisms. A recent review by a House of Commons Standing Committee also recommended enhanced Commissioner's powers.[118]

In 2015 PIPEDA was amended by the *Digital Privacy Act* to include a new power of the Commissioner to enter into compliance agreements where he has reasonable grounds to believe "that an organization has committed, is about to commit or is likely to commit an act or omission" that could amount to a breach of PIPEDA.[119] Where a compliance agreement is entered into and the organization complies with it, the Commissioner will not apply to the Federal Court for an order, and any application by the Commissioner to the Federal Court for a compliance order is put in abeyance.[120] If there is non-compliance with the agreement, the possibility of seeking an order before the Federal Court is revived.[121]

PIPEDA provides for the levying of fines against any organization who destroys data or documents relevant to a complaint under the statute, who retaliates against a whistleblower under the Act, or who obstructs the investigation of a complaint. Fines are fairly modest with the maximum on an offence punishable on summary conviction being $10,000 and for offences by indictment $100,000.[122] Fines can only be imposed by a court, and they are not available as a sanction for breaches of data protection obligations. There have been calls for the Commissioner to have broader

[114]PIPEDA, s. 14.

[115]PIPEDA, s. 15.

[116]PIPEDA, s. 16.

[117]See, *e.g. Randall v. Nubodys Fitness Centres*, 2010 FC 681 (CanLII).

[118]House of Commons (2018) Report of the Standing Committee on Access to Information, Privacy and Ethics.

[119]PIPEDA, s. 17.1.

[120]PIPEDA, s. 17.1(3).

[121]PIPEDA, s. 17.2(2).

[122]PIPEDA, s. 28.

hoeren@uni-muenster.de

authority to levy fines and for such fines to be adapted to the size and revenues of transgressing organizations.

7 Private International Law Rules

In *Lawson v. Accusearch Inc*.,[123] the Federal Court of Canada ruled that PIPEDA applied to the collection, use and disclosure of the personal information of Canadians by a U.S.-based company. The Court found that "PIPEDA gives the Privacy Commissioner jurisdiction to investigate complaints relating to the transborder flow of personal information".[124] This jurisdiction exists so long as there is a sufficient connection to Canada. Since then, the Commissioner has investigated numerous complaints relating to offshore companies, including social media platforms. In deciding on whether to investigate a foreign company, the Commissioner will take into account factors such as the : "location in which the activity takes place; location to which profits flow; location of preparatory activities; residency of parties involved; location of contract; location of any potential related proceedings; jurisdiction where promotional efforts primarily targeted; location of content provider; location of host server; location of intermediaries; location of the end user".[125]

Although the Commissioner may investigate complaints into the activities of offshore companies, he does not have the power to compel companies outside Canada to disclose records or to submit to on-site investigations. In many cases, the Commissioner has relied upon the voluntary co-operation of such companies. In a few instances, the Commissioner has also worked with the data protection authorities in the country where the organization is located. The Commissioner has no extraterritorial enforcement powers. However, in some instances, offshore companies have responded positively to the Commissioner's recommendations. It is also possible to seek an order from the Federal Court, as was done in *A.T. v. Globe24hr.com*.[126] Where such an order issues, its enforcement must be sought in the foreign jurisdiction or it will largely be without effect.

PIPEDA permits organizations to transfer personal information to an organization in another country for processing, but holds these organizations accountable. According to Clause 4.1.3 of Schedule I of PIPEDA, an organization must provide a level of protection to the information that is comparable to what it offers under its own privacy policies. This is principally done through contractual arrangements with the offshore processor. In its 2009 *Guidelines for Processing Personal Data Across*

[123] *Lawson v. Accusearch Inc.*, [2007] 4 FCR 314, 2007 FC 125.

[124] *Ibid*. at para 51.

[125] *Ibid.* at para 42.

[126] See, *e.g.* PIPEDA Report of Findings #2018-002, at para 12.

hoeren@uni-muenster.de

Borders,[127] the OPC noted the obligation of organizations to be transparent with their customers about their data handling practices. If data is to be transferred offshore for processing, customers should be notified of this. The Guidelines also state that customers should be warned that "while the information is in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities".[128]

Concerns over the potential for foreign governments to access the personal information of Canadians in the hands of offshore companies to which data has been transferred for processing by Canadian companies were heightened by the enactment of the USA Patriot Act[129] in 2001. To date, two provincial governments in Canada have amended their public sector data protection laws to prohibit the transfer or storage outside of Canada of Canadians' personal information in the hands of the public sector entities governed by those statutes.[130]

References

Statutes and Regulations

Access to Information and Protection of Privacy Act, SNWT.1994, c 20
Access to Information and Protection of Privacy Act, SNWT 1994, c 20
Access to Information and Protection of Privacy Act, RSY 2002, c 1
An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act , S.C. 2010, c 23
An Act respecting access to documents held by public bodies and the Protection of personal information, RSQ,c A-2.1
Act respecting the protection of personal information in the private sector, CQLR c P-39.1
An Act respecting the sharing of certain health information, SQ 2012, c 23
Bill C-59, An Act respecting national security matters, 41st Parl., 1st Sess
Breach of Security Safeguards Regulations, SOR/2018-64
Canadian Security Intelligence Service Act, RSC 1985, c C-23
Charter of Human Rights and Freedoms, CQLR c C-12

[127]Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, January 2009, available at: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/.

[128]*Ibid.*

[129]Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001, Pub L 107-56.

[130]In British Columbia, s. 30.1 of the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, prohibits transfers or storage outside of the country except in specified circumstances. In Nova Scotia, the *Personal Information International Disclosure Protection Act*, SNS 2006, c 3, performs a similar function.

hoeren@uni-muenster.de

Civil Code of Québec, CQLR c CCQ-1991
Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11
Criminal Code, RSC 1985, c C-46
Digital Privacy Act, S.C. 2015, c. 32
E-Health (Personal Health Information Access and Protection of Privacy) Act, SBC 2008, c 38
Electronic Commerce Protection Regulations, SOR/2013-221
Freedom of Information and Protection of Privacy Act, SA, RSA 2000, c. F-25
Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165
Freedom of Information and Protection of Privacy Act, SM 1997, c 50
Freedom of Information Act, RSN 1990, c F-25
Freedom of Information and Protection of Privacy Act, SNS 1993, c 5
Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31
Freedom of Information and Protection of Privacy Act, SS 1990-1991, c F-22.01
Health Information Act, RSA 2000, c H-5
Health Information Act, RSPEI 1988, c H-1.41
Health Information Act, SNWT 2014
Health Information Privacy and Management Act, SY 2013, c 16
Health Information Protection Act, SS 1999 c H-0.021
Personal Health Information Act, 2008 SNL c P-7.01
Personal Health Information Act, SNS 2010, c 41
Personal Health Information Protection Act, SO 2004, c 3 Sch. A
Personal Health Information Act, CCSM c P33.5
Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05
Personal Health Information Privacy and Access Act, SNB 2009, c. P-7.05
Personal Information and Electronic Documents Act, S.C. 2001, c. 5
Personal Information International Disclosure Protection Act, SNS 2006, c 3
Personal Information Protection Act, SA 2003, c P-6.5
Personal Information Protection Act, SBC 2003, c 63
Privacy Act, RSC 1985, c P-21
Privacy Act, RSBC 1996, c 373
Privacy Act, RSM 1987, c P125
Privacy Act, RSS 1978, c P-24
Privacy Act, RSN 1990, c P-22
Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c 17
Protecting Canadians from Online Crime Act, S.C. 2014, c. 31
Public Health Act, SNu 2016, c 13
Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001, Pub L 107-56

Secondary Materials

Austin LM (2015) Lawful illegality: what Snowden has taught us about the legal infrastructure of the surveillance state. In: Geist M (ed) Law, privacy and surveillance in Canada in the post-Snowden era. University of Ottawa Press, Ottawa, pp 103–126
Forcese C (2015) Law, logarithms, and liberties: legal issues arising from CSE's metadata collection initiatives. In: Geist M (ed) Law, privacy and surveillance in Canada in the post-Snowden era. University of Ottawa Press, Ottawa, pp 127–162
Forcese C (2018) Bill C-59 and the judicialization of intelligence collection, Ottawa Faculty of Law Working Paper No. 2018-13. Available via SSRN. https://ssrn.com/abstract=3157921

hoeren@uni-muenster.de

House of Commons (2018) Towards privacy by design: review of the personal information protection and electronic documents act, Report of the Standing Committee on Access to Information, Privacy and Ethics. http://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf

Innovation, Science and Economic Development Canada (2015) Transparency reporting guidelines, June 30, 2015. http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html

Penney S (2014) The digitization of Section 8 of the Charter: reform or revolution? SCLR (2d) 67:505–534

Privacy Commissioner of Canada (2009) Guidelines for processing personal data across borders. https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/

Privacy Commissioner of Canada (2011) Guidelines on privacy and online behavioural advertising. https://www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/gl_ba_1112/

Privacy Commissioner of Canada (2012) Seizing opportunity: good privacy practices for developing mobile apps. https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210/

Privacy Commissioner of Canada (2013a) Interpretation bulletin: personal information. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/

Privacy Commissioner of Canada (2013b) The case for reforming the personal information protection and electronic documents act. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/pipeda_r/pipeda_r_201305/

Privacy Commissioner of Canada (2014) Ten tips for communicating privacy practices to your app's users. https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/02_05_d_61_tips/

Privacy Commissioner of Canada (2015a) Collecting from kids? Ten tips for services aimed at children and youth. https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/02_05_d_62_tips/

Privacy Commissioner of Canada (2015b) Social networking in the workplace. https://www.priv.gc.ca/en/privacy-topics/privacy-at-work/02_05_d_41_sn/

Privacy Commissioner of Canada (2015c) Submission to Standing Committee on Industry, Science and Technology, February 17, 2015. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_20150217/

Privacy Commissioner of Canada (2016) Consent and privacy. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

Privacy Commissioner of Canada (2017) Real fears, real solutions: a plan for restoring confidence in Canada's privacy regime: Annual Report 2016-2017. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/

Privacy Commissioner of Canada (2018a) 2017-18 Departmental Plan. https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2017-2018/dp_2017-18/

Privacy Commissioner of Canada (2018b) Draft OPC position on online reputation. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/

Privacy Commissioner of Canada (2018c) Guidelines for obtaining meaningful consent. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

Privacy Commissioner of Canada (2018d) Trust but verify: rebuilding trust in the digital economy through independent, effective oversight, 2017-18 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201718/ar_201718/

Regulatory Impact Analysis Statement (2013) Available via Canada Gazette. http://www.gazette.gc.ca/rp-pr/p1/2013/2013-01-05/html/reg1-eng.html#1

hoeren@uni-muenster.de

Data Protection in the Internet: Cape Verde's National Report

José Pina-Delgado

1 Introduction

1.1 Organisation of the Report

Despite being the first African state to have a General Law on Data Protection[1]—largely borrowed, as duly recognised by its promoters,[2] from the Portuguese Data Protection Act of 1998,[3] which, in turn, implemented the European Union Data Protection Directive of 1995[4]—Cape Verde is in the process of developing a broad and robust system of personal data protection. Though enacted in 2001, the Cape Verdean Law, in the majority of cases, was not really in action,[5] but only represented

[1] See Makulilo (2012), p. 163.

[2] The Minister of Justice that presented the draft legislation on behalf of the Executive in the Parliament mentioned the 1995 Directive and a model law for Latin American Countries (Parliamentary Records (2000), 30.11.2000 (audio version) (on file with author)).

[3] See Law No 67/98, of 6 October, published in the Portuguese Official Gazette, *Diário da República*, I Série A, n. 247, 26.10.1998, and, for general comments, Sarmento e Costa (2005), Pinheiro (2015), and, in English, Oliveira e Costa (2012).

[4] See Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal data and on the Free Movement of such Data, *Official Journal of the European Communities*, No L 281/31, 23.11.1995.

[5] When Parliament discussed amendments to the Law this was duly acknowledged by their sponsors and other members of Parliament (Parliamentary Records (audio), 27.07.2013 (Afternoon Period) (on file with author)).

J. Pina-Delgado (✉)
Instituto Superior de Ciências Jurídicas & Sociais of Praia, Praia, Cape Verde

Constitutional Court of the Republic of Cape Verde, Praia, Cape Verde
e-mail: jose.p.delgado@tconstitucional.cv

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_4

hoeren@uni-muenster.de

in the books.[6] So the System started out slowly, providing a certain amount of leeway within its boundaries, but in the last couple of years has picked up pace and is progressing with increasing speed.

Cape Verde is a relatively young country that only achieved independence from Portugal in 1975,[7] a factor that could provide an explanation for the relative unease, from a technical point of view, caused by topics such as data protection and information technology. First of all, there were more important priorities in the construction of the legal order during the initial decades of the country's independence, so the creation of legal solutions relied specifically on the gradual substitution of Portuguese colonial legislation with laws that related specifically to Cape Verde. This was true even in the cases that relied heavily in recent legislation of the former colonial power,[8] which, specifically in the field of data protection, is justified by history and the fact that most Cape Verdean lawyers involved in legislative decision-making, legal consulting and the field of legal practice and application (judges, commissioners, attorneys, etc.) had their legal training in Portugal,[9] but also because of a certain lack of autonomy and of some audaciousness of local scholars and practitioners in thinking outside the box; second, the lack of legal expertise in technologically related law is also a persistent problem that affects developing countries[10] and which is only very slowly being overcome; furthermore, as is the case in many tiny societies, one cannot say that, differently from other constitutional values as freedom and even human dignity,[11] a culture of strong and comprehensive privacy is congenital to the Cape Verdean *ethos*,[12] which is an important factor because despite the understanding of privacy[13] having, at its core, some universal and shared human traits and necessities,[14] its specific manifestations are contextual,[15] which determines the broadness of its defence in a political community.

From a symbolic point of view the first Liberal Democratic Constitution of the country, adopted in 1992 after 15 years of a one-party system,[16] presented privacy as

[6]For general presentations and some background, Almeida (2004), pp. 229–268; Traça and Embry (2011), pp. 249–255; Pinheiro (2015), pp. 563–566; Traça and Gaspar (2016), pp. 249–258; Cham (2017), pp. 87–90.

[7]In the English language literature, see Lobban Jr (1995).

[8]See the evaluation of Bogdan (2000).

[9]As stressed recently by Traça and Gaspar (2016), p. 253.

[10]UNTACD (2012), p. 9.

[11]See the decision to the *Request by the Attorney General to the Constitutional Court to Control the Constitutionality of Article 9(2) of the Law on the Judicial Council*, Ruling No 07/2016, of 10 May, J. Pina Delgado (rap.), Constitutional Court, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 35, 10 May 2016, pp. 1224–1252, at II.

[12]See also National Authority on Data Protection (2017), p. 6.

[13]In general, Wacks (2010).

[14]*E.g.*, see the essay by Fried (1968).

[15]Follow the influent Whitman (2004).

[16]A glance of the transition to multi-party system is provided by Chabal (1996); Silva (2015), pp. 196 and ff, deals with constitutional law aspects.

hoeren@uni-muenster.de

an important right to be recognised in order to counter practices, that were usual in the so-called First Republic, the previous regime, of information gathering orchestrated by the police via the use of informers.[17] Moreover, if one takes into account the bigger picture, certain features of the past are still in evidence in the present, but shared moral values are also dynamic and small communities evolve. In Cape Verde, societal modernisation, government policy on internet access, digital economy and cyber-administration aimed at the creation of a 'Cyberisland'[18]; the materialisation of an ambitious program of CCTV cameras in urban spaces in order to control and reduce growing criminality[19]; the special relationship with the European Union and some of its members, necessity of upgrading, especially for this reason, its data protection system in order to facilitate important state interests in the fields of security, judicial cooperation, and commerce, banking, tourism and investment attraction, are factors driving the growing interest in the expansion of the data protection system in general.

In addition to this, there is an increasing awareness within the population on the impact of the internet on their communal and private personal lives.[20] Not so much in the field of electoral and democratic proceedings as discussed in other countries,[21] which arguably will be important in the future because the political regime of the islands and the stability of its democratic system[22] is one of its main strategic assets.[23] However, after numerous notorious cases of the leaking of citizens' private data, namely sexual and financial, on the traditional media and specially on the web

[17]Member of Parliament Arnaldo Silva in the presentation of the draft Constitution to the National Assembly in 1992 stressed that recognition of rights to protect the individual in that field was absolutely necessary to prevent "abusive use of computerized information for political police ends" (National Assembly 1992, p. 50).

[18]See also Baker (2009a) and Resende-Santos (2016), as well as the main strategic plans on that matter, the Strategic Program for Information Society (in Portuguese PESI—*Programa Estratégico para a Sociedade da Informação*) (Prime Minister's Office 2005a), the Action Plan for eGovernment (in Portuguese PAGE—Plano *de Acção para a Governação Eletrónica*) (Prime Minister's Office 2005b) and the Strategy on Cybersecurity, approved by the Government Resolution No 21/2016, of 7 March, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 14, 7.3.2016, pp. 531–549.

[19]See the Terms of Reference of the National Program on Internal Security and Citizenship approved by the Resolution No 75/2016, of 15 October, published by Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 59, 14.10.2016, pp. 1978–1979, and the Resolution No. 73/2017, of 7 July, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 39, 07.07.2017, p. 851, implementing the Project 'Safe City'. The project received the required favourable advice of the National Authority on Data Protection (Advice No 3/2018, of 30 January, on the implementation of the CCTV System of the Project Safe City, not published (on file with author)).

[20]For comments see also Traça and Gaspar (2016), p. 250, and, especially the interview of the Chairman of the National Authority on Data Protection, Faustino Monteiro (*Expresso das Ilhas*, n° 821, 23.08.2017, pp. 16–20).

[21]See, for instance, Bartlett (2018), *passim*.

[22]Meyns (2002) and Baker (2006).

[23]Baker (2009b).

hoeren@uni-muenster.de

as well as an abusive use of employee data by public services,[24] potentially exposing the integral self of the person,[25] and the growing use of devices that collect biometric data in the public and private sectors,[26] the importance of protecting online privacy has experienced incremental developments in general personal data protection law in recent years, although not always designed specifically to deal with the internet.

1.2 Subject-Matter, Purpose and Scope of the Present Report

This is a largely descriptive paper aimed at presenting the general framework of data protection on the internet in Cape Verde, including developments up until 2018. It will follow a program that will allow us to present its main features in order to compare it to other national, supranational and international systems of data on this domain. It starts with the presentation of the legal structure regarding personal data protection (Sect. 2), and then it will deal with specific problems of data protection on the internet (Sect. 3), and with the international dimension on data protection (Sect. 4) before presenting some concluding remarks (Sect. 5).

2 The General Data Protection Framework

2.1 The Applicable Norms

2.1.1 The Constitutional Rules

Data protection was inserted into the Cape Verdean Legal System by the Constitution of the Republic of 1992[27] through article 42, where it fitted in well with the liberal and democratic framework based on the values of human dignity, individual freedom, equality and solidarity.[28] The original version of that Constitutional rule included allusions to several privacy related rights and guarantees, specifically with

[24]See the reasons presented to justify the recent amendment of the core data protection act (see Parliamentary Records (audio), 27.07.13, Morning Period (on file with author)).

[25]On this, see Stephens-Davidowitz (2017).

[26]See Ruling No 26/2013, *Antonio Pedro et al v. Minister of Treasury and Planning*, Supreme Court of Justice, Request for Adoption of Provisional Measures, not published (on file with author), in which the plaintiffs requested the review of a decision to forbid entrance and suspend pay of public servants of that governmental service, who didn't supply their data to the Ministry. The measure was granted, but the case was not decided on the merits.

[27]Constitutional Law N° 1/1992, of 25 September, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, I Supplement, n. 12, 25.09.1992, pp. 1–44; for general presentations in English, Lima (2004, 2007).

[28]Pina-Delgado (2013).

hoeren@uni-muenster.de

reference to the inviolability of correspondence and telecommunications and safeguards against the use of computerised means.[29] It also contained a special constitutional remedy to protect data, the *Habeas Data* writ, inspired by the Brazilian 1998 Constitution[30] and common in Latin American jurisdictions.[31] The Fundamental Law was subsequently amended in 1999,[32] when major changes were made to former article 42 (presently article 45) that was specifically dedicated to data protection in the use of computerised means.

2.1.2 The Legislative Acts

At the infra-constitutional level, in 2001, two important acts were approved by Parliament, a general data protection law,[33] amended once in 2013,[34] and, in that same year, a data protection law in the telecommunication domain.[35] In 2013, another act that deals with the main body of the Islands Data Protection system, the National Authority on Data Protection Act, was also enacted.[36] Recently added to the list are the Video Surveillance Act of 14 April 2015[37] and the Cybercrime (and Digital Evidence) Act of 20 March 2017.[38] Additional connected legislation is also relevant in this domain, namely a 1994 Law on Special Constitutional Remedies, that includes an appeal for the protection of fundamental basic rights (*Recurso de Amparo)*—a constitutional complaint—and the already mentioned writ of *Habeas Data*.[39]

[29]See also the presentation of Traça and Gaspar (2016), pp. 251–252.

[30]For a general presentation of this writ in Brazil, see articles in Wambier (1998).

[31]A Latin American comparative perspective is presented by Tizoc Gonzalez (2015).

[32]Constitutional Law No 1/1999, of 25 November, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 43, 23.11.1999, pp. 2–34.

[33]Law No 133/V/2001, of 22 January, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 2, 22.01.2001, pp. 31–41.

[34]Amending Law No 8/VII/2013, of 17 September, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 48, 17.09.13, pp. 1214–1228.

[35]Law N° 132/V/2001, of 22 January, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 2, 22.01.2001, pp. 42–45.

[36]Approved by the Law No 42/VII/2013, of 17 September, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 48, 17.09.13, pp. 1228–1315.

[37]Law No 86/VIII/2015, of 14 April, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 24, 14.05.15, pp. 718–723.

[38]Law No 8/IX/2017, of 20 March, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 12, 20.03.2017, pp. 318–325.

[39]Law No 109/IV/1994, of 24 October, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 35, 24.10.1994, pp. 635–639.

hoeren@uni-muenster.de

2.1.3 The International Norms

Under the Cape Verdean legal system, international law is law of the land.[40] As such, international norms, independent of their conventional, customary, international organisation related origin, can be applied as a regulatory basis with reference to topics which they cover, and with a higher ranking than ordinary legislation (article 12(4)). Thus, arguably, in the event of the country being bound by international rules related to personal data protection,[41] the Constitution determines, according to the principle of respect for international law (article 11(1)) and the norms on reception of international law in the Cape Verdean Legal System (article 12), that they be taken into account by courts and other authorities that apply the law, as well as by legislative and regulatory organs whenever they enact domestic acts regarding those subjects.[42] For this reason, even if there are few international customary norms in the data protection field, the existent treaties that include rules on privacy or personal data protection can have a direct impact on Cape Verdean Data Protection Law if, according to article 12(2), the country, with respect of constitutional procedure, freely consents to be bound by them, they are in force and duly published in the official gazette of the Republic.

African Sources of the Law This is particularly important because the African Union, the continental organisation of which Cape Verde is a member, approved recently in the 23rd Ordinary Session of its Assembly in Malabo, the *African Union Convention on Cyber Security and Personal Data Protection*[43] which contains some non-self-executing norms, including relevant rules on security in electronic transactions, personal data protection and cyber security and combat on cyber crime. This is not applicable internally, however, because, under paragraph two of article 12, it has neither entered into force,[44] nor has Cape Verde consented to be bound by it as yet.

The same can be said of a legal instrument of 16th February 2010 named *Supplementary Act on Personal Data Protection within ECOWAS* (Economic Community of Western African States), sub-regional Organization of which the country

[40]In general, see Pina-Delgado (2018).

[41]Follow Bygrave (2010), pp. 165–200; Zhao (2014), pp. 1–13, and also with interest Schulhofer (2016).

[42]See the decision to the *Request by the Attorney General to the Constitutional Court to Control the Constitutionality of Article 9(2) of the Law on the Judicial Council*, Ruling No 07/2016, of 10 May, J. Pina Delgado (rap.), 2.4.1. and ff.

[43]For a general presentation, Abdulrauf and Fombad (2016), pp. 67–97.

[44]According to the 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection, African Union, 12/11/2018', available at www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf, by December 2018, only 11 countries signed and 3 ratified this convention.

hoeren@uni-muenster.de

is also a Member.[45] Despite this, it is not part of the protocol of revision that amended article 9 of the ECOWAS Treaty and consequently instituted a new regime of normative acts.[46] At least from a constitutional point of view and under its article 12, paragraph 3, though international normative acts of organisations of which Cape Verde is a member are also considered to be domestic law with direct application, in order to produce such effect, the country must have given prior consent to such a power by accepting the treaty that establishes it, which is not the case. But the application of this ECOWAS normative act in Cape Verde becomes even more tricky because the Supplementary Act was signed by a Minister, even though he lacked the power to directly bind the country without Parliamentary consent and presidential acceptance, which could arguably mean that the country is internationally bound by the instrument, even though it is not law of the land. But, under its own terms (article 48), the Act would be in force only after publication in the official gazettes of ECOWAS and of Member States, and in the case of Cape Verde this failed to happen.

It is important to stress that as a result of a very particular confluence of facts, the structure of the regime of data protection by the above-mentioned ECOWAS Act was influenced by European Union Law on that domain that was in force in 2010,[47] which, coincidently, is the same remote inspiration for the Cape Verdean Data Protection legislation—through the intermediation of the Portuguese Legislation on the same topic—and other recent national developments in this field.

European Influences and Sources of the Law Though independent from this, in the last 10 years, the borrowing of European legislation is being justified by an agreement on a special partnership that the Archipelago maintains with the Union. This understanding includes a topic on normative convergence, specifically paragraph 5.4., which stresses as a main focus of the bond "Convergence of technology and standards policies in the sectors covered by the action plan in order to facilitate alignment on EU standards and support Cape Verde's comparative advantages with a view to its development". And another, article 5.5., that underlines the aim of encouraging "Cape Verde's progress towards the "knowledge based society". (. . .) in particular through education, research and the ownership/development of information technology (a sector in which Cape Verde possesses some notable assets in the area of e-government)."[48]

The National Authority on Personal Data Protection once stressed that because a ministerial ordinance had as its main source of influence a homologous act from the

[45]See Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 37th Session of the Authority of Heads of State and Government, Abuja, 16th February 2010, and, for a general presentation, Orji (2017).

[46]See Ukaigwe (2016), Chap. 2.

[47]See Greenleaf (2012), pp. 68–92.

[48]For the text, see Commission of the European Communities (2007), and, for a general presentation, Guedes Vieira and Ferreira-Pereira (2007).

hoeren@uni-muenster.de

Portuguese Republic, a member of the European Union, it justified the compatibility of that ministerial ordinance on video vigilance with the Law.[49] However, the Constitutional Court, in a case concerning the possible application of a treaty related to another regional organisation of the same continent, the Council of Europe, where an interested party argued that a treaty that Cape Verde was not a part of, was due to be applied because of the convergence clause of the special partnership declaration, stated that the agreement was not a treaty and the direct application of European legislation could not, therefore, be justified by appealing to it,[50] which, naturally, did not, in its opinion, forbid State organs with legislative powers from incorporating solutions inspired by the European Union Law or by the legislation of one of its members—namely from the Portuguese Republic—in the draft bills that they promote and enact.

Additionally, besides African legal instruments on data protection that in the future can become binding on Cape Verde and a part of its domestic law, the Archipelago has acceded to the Budapest Convention on Cybercrime in 2018[51]—prior to this, it had to enact the Cybercrime Act of 2017[52]—and also in 2018 to the Convention 108 of the Council of Europe for the Protection of Individuals with Regard to Automated Processing of Personal Data,[53] for which it received an invitation in July of 2017 after a positive advisory opinion, and a recommendation of the Consultative Committee of that organisation.[54]

General Universal Norms and Constitutional Standards of Interpretation There are other less comprehensive international instruments on privacy and data protection, such as general international norms on privacy related rights that are part of Cape Verdean Law, namely article 17 of the Covenant

[49] Advisory Opinion No 1/2015, of 20 August, National Authority on Data Protection, available at http://www.cnpd.cv/doc.php?&id=1, accessed on 09.05.2017.

[50] In the *Request by Members of Parliament to the Constitutional Court to Control de Constitutionality of Norms Amending the Environmental Tax Law*, which had at its core questions involving local government autonomies, the Court rejected the idea that, in reason of the normative convergence clause of the special partnership declaration, the European Charter on Local Self-Government was applicable as such in Cape Verde (See Ruling No 01/2017, J. Pina Delgado (rap.), published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 10, 27.02.2017, pp. 218–260, at 4.4.1).

[51] Approved for Accession by the National Assembly Resolution No 11/VIII/2014, of 19 November, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 70, 19.14.2014, pp. 2107–2133.

[52] As the previous footnote mentions Parliament approved accession in 2014, but, according to the Minister of Justice that in the name of the Government sponsored the legislation on cyber crime, one of the members of the Council of Europe blocked accession because in its opinion existent Cape Verdean rules applicable to cyber crime were not adequate (Parliamentary Records, 30.11.2000, on file with author).

[53] Approved for accession by the National Assembly's Resolution No 49/IX/2017, of 11 June, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 40, 11.06.2017, pp. 862–878.

[54] Available at https://rm.coe.int/16806ee23f, accessed 15.05.2017.

hoeren@uni-muenster.de

on Civil and Political Rights,[55] article 14 of the Migrant Workers Convention,[56] articles 16 and 40 (2) (vii) of the Convention on the Rights of the Child,[57] article 10 of the African Charter on the Rights and Welfare of the Children,[58] article 7 of the African Youth Charter,[59] article 22 of the Convention on the Rights of People with Disabilities.[60] Of special importance are article 30 of The Hague Convention on the Protection of Children and Co-operation in Respect of Inter-Country Adoption,[61] and article 22, paragraph 2, of the Convention on the Rights of People with Disabilities.

It is important to stress that under Cape Verdean Constitutional Law (article 17 (1)), even if a right is not enumerated in the Fundamental Law, it can still be considered as integrated in the Cape Verdean system of fundamental rights protection if it is not mentioned by the Constitution, if it is recognised by an international treaty or even by a sub-constitutional law of the state, if it is a civil or a political right and if it is substantively similar to other enumerated rights from the point of view of the spheres of the individual that it protects.[62] With reference to article 12 of the Universal Declaration on Human Rights, though not being a treaty-norm, its importance for the system can be established, because under article 17, paragraph 3, of the Archipelago Basic Law, fundamental rights norms, both constitutional and legal, shall be interpreted according to the instrument approved by the UN General Assembly.[63]

[55]Approved for accession by the Law No 75/IV/92, of 15 March, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 8, 15.03.1992, pp. 2–28.

[56]Approved for ratification by the National Assembly's Resolution No 46/V/1997, of 17 June, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 23, 2. Supplement, 17.06.1997, pp. 14–31.

[57]Ratified by the Law No 29/IV/91, of 30 December, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 52, 30.12.1992, pp. 1–26.

[58]Approved by the National Assembly's Resolution No 32/IV/1993, of 19 July, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 26, 19.07.1993, pp. 317–325.

[59]Approved for accession by the National Assembly's Resolution No 124/VII/2010, of 22 March 2010, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 11, 22.05.2010, pp. 216–226.

[60]Approved for accession by the National Assembly's Resolution No 148/VI/2010, of 24 January, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 4, 24.01.2010, pp. 317–325.

[61]Approved for accession by the National Assembly's Resolution No 105/VII/2009, of 29 June, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 24, 29.06.2009, pp. 474–486.

[62]See the abovementioned decision to the *Request by the Attorney General to the Constitutional Court to Control the Constitutionality of Article 9(2) of the Law on the Judicial Council*, Ruling No 07/2016, of 10 May, J. Pina Delgado (rap.), para. 2.11.5.

[63]*Ibid*., para. 2.10, and especially the decision of the Constitutional Complaint, *Maria de Lurdes Ferreira v. Supreme Court of Justice*, Ruling No. 11/2017, of 22 June, J. Pina Delgado (rap.), published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 42, 21.07.2017, para. 2.1.6.

hoeren@uni-muenster.de

2.1.4 Case Law on Data Protection

In general, specific case law concerning privacy related topics and particularly concerning data protection is scarce. On a rare occasion in 2007, the Constitutional Court dealt with a video-surveillance related matter in an advisory capacity.[64] The main issue to be dealt with was the review of a norm inserted in the Criminal Investigation Organization Act that allowed for the use of sounds and images obtained by private security cameras of surveillance as evidence in a criminal proceeding—to start investigation or to indict—and that granted a power to order the presentation of recorded data without the need to request consent of concerned persons. The Court considered that it was a matter of restriction of rights, governed by article 17, paragraphs 4 and 5, of the Fundamental Law, and as such to pass constitutional scrutiny it had to be subjected to a test of proportionality. The conclusion was that it did not pass because it was manifestly unbalanced, without sufficient legal checks—in part, according to the justices because in the past the country lacked a comprehensive law on video surveillance—and created the risk of sacrificing those rights in a manner that would have been excessive, arbitrary and abusive.[65]

Recently, the same court delivered opinions on matters related to data protection in relation to freedom of information and freedom of the press.[66] This was important in the sense that it tried to balance the public's interest in transparency in the exercise of public functions and the level of privacy and data protection from which holders of public office could benefit, favouring, in this case, the former over the latter. In another case involving the acceptability of evidence gathered by the police using abusive interference in the mobile phone data of a suspect,[67] the Court delivered an opinion stressing that the fact that an act of communication was not ongoing did not mean that the data, including the registration of phone calls received and made, was not protected by the Constitution. Therefore, though it could not recognise an absolute right insusceptible of being limited, it stressed that even when, in exceptional situations, such interference was necessary, it had to be duly authorised by a judge and not promoted independently by the Criminal Police as was the case. So, it

[64] Advisory Opinion No 1/2007, of 6 September, *Request by the President of the Republic to the Constitutional Court of Advisory Opinion in Order to Control Preventively Norms of the Criminal Investigation Organization Act*, Supreme Court of Justice as Constitutional Court, J. Coronel (rap.), published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 35, 17.09.2007, pp. 659–667.

[65] *Id*.

[66] Ruling No 16/2017, of 31 July, *Request for Access to Declarations of Propriety, Assets and Interests of Holders of Public Office*, C. J. Pinto Semedo (rap.), published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 35, 08.08.2017, II, para. 2.

[67] Ruling n° 27/2018, of 20 December, *Judy Ike Hills v. Supreme Court of Justice*, Constitutional Court, J. Pina Delgado (rap.), published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 11, 31.01.2019, pp. 146–178.

hoeren@uni-muenster.de

ordered the exclusion of that evidence that was essential to the condemnation of the suspect.

2.2 The Notion of Personal Data

2.2.1 A Right to Data Protection and Its Legal Nature

The original version of current article 45 of the Constitution did not contain a formula explicitly acknowledging the existence of a right to data protection. Hence, at least in an explicit manner, a reference to the recognition of a subjective right to data protection or to legal positions related to it was, in general, lacking, though it could be inferred for the limitation of treatment of sensitive data recognised by the Basic Law and the reference to *Habeas Data*, both present in that version. However, in 1999, an amendment inserted a precept establishing that "1. All citizens shall have the right of access to computerised data that affects them and for the same to be rectified and updated, as well as the right to be informed about the purposes of the data, in the terms of the law". From a constitutional point of view, it recognised a subjective right to personal data protection, though through a very limited and not very clear legal construct.

The interpretation of this norm in the sense of the recognition of the right to data protection was operated by administrative and, specially, judicial decision. Despite the flaws of the abovementioned constitutional construction, in its first opportunity to deal with the matter, the Constitutional Court, in an already mentioned case, *the Request by the President of the Republic to the Constitutional Court of Advisory Opinion in Order to Preventively Scrutinize Norms of the Criminal Investigation Organization Act,* was also not absolutely fluid in its position, because it opted for reviewing the legislative norm under the right to image, the right to speech and the right to intimacy of private life. In the explicit *ratio decidendi* used to justify the decision, it abstained from mentioning that right, limiting itself to underscoring a violation of the "rights to image, to speech and intimacy of private life".[68] Nevertheless, without clearly mentioning it, a constitutional guarantee attached to the rights of protection of personal data, was recognised at least implicitly.

On the other hand, the National Authority on Data Protection was more consistent in considering the existence of a personal data protection right,[69] though without much development, and recently in *Judy Ike Hills v. Supreme Court of Justice*, the Constitutional Court, stressing its self-proclaimed role in adjusting the rights system

[68] Advisory Opinion No 1/2007, of 6 September, *Request by the President of the Republic to the Constitutional Court of Advisory Opinion in Order to Preventively Scrutinize Norms of the Criminal Investigation Organization Act*, p. 666.

[69] For instance, in one of its annual reports it mentioned a fundamental right to data protection (National Authority on Data Protection 2017, p. 6; National Authority on Data Protection 2016, p. 2).

hoeren@uni-muenster.de

to a permanently dynamic field as technology,[70] considered that the Fundamental Law recognises a right to data protection directly linked to a general right to privacy anchored in human dignity, liberty and personal autonomy,[71] with a dimension of the right to be left alone[72] (isolated) and a right to control information about oneself (informational self-determination)[73] as a comprehensive safeguard[74] that, in its turn, spreads as special guarantees.[75]

The Court adopted a doctrine according to which, data protection constitutional guarantees result from the broad reading of article 45 of the Basic Law, which means more than explicitly recognising a simple right to access, rectify and be informed about the objectives of its gathering, storage, and treatment, in the sense that it also includes a substantive protection of informational self-determination sheltering against the collection of personal data by the State or other entities. According to the adopted understanding of the Court, people have the right (albeit a limitable right) to prevent their data being gathered by any other entity. In other words, according to constitutional rights limitations mechanisms, it can be limited, to a certain extent, by law, it can be waived by the rights holder and it can be subject to suspension in situations of declared constitutional emergencies even if only to support an important public purpose or a personal interest and only if it is done in a proportional manner and without interfering with the core of the right.[76]

2.2.2 The Relationship Between the Right to Data Protection and Other Constitutional Principles and Rights

In addition, as far as the right of protection of identity, the right to personal image and the right to intimacy of private and familiar life are recognised by another fundamental precept, article 41, the system departs from these rights to construct the safeguards to protect data. For this reason, one would have to consider that data protection is not an autonomous basic right recognised by the Constitution of the Republic that has attached to it a number of fundamental legal positions, safeguards and guarantees, but mostly a fundamental legal tool to guarantee those rights.[77] According to the Constitutional Court in *Judy Ike Hills v. Supreme Court of Justice*, there is a general right to privacy from which unfolds a number of explicit

[70] See also from a comparative perspective the introduction and articles in Leenes et al. (2008).

[71] See also the conceptualization of Buitelaar (2012), pp. 182–202, and, before that, Solove (2006).

[72] Warren and Brandeis (1890).

[73] For the concept, Eberle (2001).

[74] See also the perspectives of Gavison (1980), Cepeda Espinosa (2012) and Rouvroy and Poullet (2009).

[75] Ruling No 27/2018, of 20 December, *Judy Ike Hills v. Supreme Court of Justice*, Constitutional Court, J. Pina Delgado (rap.), II, para. 4.8–4.9.

[76] *Ibid.*, II, para. 4.9.

[77] *Ibid.*, II, para. 4.8–4.9.

hoeren@uni-muenster.de

guarantees, namely linked to its informational self-determination sphere and to data protection.[78] Thus, the understanding is that the data protection is a complex group of constitutional safeguards associated with a general right to privacy and eventually to the right to image and to the right to identity, besides being related to a right of individuals to develop their own personality.[79] The main effect of the opinion of the Constitutional Court is that substantive rights that justify data protection (image, identity and, especially, privacy) are still applicable, dependent on the circumstances of the case, to the situations where a specific explicit safeguard on personal data protection is not directly recognised by any constitutional norm.[80]

2.2.3 The Content of the Constitutional Right to Data Protection

Hence, the right to data protection corresponds to a plurality of safeguards recognised by the Constitution in order to protect any information of persons, being treated by informatised means or not, in the sense that paragraph 7 of article 45 extends the application of the guarantees to manual gathering, storage, access, treatment and transfer.

It includes a safeguard that limits any information gathering and subsequent operations to the existence of legitimate public purposes and/or personal interests; another that forbids, according to the Constitutional Court, the storage in a unique file of all personal data of a person in reason of paragraph 5 of the same article that proscribes the attribution of a single number to persons[81]; a third that limits treatment of sensitive data to few exceptions (para. 2), a fourth that bans access to third persons' files and its inter-institutional transfer, except in cases established by law or according to a judicial decision (para. 4), and others that safeguard regarding treatment of data by delegating powers to the legislative body to establish an adequate and meaningful system to protect personal data (para. 3), namely with regard to constitution and use of data files and respective computerised support by public and private entities (id.) and the cross-border flow of personal data (para. 5). Additionally, people have a right to access their stored data, to be informed of the purposes of the treatment of their data, and to demand its correction and updating (para. 1), and to *Habeas Data* (article 46). In addition, these constitutional rights are completed or materialised by the specific rights mentioned by the general law on personal data protection: to information (article 11), of access (article 12), of opposition (article 13), of non-subjection to automated individual decisions (article 14), to security of data (articles 15 and 16) and to confidentiality in data processing (articles 17 and 18).[82]

[78] *Ibid.*, II, para. 4.8.
[79] *Id.*, II, para. 4.9.
[80] *Ibid.*
[81] *Id.*, II, para. 8.2.
[82] For further comments, Traça and Embry (2011), pp. 252–253.

hoeren@uni-muenster.de

2.2.4 The Concept of Data Protection

Naturally, the Basic Law refers to data protection in article 45, but it does not provide for any elaborate concept or, for that matter, notion. It does not mean that orientations on the meaning of data protection cannot be inferred from the fundamental text. With regard to the connexion with substantive rights such as privacy, image and identity, the content of personal data is necessarily linked to the idea of a person's control of information about oneself and how that integrates their own identity as an individual. Therefore, any concept, independent of definition by the legislative entity, by the courts or by a descriptive doctrine must be as broad as possible with the aim of protecting any type of information that can be assembled on a person,[83] meaning any physical person, namely children and foreigners.[84] Consequently, under article 5 a) of the Data Protection Act of 2001 (consolidated version), personal data, "shall mean any information of any type/nature and irrespective of the medium involved, including sound and image relating to an identified or identifiable person", which means that it integrates the comprehensiveness of the constitutional notion by absorbing all kinds of information, by disregarding the means of gathering or processing and by focusing on the persons as long as they are at least identifiable.

2.2.5 Categories of Data Protection

The legislation includes two main categories in order to develop different, though integrated, legal regimes. It departs from the most important one: sensitive personal data, which, in a positive sense, is considered by paragraph 1 of article 7 of the Data Protection Act as comprising data that reveals "philosophical, ideological or political beliefs or penalty (sic), religion, political party or trade union affiliation, racial or ethnic origin, privacy, health and sex life, including genetic data". These legal limits result in large measure of a direct constitutional injunction, because according to article 45(2) of the Basic Law, "The use of computer means to register and process identified individual data related to political, philosophical or ideological convictions, religious beliefs, political or trade union affiliation or private life shall be prohibited".

The legal definition is apparently more generous than the one integrated in the Constitution. They both focus on information that defines one's consciousness and beliefs (philosophical, ideological or political), related to immutable parts of one's body and/or culture (race and ethnicity); or that integrates an inherited or adopted identity (religion); or are essential in a free and democratic society (political or trade

[83]Ruling No 27/2018, of 20 December, *Judy Ike Hills v. Supreme Court of Justice*, Constitutional Court, J. Pina Delgado (rap.), II, 8.2.

[84]In *Id.*, II, para 1.2, the plaintiff was a Nigerian national resident in Cape Verde, and the Constitutional Court has explicitly said that he was entitled to the general right to privacy and all related safeguards, connected both to criminal procedure and to data protection.

hoeren@uni-muenster.de

union affiliation), but the legal rule also mentions health, sex life and personal data. This would appear to be an expansion of the constitutional definition, but as a matter a fact the legal rules try to materialise the protection due to "private life" by translating it to dimensions of private life that are more intimate and that people need to protect with more intensity. The National Authority on Data Protection, in its recent practice seems to have excessively extended the notion by considering as sensitive almost all personal data that touches any aspect of private life,[85] which in practice has the potential of blurring the distinction between sensitive and ordinary data, a logic that if generally adopted would additionally have the potential to hinder operations of legislative and judicial balancing with other rights, particularly those related to speech, information and press, and important or even compelling state interests.

The reason for the protection of this dimensions of one's life is not just aimed at serving privacy for its own sake, but also to protect people from the discrimination that would arise if certain information were disclosed, besides blocking or at least delaying, in dark times, to use an Arendtian expression,[86] the reunion of undesirable persons to other moral and constitutional unacceptable purposes (massive detention, racial, religious or ethnic cleansing, extermination, etc.). For this reason the Cape Verdean Constitution, in the same article, forbids the attribution of a single number to an individual, which according to a thesis of the Constitutional Court serves a symbolic objective of eliminating the possibility of reducing the status of the person and the denial of their personal identity, but also to prevent the State having a unique file on them or a complete interconnection between files that would permit the total or substantial reconstruction of self.[87]

As previously mentioned, the constitutional norm also integrates some exceptions that allow for the gathering and treatment of sensitive data when there is (a) expressed consent of the holder/data subject; (b) authorisation provided by law, with assurance of non-discrimination; or (c) for data processing of non-identifiable individual statistics purposes.

In a negative construction, one can recognise other data that are considered non-sensitive, ordinary data, that are not protected with such intensity, but that, nevertheless, enjoy a reasonable level of protection, starting with the fact that because of the recognition of a right of protection of personal data that encompasses a right to not having data collected by the State, the limitations are considered

[85]The Authority since 2015 when it provided its first advice on the installation of CCTV cameras in airports adopted this understanding (the first was Advice No 4/2015, 05/2015 and 06/2016, 7/2015, all of 24 December); recently, see Advice No 05/2017, 4 August, 1.1 (on file with author), 2, and Advice No 09/2017, 13 December, 1.1 (on file with author). But lately it added some important criteria for determining sensitive data by linking access to image to the capacity of the profile determination of a certain person (Advice No 3/2018, of 30 January, on the implementation of the CCTV System of the Project Safe City, 8 and ff).

[86]Arendt (1968).

[87]In the Ruling No 27/2018, of 20 December, *Judy Ike Hills v. Supreme Court of Justice*, Constitutional Court, J. Pina Delgado (rap.), II, 8.2.

hoeren@uni-muenster.de

exceptional and only possible in those situations in which there is a public or private interest that justifies it. Provided that this is the case, ordinary data can be assembled, but only if it sticks to the general conditions of safeguarding and monitoring mentioned generally by the Constitution and established by the Personal Data Protection Act.

2.2.6 Entities Covered

In a general sense, under article 2 of the Personal Data Protection Law the scope comprises all entities and there is no special regulation in place for different species, especially public ones. From a broad perspective, General Data Protection Laws are arguably, at least under the definition of the European model,[88] applicable more naturally to private entities than public ones, which is totally understandable because today Big Brother,[89] and the little brothers, can be anyone, not only tech companies, but small businesses and potentially, any person, anywhere.[90] This, provided that it is balanced and that it respects the principle of the autonomy of relations between private entities does not create a constitutional problem in Cape Verde. Not only because in some cases it establishes that such entities are also directly bound to respect basic constitutional rights (article 18 of the Constitution), especially when important fundamental values are at stake—such as dignity or equality—or the relations are marked by a notable difference in economic and social power or special levels of subjection, but also because the State has the obligation to assure through law and executive action the efficacy of those rights in the relations between private entities according to paragraph 1 of article 15 of the Fundamental Law. Anyhow, the Constitution specifically mentions in paragraph 3 of article 45 "public authorities and private entities".

Due to its nature, constitutional rights operate primarily to constrain public powers, and fears of state interference in privacy have increased over the years and are of current concern worldwide, particularly because the "Digital Leviathan" can regiment the help of communications companies for these purposes. In any event, what happens is that in the public sector, in addition to its submission to general privacy laws, it sometimes becomes necessary to adjust the legal regimes that are applicable, because the interests that legitimate its interference with personal data can be different to those interests of the private entities. This is why the System includes the possibility of specific rules being established by special legislation of the sectors of public safety, national defence and state security (article 2(6)), which will be dealt ahead on this report, as well as an exception to "processing of personal data carried out by individuals in the course of purely personal and household activities" (article 3).

[88] As described in the conclusion of the General Report, 5.2.

[89] Orwell (1949).

[90] Like the contemporary dystopia of Eggers (2013).

hoeren@uni-muenster.de

2.3 The Supervising Authorities

In 2001, the Data Protection Act, with article 21, created an Independent Parliamentary Commission to oversee the processing of personal data, but it never came into being. This was one of the main flaws of the initial legal regime on data protection in Cape Verde and the main difference from the one inserted in the European Directive on Data Protection and the Portuguese Data Protection Law,[91] though the possibility of the establishment of a National Authority on Data Protection was discussed in Parliament, but dismissed by the promoters with the justification that an oversight of the Parliamentary Commission with the possibility of judicial review was sufficient to guarantee data protection rights.[92]

When the Law was amended in 2013, after criticism, particularly by the National Commission for Human Rights and Citizenship,[93] of inadequacy of the system and absence of meaningful supervision, it was substituted by a National Authority on Data Protection. Internal reasons were provided justifying the adoption of another institutional model, because according to the sponsoring members of parliament of the new majority party in the National Assembly, the model was wrong because it depended on members of parliament that were not suited to conducting that kind of time consuming job directly associated with the nature of the powers and functions of oversight of the organ established by the law and because it would, arguably, violate the principle of separation of powers if Members of Parliament received such administrative powers.[94]

The new body has the functions of follow-up, evaluation and control of the activities of legally competent entities for the processing of data, with the aim of safeguarding the fulfilment of the Constitution and the Law, especially the fundamental rights, freedoms and guarantees of citizens (article 21). Thus, the Authority is the supervisor of the national personal data processing system with the legal nature of an independent administrative agency (article 22).

According to the previously mentioned National Authority on Data Protection Act, the Authority consists of three members, all elected by the National Assembly by a two-thirds majority of deputies present as long as they are superior to the absolute majority of that legislative organ (article 13(1)), with the chairmanship being assumed by rotation of all members for a period of 2 years each (article 13(2)). However, this rule was not followed by Parliament when it elected one of the members because it modified the order of the candidates, not following alphabetic

[91]This was the main difference between the original Cape Verdean Model and the European and Portuguese ones, as stressed previously by Traça and Embry (2011), p. 251; Pinheiro (2015), p. 564.

[92]Parliamentary Records (2000), 30.11.2000 (audio version) (on file with author).

[93]National Commission for Human Rights and Citizenship (2011), pp. 61–63.

[94]Parliamentary Records (audio), 27.07.13, Morning Period (on file with author).

hoeren@uni-muenster.de

order established by law,[95] nor was it followed by the Authority itself because the rotation rule was not obeyed at the end of the first 2 years cycle.[96]

Members must be citizens with full enjoinment of their civil and political rights and of recognised competence and moral integrity (article 16). They will have a mandate of 6 years that can be renewed once for an equal period (article 14). After taking the oath of office before the Chairman of the National Assembly (article 15), they become irremovable and can only cease functions in case of death or permanent physical incapacity; resignation or loss of mandate. In the last case if they are affected by any incapacity or incompatibility—the same regime that is applicable to holders of high public positions—absence, within a year, from three consecutive meetings or six meetings without justified reasons (article 17).

The organ was installed and started its activities in 2015 after the elections of its first members, a career judge, who presides, a computer engineer and a former member of parliament. Although, according to its first Annual Report (2015),[97] minimal conditions to operate were only met in the last trimester of that year, in its period of existence, it had and has still seen a notable increase in activity reflected in advisory opinions presented to the government in draft bills related to personal data protection,[98] authorisations to controllers of data, specially related to the use of video surveillance and biometric devices, and data collection for research and statistic purposes.[99] 160 authorisations were granted in 2015 according to the 2016 Annual Report[100] and 191 in 2017.[101] In the 2017 Report the Authority stressed that for the first time it could rely on staff with law and computer science degrees,[102] but it still complained of inadequate staffing and facilities.[103]

With the exception of the special case of intelligence agencies or organs, and the residual role of another Administrative Authority—the National Authority on Communications—as will be seen, the National Commission on Data Protection is the

[95]Parliament Resolution No 126/VIII/2015, of 14 April, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 24, 14.05.2015, p. 783. The non-official version was that there was an agreement between the Members of Parliament to assure that the only lawyer candidate—a judge—assumed the function, because this professional and personal profile was more suited to what was required to the first chairmanship of the Authority.

[96]Apparently, according to non-official sources, with the acquiescence, if not the support, of other members that informally adopted the understanding that it was not necessary to follow the rotation principle.

[97]National Authority on Data Protection (2015), pp. 5–6.

[98]Though in the 2017 report it stressed that Parliament was approving legislation on personal data related matters without consulting the Authority (National Authority on Data Protection 2017, p. 13).

[99]National Authority on Data Protection (2016), p. 11.

[100]*Ibid*, 9.

[101]National Authority on Data Protection (2017), p. 12.

[102]*Ibid.*, 1.

[103]*Ibid.*

hoeren@uni-muenster.de

only body that supervises the data protection processing in Cape Verde.[104] In general, under paragraph 2 of article 8 and article 10, the Authority has very broad powers, in particular to supervise and monitor compliance, investigate, deliver opinions, impose conducts and sanction. Despite this, its decisions can be appealed to the courts and constitutional remedies exist in order to allow the subjects of data protection related legal positions to access the ordinary courts and the Constitutional Court with the aim of protecting them (article 46).[105]

2.4 The Self-Regulation Instruments

Article 28 of the Data Protection Act considers that "codes of conduct are intended to contribute in relation to the characteristics of the different sectors for the proper implementation of the provisions of the present Law", attaching to it a complementary role of the Authority in regulation. Under article 29, the impulse to draft codes of conduct can be promoted by the Authority, which can help elaborate them. The controllers also have initiative, but, in the last case, they shall submit the draft Codes of Conduct to the Authority to obtain a declaration of conformity with laws and applicable regulation on data protection. Though there is a request pending from the Civil Aviation Authority,[106] to this date there is only a general corporate code of conduct put in place by controllers and recognised by the Authority. It was promoted by the Airport Management Company (ASA)[107] and includes a norm on data protection. Notwithstanding, these are mere references to some norms on data protection which are far away from creating broad codes of conduct with the aim of regulating in a particular way a certain field of activity or to strengthen the protection guaranteed by the general law as existent in other countries.[108]

[104]Under article 8 of its Law, the National Authority on Data Protection "is the national authority endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law".

[105]See infra Sect. 3.5.

[106]Civil Aviation Authority (2016), para. 2.1.4, though it limits itself to mentioning the need to follow the general law on data protection.

[107]National Company on Airports and Air Security (2016), established under its Article 16 a duty to inform the employee of the objectives, nature and circumstance of its personal data access, a right of the employee to request a full report on its data and to its preservation.

[108]*E.g.*, Hirsch (2011).

hoeren@uni-muenster.de

3 Specific Problems Concerning Data Protection on the Internet

3.1 Personal Data Processed by Electronic Means

With regard to the general regulation of data protection and other acts—that cover certain aspects of personal data processed by electronic means—there is no specific Cape Verdean legislation that broadly encompasses services provided from a distance by electronic means, protection of minors[109] or that recognises the right of erasure of personal data processed by electronic means, tough, as will be seen, this can be a protective measure taken by supervisory entities. Notwithstanding, this does not present an unsurmountable problem, because as far as all Cape Verdean Courts are organs of rights protection, taking into consideration that constitutional norms which recognise civil and political rights are directly applicable even without the interposition of the legislative body, and in light of the fact that courts are obliged to interpret existent ordinary law in conformity with those constitutional norms, Pretorian constructions departing from the Basic Law can solve some of the eventual lacunae in this domain.

In some cases, Esignature and Ecommerce Contracts Act of 2007[110] and the Telework Act of 2018,[111] legislation applicable to electronic matters, includes data protection rules, but with norms that defer to the regulation of the general law on data protection or other and do not establish a specific regulation. A topic that is covered by the domestic legislation is, in a very mild manner, protection of data in the context of electronic communications for marketing purposes by the Data Protection in the Telecommunications Sector Act discussed below (Sect. 3.2), though, in general, it is not well suited to electronic communications, but essentially to telephone and fax communication.[112]

However, the regulation of the processing of personal data of employees through electronic means is present. The Labour Code enacted in 2007[113] regulates this

[109]Despite the Children and Youth Statute (approved by the Law No. 50/VIII/2013, of 26 December, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 70, 26.12.2013, pp. 2309–2337, establishing, under its article 53, a guarantee of supervision by public powers of content of information transmitted to minors on internet sites.

[110]Law-Degree No 33/2007, of 25 of September, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 36, 24.09.2017, pp. 670–689.

[111]Legislative Decree [adopted under a Parliamentary delegation of legislative powers] No 11/2018, of 5 September, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 79, 05.12.2018, pp. 1920–1923.

[112]In its last report, the National Authority on Data Protection (2017), p. 16, recommended the amendment of this law, but it did not clarify if the purpose would be the insertion of rules that would address internet related issues and other advancements in the field of communications.

[113]Approved by the Legislative-Decree No 5/2007, of 16 October, published the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 37, Sup., 16.10.2007, pp. 2–63, amended by Legislative-Decree No 5/2010, of 16 June, published by the Republic's Official Gazette [*Boletim Oficial*], I

hoeren@uni-muenster.de

matter under its articles 45 (data protection), 46 (distance surveillance instruments), 47 (private and family life), and 49–51 (electronic mail).[114] It covers any data concerning information requested by the employer to a worker or to an employment candidate or collected in any other form—in the case of sensitive data—and also information gathered by distance surveillance instruments and electronic mail. According to relevant dispositions, specifically article 45 of the Labour Code, only information "directly and necessarily" linked with a certain position or with the evaluation of professional skills of the worker is permitted with the specific aim of determining the capacity of a person to perform a job.

The gathering of sensitive data related to political and philosophical convictions, union or party membership, religious faith, racial or ethnic origin, health, sex life and genetic data, family and private life, is, in general, interdicted (article 45 (2)). Workers' information rights about their own personal files, the ban on transfer to other entities without prior consent and to request the correction and suppression of personal, familiar or professional data, even when gathered with previous consent, are also recognised (article 47).

The Labour Code forbids, under article 46, the use of technological related equipment that permits surveillance from a distance, such as closed circuit television (CCTV) cameras, by employers with the objective of monitoring job performance by the worker, but they can use them in situations necessary to protect and secure persons and property or in case the particular nature of certain specific professional careers justifies it; there is an obligation to inform the worker of the existence and purposes of such means. In a recent case the District Court of Praia had the opportunity of ruling on the legality of the use of CCTV Cameras to collect evidence for disciplinary procedures aimed at firing a worker, but instead favoured dismissal based on the non-availability of the recorded data for the plaintiff's—the worker's—defence.[115]

With regard to the nature of the information (public or private information) shared by employees through social networks and on the possibility of using it as evidence within disciplinary proceedings there are no specific rules in the Cape Verdean Legislation, nor have the Courts provided specific guidance on this particular matter, but it is not clear that privacy expectations were present in all those situations. Under the Labour Code, the use of electronic means is covered by general norms on the use of employer's equipment to access internet and electronic mail. The main rule establishes that the employer has the power to decide if and under which conditions an employee can have access to those electronic means (article 49), but if authorised the employers have no power to access a labourer's electronic mail or other forms of

Serie, n. 22, Sup., 16.06.2010, pp. 2–4, and by the Legislative-Decree No 1/2016, of 2 February, corrected version published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 22, Sup., 16.06.2016, pp. 271–284.

[114]For general comments, Almeida (2010), pp. 382–399.

[115]*M.A.C. v. Banco Angolano de Investimentos de Cabo Verde (BAI-CV)*, District Court of Praia, Judge Sebastião de Pina, Ruling of 21 April 2017 (not-published; on file with author).

hoeren@uni-muenster.de

internet communication, including social media (*Id.*). Contrarily, the employer can access email and, arguably, other social media that it creates for an employee, with his consent, with the aim of pursuing the company's activities (article 50).

3.2 Data Protection in the Electronic Communications Sector

There is specific legislation that regulates some aspects of the matter approved in 2001: the already mentioned Protection of Personal Data in the Telecommunication Sector Act. In some aspects it resembles the European E-Privacy Directive,[116] but it was enacted prior to this, which can be explained by the fact that its promoter probably took the draft directive into account. It focuses globally on all kinds of telecommunications.

Nonetheless, according to article 4, the "law is applicable to data treatment of personal data in connection with the offer of telecommunications service available to the public in public telecommunications networks", which means that any entity that offers services of telecommunications falls under the obligations inserted in that Act. Furthermore, the law does not include a concept of communication data, though it mentions that it is applicable to all services provided through the digital web with services integration. Regrettably, there is no relevant case law that has tried to deal with the concept, especially designed to define its scope with regard to possible application to internet-provided services in the sense that the Act only contains a general framework regarding all forms of telecommunications, without a classification in different categories.[117]

There is a general norm in the Act—article 6—that guarantees confidentiality and secrecy of communication through any means of telecommunication accessible to the public and public webs of telecommunication, forbidding eavesdropping, interception or surveillance of communication and storage of data without the consent of users. In addition, the Act, under article 7, applies to all forms of telecommunication, traffic data, which must be erased or anonymised. Article 5 establishes, generally, that the service provider is obliged to adopt all necessary measures to guarantee security of telecommunications services—which must be, according to it, 'adequate'—to cover existent risks, though subject to the principle of proportionality, considering costs of adopting such measures and the state of technological development of the country. In the case of special risk of security breaches, according to article 5, paragraph 3, the service provider has a duty to inform subscribers of that situation, as well as of the possible solutions to avoid its materialisation and respective costs.

[116] As stressed by Traça and Embry (2011), p. 255.

[117] For this reason, the National Authority on Data Protection (2017), p. 16, has recommended its amendment.

hoeren@uni-muenster.de

Under this Act, the same body created by the Data Protection Act, a Parliamentary Supervising Commission, never installed, and an Independent Authority established by the Cabinet, had both sanctioning powers, and the latter regulatory powers.[118] In 2006, Cape Verde created an independent administrative agency for communications with a regulatory nature, called ANAC (National Authority on Communications),[119] with some residual powers in this domain, in particular to impose fines on telecommunication companies that violated duties related to data protection and privacy. This administrative agency was subsequently merged with the Agency on Economic Regulation creating a Multisectorial Regulatory Agency, which received all the powers it held.[120]

3.3 Data Protection and Digital Forensics

There were scarce references in the legislation that—though not specific—could be applied to digital forensics, especially in the evidence domain. Previously, in the Criminal Procedure Code of 2004[121] (as amended by a law of 2015),[122] there was nothing specifically designed with that objective, though some general rules applied to electronic mail (article 255 (1)). However, a recent act introduced a more comprehensive regulation on the collection of evidence in the cyber world. The Cybercrime Act (and Digital Evidence) of 2017 contains the legal framework for the collection of evidence by electronic means. Nonetheless, according to its article 20 (4) and to the Constitutional Court[123] many norms on interception and recording of communication of the Criminal Procedure Code are still applicable.[124]

The above-mentioned special act provides for a very large umbrella, under which fall cyber crimes described by the law, crimes committed by means of a computer system or any crime "when it is necessary to collect evidence in electronic form"

[118]Parliamentary Records, 30.11.2000.

[119]Law-Decree No 31/2006, of 19 June, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 17, 19.06.2006, pp. 436–456, subsequently amendment by the Law-Decree No 33/2015, of 4 June, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 34, 4.06.2015, pp. 1078–1091.

[120]Law-Decree No 50/2018, of 20 September, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 60, 20.09.2018, pp. 1544–1557.

[121]Approved by the Legislative-Decree No 2/2005, of 7 February, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 6, Sup., 7.02.2005, pp. 2–87; for background, Fonseca (2003), pp. 114–115; for general presentation, Patrício (2009), pp. 240–241, and, with a critical analysis, Leite (2009), pp. 9–48.

[122]Legislative-Decree No 5/2015, of 11 November, published by the Republic's Official Gazette [*Boletim Oficial*], I Serie, n. 69, 11.11.2015, pp. 2247–2341.

[123]Ruling No 27/2018, of 20 December, *Judy Ike Hills v. Supreme Court of Justice*, Constitutional Court, J. Pina Delgado (rap.), II, para. 8.

[124]For comments, Fonseca (2009).

hoeren@uni-muenster.de

(article 1). It establishes rules targeting preservation of electronic data, research on electronic data, apprehension of electronic data, interception of electronic data and reading of electronic data, email and other similar manners of communication.

Expediting the preservation of data requires, in principle, a judicial warrant or a public prosecutor order. But, if there is "emergency or danger in delay" they can be ordered by a criminal police organ (article 14); if, in the case of search of computer data, the person who has the availability or control of such data, provides voluntary and documented consent or in cases of terrorism, violent or highly organised crime, when there is evidence of the imminence of a crime which poses a serious risk to life or health of any person; in the case of seizure of computer data, in addition to the abovementioned reasons, in cases of emergency or danger in delay. In such situations, there is a duty to give notice to the judicial authority or submit the data for judicial validation. Research on electronic data (article 17) and apprehension of electronic data (article 18) and email correspondence and other related communications (article 19) follow a similar path, depending on judicial or public prosecutor's authorisation, and only in exceptional circumstances following an order of a criminal police organ.

Article 20 of the Cybercrime Act and, as subsidiary legislation, the Code of Criminal Procedure is the relevant regulatory instrument on the matter of interception. Interception of content data and traffic data is allowed, in the cases of crimes established by that law, in particular computer forgery, computer damage, computer sabotage, illegal access, misuse of devices, offences related to child pornography and revenge porn, and of other crimes if punishable with a maximum sentence limit of over 3 years, crimes against sexual self-determination, terrorism and violent or highly organised criminality, crimes against the protection due to children, drug trafficking, smuggling related offences and insult, threat, coercion, disclosure of private life and disturbance of peace and quiet, when committed by means of electronic device. It is a requirement that it must be authorised by a reasoned judicial decision—which shall contain its specific scope—after a request made by the Prosecution's Service, if there are reasons to believe that this is essential to establishing the truth or that gathering the evidence would otherwise be impossible or very difficult to obtain by other means.

The remaining rules applied are inserted in the Criminal Procedure Code, in article 255, paragraph two, that limits interception of communication data subjectively to suspects or to persons against whom there are grounds to believe that they receive or transmit messages aimed at the suspects or that a suspect uses their electronic equipment. In addition, paragraph three of the same article establishes that the time-limit of the operation is 3 months, renewable for equal periods, provided that the respective requirements for admissibility have been met, especially in addition to what was mentioned above, if there are grounds to believe that it will help the Court to "discover [...] the truth".[125] Interception of communication between the defendant and its counsel or other persons subjected to a duty of

[125] See the critic of Fonseca (2003), p. 114.

hoeren@uni-muenster.de

professional secrecy is forbidden, with the exception of any situation in which they are also suspects of committing the same crime.

The disrespect for such conditions and requirements, under article 257 of the Criminal Procedure Code, determines the exclusion of the evidence obtained, an effect that the Constitutional Court recently underlined in the case *Judy Ike Hills v. Supreme Court of Justice* when it considered that the non-exclusion of evidence apparently decisive in convicting suspects of drug-trafficking in a situation where the criminal police read their mobile telephone data without a judicial warrant violated their constitutional rights to inviolability of communication, the general right to privacy and their right to personal data protection.[126] Thus, it adopted an injunction ordering the lower court to exclude this evidence, in a country that used to be very understanding of efforts made by police agencies to combat drug-trafficking even when blunders were made when investigating the crimes and sloppy work curtailed basic procedural and substantive rights of suspects and where criminal police and even some public prosecutors and judges were sympathetic in the sense that those irregularities were minor flaws that should be acceptable to people that have 'nothing to hide',[127] neglecting not only the rights of the affected persons, but also the substantive public value of privacy and personal data protection.

With regard to data retention, there is no specific legislation, but this is dealt with by the Criminal Procedure Code under articles 256 and 257, the Cybercrime Act and the Video Surveillance Act. The Video Surveillance Act of 2015 was enacted after the Constitutional Court gave an Advisory Opinion considering that, from a constitutional point of view, there were insufficient guarantees under an Organization of Criminal Investigation bill that Parliament approved.[128] After a very general norm was inserted in the same bill and approved as an Act, those guarantees were introduced by the 2015 Law. Under this legislation, images can be retained for a maximum period of 30 days and destroyed after proceedings (articles 21 and 23).

More specifically, the Cybercrime Act, as mentioned, permits, in general, traffic data interception, considering that whenever it is silent, according to article 30, the Criminal Procedure Code is applicable, which in its articles 256 and 257 permits retention of data for those purposes. Therefore, the law determines that the technical materials that are not transcribed to the case-file, will remain under the Public Prosecutor Service guard, but must be destroyed before (if they happen to be unnecessary for related purposes) or after a decision that is final and not subject to an appeal, and if so requested by any interested person to the judge that ordered or authorised the collection. In this case the same general requirements for interception of data apply.

[126]Ruling No 27/2018, of 20 December, *Judy Ike Hills v. Supreme Court of Justice*, Constitutional Court, J. Pina Delgado (rap.), III, 1 (c).

[127]See Solove (2011), for the borrowed expression.

[128]Above Sect. 2.1.4.

hoeren@uni-muenster.de

3.4 Data Protection and Electronic Surveillance for Security and Defence Purposes

As already stated, from a symbolic point of view, the recognition of privacy related rights and data protection guarantees was justified by the necessity to prevent the possibility of uncontrolled gathering of personal information by the security agencies of the Government.[129] Of course, the secret police of the so-called First Republic, under a one party system, was no Stasi and the level of informers and arguably of dossiers in personal files was far from reaching the levels of the German Democratic Republic,[130] despite the fact that many agents of the security apparatus of the regime were trained there.[131] Certainly, the one party system was 'just' an authoritarian[132] and at times repressive regime[133] not a totalitarian one, so one will not find features similar to Nazi Germany, Stalinist Soviet Union or even from other African Dictatorships when looking at the structure and practices of the First Republic.[134] Finally, the level of technological development and organisation would never permit the degree of digital communications surveillance similar to the ones conducted for instance by the National Security Agency of the United States of America.[135]

Nonetheless, even the creation of a national intelligence agency, the Republic's Intelligence Services, in 2005, was received with distrust, especially because it was promoted by the former leading party of the First Republic after returning to Government 4 years earlier, with different actors expressing concerns on its possible misuse to gather information about opposition and inconvenient civil society personalities,[136] especially because the draft act had no lustration clause forbidding former members of the secret police of being recruited to become agents of the created service.[137]

[129] Above, Sect. 1.1.

[130] See articles in Spiekermann (2014).

[131] According to Cardoso (1993), p. 59, members of the police were trained by the GDR Stasi, Romania Securitate, and their pairs from the Union of Socialist Soviet Republics and the Popular Republic of China.

[132] See Cardoso (1993).

[133] See Silveira (1992).

[134] See this context in 'Serviços de Informação da República. Ninguém fala, é segredo', Expresso das Ilhas, 23 de fevereiro de 2015, available at https://expressodasilhas.cv/politica/2015/02/23/servico-de-informacoes-da-republica-ninguem-fala-e-segredo/44034, last accessed 5 january 2019.

[135] For instance, Sloan and Warner (2016).

[136] See Parliamentary Records, 26.04.2005, 162.

[137] See *Id.*, and Parliamentary Records, 30.03.2005, pp. 237 and ff.

hoeren@uni-muenster.de

Since then the Service, besides the slow start and critics of absence of efficacy[138] or maybe for those reasons, is keeping itself out of the public eye without generating any polemic, despite the fact that it is authorised to gather information for security purposes under the Republic's Information System Act of 2005[139] and related legislation and regulations, namely concerning its Data Centre[140]—responsible for the processing, treatment and storage of information and data—and from the Professional Statute of its Directors and agents.[141]

The Armed Forces also have an intelligence service, but its intervention in the gathering of information and data processing is rather loosely regulated by the Republic's Information System Act of 2005 (article 17). Nevertheless, it has been developed by the Armed Forces Organizational Decree (article 14),[142] and related legislation (Regulation on Armed Forces Organization article 12)[143] so that the scope of its activities is limited only to military information related to the missions that are constitutionally reserved for the Armed Forces (article 247 of the Constitution) and so that it is subject to the Minister of National Defence, through the Chief of Staff, oversight (article 18).

On the one hand, despite its sponsor in the Parliament that assured concerned members of the opposition that it would not have powers in order to intercept and monitor communication,[144] the scope and the wording of the Law is potentially very broad and permissive in the case of the Republic's Information Service. This is especially because the law is not sufficiently clear on the limits and requirements of collection of information and data, as long as it respects an activity that "threatens or may threaten the security of the State and the permanent survival of the Democratic State and the Rule of Law constitutionally established or any other fundamental interest of the country as defined by the Council on National Security" (article 9 a)); activities mentioned by the law cover matters of national defence in the classic meaning of the word, but also other non-conventional threats. On the other hand, the Law determines that such activities of data collection cannot violate basic rights as defined by the Constitution and applicable ordinary legislation (article 4) and are subject specifically to the ones related to privacy and data protection. Be this as it

[138]The abovementioned newspaper's piece in 2015 reported that the Service only started operating in 2009 and that its production of valuable information was close to zero ('Serviços de Informação da República. Ninguém fala, é segredo').

[139]Law No. 70/VI/2005, of 27 June, on the Republic's Information System, published by the Republic's Official Gazette [*Boletim Oficial*], I Série, n. 26, 27.06.2005, pp. 768 and seq.

[140]Law-Decree No 29/2016, of 16 April, published by the Republic's Official Gazette [*Boletim Oficial*], I Série, n. 28, 16.04.2016, pp. 1016–1026.

[141]Minister's Council Resolution No 36/2009, of 14 December, published by the Republic's Official Gazette [*Boletim Oficial*], I Série, n. 47, 14.12.2009, pp. 1062–1065.

[142]Law-Decree No 30/2007, of 20 August, published by the Republic's Official Gazette [*Boletim Oficial*], I Série, n. 31, 20.08.2007, pp. 567–573.

[143]Regulatory-Decree No 6/2009, of 26 January, published by the Republic's Official Gazette [*Boletim Oficial*], I Série, n. 4, 26.01.2009, pp. 76–81.

[144]See Parliamentary Records, 30.03.2005, 260.

hoeren@uni-muenster.de

may, these and other constitutional norms are always applicable even in the absence of legislation and even if contradicted by legislation.

The Republic's Information Service Regulation, in its article 6(3), considers that threats which the Office has the obligation to prevent have to be especially serious, such as, for example, action by radical and anti-democratic groups and other acts against the constitutional principles, transnational organised crimes and mafias, terrorism, speculation with capital, destructive sects, both religious and exoteric, proliferation and smuggling of arms and its use by criminal groups, technological crimes and the use of cybernetic technology with criminal purposes.

It would seem that this is the main explicit requirement according to the law, because, apparently, an order leading to the gathering and to the storage of information and data is not subject to previous judicial authorisation, nor has it to be validated *ex post factum*, as long as it is necessary for the purposes that justify the existence of the intelligence service in general, and the specific threat. In addition, it would create the impression that, in principle, any entity and person, national or foreign, can be the subject of data processing for those purposes, and for the time that is deemed necessary to counter the threat. This is not the best interpretation, however, because constitutional norms that protect privacy and personal data condition interference with mail—including electronic mail—and all kinds of methods of communication do so by using an authorisation established by law and a judicial warrant. Besides this, additional control is related with the existence of a commission composed by three members of the Public Prosecution's Service that supervise the Data Centre (article 15) and the general political oversight of a special parliamentary commission that shall monitor the intelligence service according to the Law (Articles 20 and 21).

3.5 Remedies and Sanctions

The Personal Data Protection Act provides for a myriad of remedies, both civil, administrative and ordinary judicial ones, because it recognises that "without prejudice to the right to submit a complaint to the CNPD, according to the law any individual may seek legal recourse regarding violations of rights granted him by the present law" (article 30).

Thus, the Personal Data Protection Act allows data subjects to lodge complaints with the Authority in cases of administrative offences, specifically negligence in the obligation to notify the Authority of processing of data, presentation of false information or inobservance of requirements of information in authorisation requests, continuance of permission of access to open data transmission networks to controllers who fail to comply with the provisions of the law can be fined to a minimum of 300,000 CVE (around US$3000/€27,244) and a maximum of 3,000,000 CVE (around US$30,000/€27,244) if a legal entity or to a minimum of $50,000 CVE (around US$515/€454) and a maximum of $500,000 CVE (around US $5159/€4540) if a physical person, with the possibility of applying double that

hoeren@uni-muenster.de

amount in some cases (article 33). Besides, the Authority under article 46 can order the temporary or permanent prohibition of processing, blocking, erasure or total or partial destruction of data; and the publication of the judgement, at the expense of the person, in a newspaper close to the place of the infringement and issue a public warning or censure of the controller of the processing of the data. According to its 2016 Annual Report complaints are rare and the Authority refrained from the use of its sanctioning powers, opting, in its first couple years of existence, for a more pedagogic approach.[145] The first procedure in order to determine the existence of an administrative offence was started only in 2017 and finished with a recommendation directed at an insurance company.[146] In another case a fine of 2,400,000 CVE (two point four million escudos), almost US$25,000/€21,795, was applied to the most important food retailer of the main Island, Santiago.[147]

Additionally, the Law on the Protection of Personal Data in the Telecommunication Sector established financial sanctions for certain offences, in particular in observance of the duty to assure information or to obtain advanced consent before recording communication or of obligations related to billing and marketing which can lead to the application of fines from 100,000 CVE (around US$1000/€908) to 1,000,000 CVE (around US$10,000/€9081).

The decisions of these Authorities can be appealed at the Courts through contentious administrative procedures and data subjects have a special constitutional remedy called *Habeas Data*, which covers some, if not all, of the data protection safeguards. Under article 46 of the Constitution, "All citizens shall be granted *Habeas Data* to ensure the knowledge of the information contained in files, computer archives and registers that affect them, as well as to be informed about the purposes of the data and for the same to be rectified or updated". The Law of 1994 on Special Constitutional Remedies (Constitutional Complaints and *Habeas Data*) and the Constitutional Court Act establish the procedure, which recognises legitimacy of a person, directly and effectively affected by a denial of access to personal data or a request to provide information about the purposes of the gathering or of rectification or actualisation, to appeal, provided that administrative means are exhausted, to the main court of the land, the Constitutional Court. The decision can order access to the data by the subject, information and documents to be provided as well as the rectification and actualisation requested. In the case of non-compliance, government members are subject to penalties for a crime of responsibility and public servants to civil, administrative and criminal responsibility, and according to the doctrine adopted by the Constitutional Court in *Judy Ike Hills* it would not be strange if it admitted *Habeas Data* requests in order to scrutinise the mere gathering of data. Courts—the Supreme Court initially and after 1999 the Constitutional Court—have never received a *Habeas Data* request since 1992.

[145]National Authority on Data Protection (2016), p. 9.

[146]National Authority on Data Protection, decision of 7 July 2017 (on file with author).

[147]National Authority on Data Protection, Process No 053/2018, *Sociedade Comercial Calú & Ângela, Lda*, decision of 23 April 2018 (on file with author).

hoeren@uni-muenster.de

In addition, ordinary remedies and sanctions are also available. In this case, the recourse to the ordinary courts can be civil, when the subject of data treatment is entitled to sue and receive compensation as a result of an unlawful processing operation and other acts incompatible with applicable laws in the domain of data protection. Nevertheless, according to the General Data Protection Act, the controller can claim that it should be totally or partially exonerated from liability if it proves that the fact that caused harm is not attributable to it (article 31).

In the criminal sphere, complaints are possible, but depending, in most of the cases, on a decision by the State Prosecution's Service to indict based in the commission of crimes established by the Criminal Code (Crimes against the intimacy of private life: as private life abuse, computer abuse, breach of correspondence or telecommunications; breach of secrecy, improper advantage of secrecy as well as article's 212 fraud through computerised means) or by special law that covers data protection, namely by the general law: certain omissions of notification, presentation of false information in the process of authorisation, misappropriation or uses incompatible with the purpose of collection, illegal combination of personal data, undue access, invalidation and destruction of data, qualified non-compliance, violation of duty of secrecy. Depending on the specific crime the sanction can be a fine or a penalty that can go up to a maximum of 4 and a half years of imprisonment in the case of a violation of duty of secrecy by a civil servant, or if the intention of the agent was to obtain a material advantage or other unlawful gain or it adversely affects the reputation, honour and esteem or the privacy of a person. In addition, the Cybercrime Act incriminates certain relevant acts and omissions relevant to data protection (informatics damage; informatics sabotage; illicit access to informatics systems; illicit interception; revenge porn); additionally, under article 19 of the Republic's Information System Act, violation of rules on access, use or transfer of data is a crime punishable with a penalty that can reach 3 years of imprisonment.

On the other hand, besides the administrative and judicial—civil, criminal and constitutional—remedies mentioned, there is no specific remedy for protection of personal data in the context of services provided from a distance, by electronic means, at the individual request of a recipient of services, protection of personal data in the context of electronic communications for marketing purposes, electronic processing of personal data of employees, security of personal data processed by electronic means, the processing of personal data in the electronic communications sector; protection of personal data for the purpose of the investigation, detection and prosecution of crimes through electronic means, to the electronic processing of personal data for security and national defence purposes, though in some cases other administrative services can intervene, like the National Direction of Labour in the case of treatment of employee data.

There is no specific supervisory body with powers to impose a financial penalty or to sanction for most of those areas, though, in the case of the Republic's Information Service under article 16 of the Republic's Information System Act, the Prosecutors' Commission can impose the rectification or destruction of data collected in violation of basic rights and institute criminal proceedings when justified for the practice of specific crimes linked to data protection as violation of rules

hoeren@uni-muenster.de

related to the access, use and transmission of data punishable with a penalty of 6 months to 3 years of imprisonment, if other is not applicable. For the misuse of function for purposes alien to the mission of the organ, a disciplinary sanction that can lead to the agent dismissal from service is available.

4 The International Dimension of Data Protection

4.1 The Territorial Scope of Rules on Data Protection

The scope is defined by article 2 of the Data Protection Act defining a basic level of application by taking the place of the establishment of the controller as the criteria, under which it is applicable when the data processing is carried out in the context of the activities of an establishment of a controller situated within the national territory as specified by International Law and article 6 of the Constitution.

4.2 The Applicability of Data Protection Rules to Foreign Entities

Article 2 of the Data Protection Act also defines that data protection rules are applicable outside national territory in areas where, under International Law, Cape Verdean Law applies, namely under International Law of the Sea, International Air Law and International Diplomatic Law. The same article includes an exception under its number three, permitting the application of data protection rules to foreign entities, namely to a controller that makes use of automated or other types of equipment situated in Cape Verde, except in the case that such use has only the purpose of transit. So, the extraterritoriality of the Cape Verdean data protection rules application is very limited, not providing for a very clear protection in cases where controllers are not established in the national territory.

4.3 The Specific Conditions Applicable to the Transfer of Personal Data to a Foreign Jurisdiction

The general rule of the Law establishes both substantive and procedural conditions for the transfer of data to a foreign jurisdiction, respectively that the country has an adequate level of data protection, assessed in light of all circumstances surrounding a data transfer or a set of data transfers, in particular the "nature of the data, the purpose and duration of the proposed processing, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the State in

hoeren@uni-muenster.de

question, as well as the professional rules and security measures which are complied with in that country", and a request to the National Authority, that, through a case by case analysis, will decide if the State ensures an adequate level of protection.

But some exceptions are applicable to cases where a State doesn't have an adequate level of protection, which comprises the following situations: (a) If the data subject has given his "unequivocal consent to the proposed transfer" or, alternatively, if it is necessary for "the performance of a contract between the data subject and the controller of the processing of the data or the pre-contractual measures taken in response to the request of the subject"; for "the execution/performance or the signing of a concluded or to be concluded contract in the interest of the data's subject between the controller and a third party"; or if it is "legally required on the grounds of important public interest, or for the establishment, exercise of defence of legal claims; for the protection of vital interests of the data's subject; or, made from a public register, within the contexts of the laws or regulations, is intended for information of the public and which is open to consultation either by the general public or by any person who can demonstrate legitimate interest provided the conditions laid down in law for consultation are fulfilled in this case"; (b) In other situations, if the processing controller, "provides adequate guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contractual clauses"[148]; on the other hand, (c) transfer of personal data protection for purposes of national security ("State, security, defence; public safety") and international criminal cooperation are regulated by international conventions to which Cape Verde is party or by special legal provisions of other acts, in this case being specially important article 5 of the Republic's Information System Act—though dependent of a Regulation that was not approved yet—and of the Law on Judicial Cooperation in Criminal Matters.

4.4 The Law Applicable to Liability for Damages Caused by the Unlawful Processing of Personal Data

With regard to the law applicable to liability for damages caused by the unlawful processing of personal data, there is no special rule in force. Thus, the main instrument is still the Civil Code, despite the existence of a law that covers certain aspects of electronic contracts, with all its limitations with regard to new techniques of commerce, specifically trans-boundary e-commerce and technologically related developments.

Cape Verdean Private International Law is mainly inserted in the Civil Code (articles 25–63), which is the same as the Portuguese Civil Code of 1966, so the

[148]Traça and Embry (2011), pp. 253–254.

hoeren@uni-muenster.de

adopted regime is the same.[149] In addition to articles 41 and 42 that provided for a criteria to contractual obligation and subsidiary norm applicable in the case of absence of a specific manifestation of the will of the parties which is not well suited to the internet, the basic rule on this matter is article 45 that regulates extra-contractual liability, adopting as a basic criteria the idea that the applicable law is the law of the State where the main act that caused the harm occurred or of the State where one should have acted. But, if the law where the act happened does not consider the agent liable, the law of the state of the victim would be applicable, but only if the latter should have foreseen the harm in that country as a consequence of their actions. Another exception encompasses cases where both agent and victim are of the same nationality or in the absence of this have the same place of residence and accidentally they are abroad, when the applicable law will be of the country of nationality or of the country in which they habitually reside, despite the applicability of those provisions of the local State that are applicable to all persons.

5 Concluding Remarks

5.1 The Basic Approach to Regulation of Data Protection on the Internet

a) The General Cape Verdean System on Data Protection is grounded in a Constitutional Right, the right to data protection, that the Basic Law as interpreted by the Constitutional Court considers a group of safeguards and guarantees connected to a general right to privacy and also to the rights to image, identity and development of personality;
b) The System is developed in a centralised and systematic manner, *i.e.*, with a general law on data protection at its centre, which is completed by other more specific legislation, that often defer regulation to that law;
c) The System is comprehensive and adopts a very broad concept of data protection and divides it into two species: sensitive data and ordinary data, with stricter limits to the gathering and processing in the case of sensitive data in general associated to thought, conscience and immutable personal characteristics and circumstances;
d) Self-regulation by corporate codes of conduct and similar, play in law and still more in practice a limited role in regulation, designed exclusively to allow adaptation to particularities of different sectors of activity and enhance the general protection, without the possibility of downgrading its level;
e) Relevant rules impose duties of conduct both on public and private entities and, in a limited manner, it is applicable extraterritorially;

[149] Moura Vicente (2005), pp. 307–309.

hoeren@uni-muenster.de

f) There are also rules aimed at controlling the transborder flow of data that openly conditions it to the existence of an adequate level of protection, despite some exceptions that can permit the transfer;
g) The dimension of specific rules on data protection on the internet is still underdeveloped, but growing. In any case, though causing problems of inexistence of norms more suited to regulate special problems related to the internet, perhaps with the exception of some sanctionatory matters, does not leave the field unregulated because general norms and rules related to data protection in the telecommunications field are applicable, and courts have powers to interpret broadly ordinary law and appeal directly to the constitutional rights that protect privacy and data;
h) Rules on data protection gathered by intelligence agencies—both civil and military—lack precision and may create hermeneutical problems, specially related to powers to obtain information on the internet by communication monitoring or analysis of metadata and related judicial control, but as far as the organisation and capacity of the services are still limited the problem is frozen for a while;
i) With regard to data protection in criminal proceedings, though permissible under the law, the regime inserted in the Code of Criminal Procedure and in the Cybercrime (and Digital Evidences) Act is rather strict and marked by a principle of judicial authorisation and by the possibility of exclusion of evidence obtained by arbitrary intervention in private life;
j) Another important feature is the existence of an independent administrative agency, the National Authority on Data Protection, specially designed to protect data, through preventive intervention by necessary authorisation to data controllers; advice prior to data treatment, powers to impose sanction, and competence to receive complaints;
k) Appellative role of courts; for this reason, despite the existence of a special administrative agency, courts, specially the Constitutional Court, are involved in this field without much space to be excessively deferential with decisions of the National Authority on Data Protection;
l) Common remedies to protect data are part of the system, namely the possibility of lodging complaints in administrative agencies, starting civil proceedings for liability in data processing, and the possibility of seeking criminal responsibility through the Office of the Public Prosecutor, but it has two special procedures that can permit access to the Constitutional Court: a general remedy for civil and political rights judicial defence that can be used to protect both the general right to privacy and the safeguards linked to data protection, the *Recurso de Amparo*, a Constitutional Complaint; and a special writ to protect data, the *Habeas Data*.
m) The sanctionary regime is not yet complete and though a tendency of its toughen up is visible in the last amendment to the general law on data protection and in new special legislation in this field, it follows a path of moderation both at the administrative and criminal domains.

hoeren@uni-muenster.de

5.2 A General Assessment

Cape Verde's basic approach is largely determined by the fact that its legislation is inspired by the former European Union Data Protection Directive and the way it was received by Portuguese Law, legal system that has influenced the greatest part of the most relevant legislation of the country. The approach is also determined by the fact that its economy and international cooperation is closer to Europe than the United States. Hence, it is not surprising that the data protection system that it has adopted and is developing is clearly a projection of the Union Model.

Despite this, the system also has integrated influences from other sources, namely the procedure of *Habeas Data* from Latin America, which can conduct to another paradigm, but that in my opinion can also be harmonised with the European model of data protection, because they are not mutually exclusive. It is also important to stress that in reality some influences of American constitutional law can be observed, namely in the field of exclusion of evidence and of protection of expression, speech and the press, in situations of collision with privacy.

In the near future, decision-makers and important operators in the field of data protection have already signalled the continuing development of the system according to the parallel development of the European Data Protection System[150]—which is positive for the abovementioned economic reasons—but it is possible that some adjustments will be made in order to accommodate them with the elements imported from other constitutional traditions (the United States and Latin American) and to the local customs, traditions and attitudes natural to small, archipelagic and *créoule* societies, allowing application of the law to move in its own direction.[151]

References

Abdulrauf LA, Fombad CM (2016) The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa? J Media Law 8(1):67–97

Almeida GC (2004) Subsídios em Torno dos Direitos de Cidadania na Sociedade de Informação. Direito e Cidadania 19:229–268

Almeida GC (2010) Direito do Trabalho Cabo-Verdiano. ISCJS, Praia

Arendt H (1968) Men in dark times. Harcourt Brace, Orlando

Baker B (2006) Cape Verde: the most democratic nation in Africa? J Mod Afr Stud 44(4):493–511

Baker B (2009a) Africa's secret story of success: Cape Verde. Br Acad Rev 11:43–45

Baker B (2009b) Cape Verde: marketing good governance. Afr Spectr 44(2):135–147

Bartlett J (2018) The people vs the tech. How the internet is killing democracy (and how can we save it). Ebury, London

[150] See the Interview of Faustino Monteiro, Chairman of the National Authority, in Expresso das Ilhas, n° 821, 23.08.2017, 17.

[151] See Bygrave (2010), p. 195.

hoeren@uni-muenster.de

Bogdan M (2000) The law of the Republic of Cape Verde twenty five years after independence. J Afr Law 44(1):86–95
Buitelaar JC (2012) Privacy: back to the roots. German Law Rev 13(3):171–202
Bygrave L (2010) Privacy and data protection in international perspective. Scan Stud Law 56:165–200
Cardoso H (1993) O Partido Único em Cabo Verde. Um Assalto à Esperança. Imprensa Nacional de Cabo Verde, Praia
Cepeda Espinosa MJ (2012) Privacy. In: Rosenfeld M, Sajo A (eds) The Oxford handbook of comparative constitutional law. Oxford University Press, Oxford, pp 966–981
Chabal P (1996) The transition to multi-party politics in Lusophone Africa. Problems and prospects. Lusotopie:57–69
Cham (2017) Cape Verde. In: Data protection laws of the world, pp 87–90. https://www.dlapiperdataprotection.com/index.html. Accessed 16 May 2017
Civil Aviation Authority (2016) Proposta de Código de Conduta e Ética [Draft code on behaviour and ethics]. AAC, Praia (on file with author)
Commission of the European Communities (2007) Communication from the Commission to the Council and to the European Parliament on the Future of the Relations between the European Union and the Republic of Cape Verde (2007), COM (2007), Brussels 24.10.2007. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0641&from=EN. Last accessed 6 Jan 2019
Eberle EJ (2001) The right to informational self-determination. Utah Law Rev 4:965–1006
Eggers D (2013) The circle. Knopf, New York
Fried C (1968) Privacy. The Yale Law Journal 77 (3):475
Fonseca JC (2003) Um Novo Código de Processo Penal para Cabo Verde. Estudo sobre o Anteprojecto do novo Código. AAFDL, Lisboa
Fonseca JC (2009) Fundamental rights and constitutional limits and constraints to the police action in the criminal procedure: several aspects in some Juslusophony systems. In: Oliveira J, Cardinal P (eds) One country, two systems, three legal orders – perspective of evolution. Springer, Berlin, pp 359–373
Gavison R (1980) Privacy and the limits of law. Yale Law J 89(3):421–471
Greenleaf G (2012) The influence of European Data Privacy Standards outside Europe: implications for the globalisation of Convention 108? Int Data Privacy Law 2(2):68–92
Guedes Vieira AL, Ferreira-Pereira L (2007) The European Union-Cape Verde special partnership. The role of Portugal. Portuguese J Int Aff 1:42–50
Hirsch D (2011) The law and policy of online privacy: regulation, self-regulation, or co-regulations? Seattle Univ Law Rev 34:439–480
Leenes R, Koops B-J, De Hert P (eds) (2008) Constitutional rights and new technologies. A comparative study. T.M.C. Asser Press, The Hague
Leite AL (2009) Algumas considerações sobre o regime jurídico das escutas telefónicas em Cabo Verde. Direito e Cidadania 29:9–48
Lima A (2004) Cape Verde. In: Heyns C (ed) Human rights law in Africa, vol II. Martinus Nijhoff, Leiden, pp 954–959
Lima A (2007) Cape Verde. In: Robbers G (ed) Encyclopaedia of world constitutions, vol I, Facts on file. New York, pp 174–178
Lobban R Jr (1995) Cape Verde. From colony to independent nation. Westview Press, Boulder
Makulilo AB (2012) Privacy and data protection in Africa: the state of the art. Int Data Privacy Law 2(3):163–178
Meyns P (2002) Cape Verde: an African exception. J Democracy 13(3):153–165
Moura Vicente D (2005) Problemática Internacional da Sociedade de Informação. Almedina, Coimbra
National Assembly (1992) Atas da Sessão Parlamentar de Aprovação da Versão Originária da Constituição de 1992. Assembleia Nacional, Praia

hoeren@uni-muenster.de

National Authority on Data Protection (2015) Relatório de Atividades. CNPD, Praia (not published; on file with author)
National Authority on Data Protection (2016) Relatório de Atividades 2016. CNPD, Praia. (not published; on file with author)
National Authority on Data Protection (2017) Relatório de Atividades. CNPD, Praia
National Commission for Human Rights and Citizenship (2011) I Relatório Nacional de Direitos Humanos, 2004–2010. CNDHC, Praia
National Company on Airports and Air Security (2016) Código de Conduta: Uso da Internet, Correio Eletrónico, Computador e Documentos [Code of conduct: internet use, electronic mail, computers and documents]. Sal, ASA, approved on 18 March 2016 (on file with author)
Oliveira e Costa M (2012) Portugal. In: Kuschewsky M (ed) Data protection & privacy. Jurisdictional comparisons. Sweet & Maxwell, London, pp 419–439
Orji UE (2017) Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act. Int Data Privacy Law 7(3):179–189
Orwell G (1949) Nineteen eighty-four. Penguin, London
Patrício R (2009) Da Prova no Novo Código de Processo Penal de Cabo Verde. In: Dias AS, Fonseca JC (eds) Direito Processual Penal de Cabo Verde. Sumário do Curso de Pós-Graduação sobre o Novo Código de Processo Penal de Cabo Verde. Almedina, Coimbra, pp 221–246
Pina-Delgado J (2013) Constituição de Cabo Verde de 1992 – Fundação de uma República Liberal de Direito, Democrática e Social. In: Pina-Delgado J, Silva MR (eds) Estudos Comemorativos do XX Aniversário da Constituição de Cabo Verde. Edições ISCJS, Praia, pp 113–159
Pina-Delgado J (2018) O Direito Internacional Público no Direito Cabo-Verdiano. In: Bacelar Gouveia J, Pereira Coutinho F (eds) O Direito Internacional Público nos Direitos de Língua Portuguesa. CEDIS, Lisboa, pp 81–176
Pinheiro AS (2015) *Privacy* e Proteção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional. AAFDL, Lisboa
Prime Minister's Office (2005a) PAGE – Plano de Acção para a Governação Electrónica. Gabinete do Primeiro Ministro, Praia
Prime Minister's Office (2005b) Programa Estratégico para a Sociedade de Informação. Gabinete do Primeiro Ministro, Praia
Resende-Santos J (2016) Electronic government in Cabo Verde: the prospects and limits of innovation in small island developing states. In: Adesida O, Karuri-Sebina G, Resende-Santos J (eds) Innovation Africa. Emerging hubs of excellency. Emerald, Bingley, pp 99–165
Rouvroy A, Poullet Y (2009) The right of informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: Gutwirth S et al (eds) Reinventing data protection? Springer, Cham, pp 45–76
Sarmento e Costa C (2005) Direito da Informática, Privacidade e Dados Pessoais. Almedina, Coimbra
Schulhofer S (2016) An international right to privacy? Be careful what you wish for. Int Constitutional Law J 14(1):238–261
Silva MR (2015) Contributo para a História Político-Constitucional de Cabo Verde, 1974–992. Almedina, Coimbra
Silveira O (1992) A Tortura em Nome do Partido Único. O PAICV e a sua Polícia Política. Terra Nova, Ponto e Vírgula, Mindelo
Sloan R, Warner R (2016) The self, the Stasi, the NSA: privacy, knowledge and complicity in the surveillance state. Minn J Law Sci Technol 17(1):347–408
Solove D (2006) A taxonomy of privacy. Univ Pa Law Rev 154(3):477–560
Solove D (2011) Nothing to hide. The false tradeoff between privacy and security. Yale University Press, New Haven
Spiekermann U (ed) (2014) The Stasi at home and abroad. Domestic order and foreign intelligence. German Historical Institute, Washington, DC
Stephens-Davidowitz S (2017) Everybody lies. Big data, new data and what internet reveals about who we really are. Day Street, New York

hoeren@uni-muenster.de

Tizoc Gonzalez M (2015) Habeas data: comparative constitutional interventions from Latin America against neoliberal states of insecurity and surveillance. Chicago-Kent Law Rev 90 (2):641–668
Traça JL, Embry B (2011) An overview of the legal regime for data protection in Cape Verde. Int Data Privacy Law 1(4):249–255
Traça JL, Gaspar PM (2016) Data protection in Cape Verde: analysis of the state of the art. In: Makulilo AB (ed) African data privacy laws. Springer, Cham, pp 249–258
Ukaigwe J (2016) ECOWAS law. Springer, Cham
UNTACD (2012) Harmonizing cyberlaw and regulations. The experience of the East African Community. UNTACD, Geneva
Wacks R (2010) Privacy: a very short introduction. Oxford University Press, Oxford
Wambier TAA (ed.) (1998) Habeas Data. Revista dos Tribunais, São Paulo
Warren S, Brandeis L (1890) The right to privacy. Harv Law Rev 4(5):193–220
Whitman J (2004) Two western cultures of privacy: dignity versus liberty. Yale Law J 113:1151–1221
Zhao B (2014) The internationalisation of data privacy: toward a common protection. Groningen J Int Law 2(2):1–13

hoeren@uni-muenster.de

National Report: Czech Republic

Radim Polčák, František Kasl, and Jakub Míšek

1 General Data Protection Framework

1.1 Legislation and Case-Law

Protection of personal data is considered a specific fundamental right. It is explicitly recognized by Art. 10(3) of the Constitutional Act No. 2/1993 Sb., the Charter of Fundamental Rights and Freedoms, which reads as follows: "Everyone has the right to be protected from unauthorized gathering, public revelation, or other misuse of their personal data."

The Czech Republic is an EU member-state which means that the main statute for protection of personal data is Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation—GDPR).

Despite being self-executing, the GDPR requires, in some areas, national legislative implementation in a similar manner as if it was merely a directive. In addition, the GDPR is accompanied by the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. That Directive is not directly applicable and needs to be harmonised into the Czech law.

The Czech transposition of current EU personal data protection framework should be based on a special act (Personal Data Processing Act) that should mainly include provisions for processing of personal data for public interest and an

R. Polčák (✉) · F. Kasl · J. Míšek
Masaryk University, Faculty of Law, Institute of Law and Technology, Brno, Czech Republic
e-mail: radim.polcak@law.muni.cz

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_5

hoeren@uni-muenster.de

amending act that should subsequently change a number of indirectly related statutes (*e.g.* the Police Act, Code of Criminal Procedure, Code of Civil Procedure etc.) However, both aforementioned acts, *i.e.* the 'Personal Data Processing Act' and the 'Act Amending Certain Statutes with Regards to the Adoption of the Personal Data Processing Act' are at the time of editing of this text (Fall 2018) still pending at the Czech Parliament.

Consequently, even after the GDPR came into force and the Directive the No. 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, was repealed, there still applies the old Czech Act No. 101/2000 Sb., on the Protection of Personal Data and on Amendment to Some Acts that originally had implemented the Directive No. 95/46/EC. This situation is quite unfortunate and leads to high uncertainty namely among controllers and processors of personal data. It is highly questionable which parts of the Act No. 101/2000 Sb. have been materially derogated by the GDPR and which provisions still apply.

There has been so far established no case-law upon the GDPR. However, thanks to the use of analogical fundamental principles and definitions related to protection of personal data with previous legislation, it is possible to use existing case-law namely of the Court of Justice of the European Union (CJEU) and the Czech Supreme Administrative Law. The most relevant cases of the CJEU include:

- Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*.
- Case C-582/14, *Patrick Breyer v. Germany*.
- Case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmiés Információszabadság Hatóság*.
- Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*.
- Case C-212/13, *František Ryneš v Úřad pro ochranuo sobních údajů*.
- Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.
- Joint cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications et al*.
- Case C-461/10, *Bonnier Audio AB et al. v Perfect Communication Sweden AB*.
- Case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH*.
- Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*.
- Case C-101/01, *Bodil Lindqvist*.

Compared to other EU member-states, the Czech case-law is relatively scarce. The most relevant cases are listed below:

- Supreme Administrative Court 9 Azs 49/2018—50.
- Supreme Administrative Court 3 As 3/2017—38.
- Supreme Administrative Court 3 As 118/2015—34.
- Supreme Administrative Court 1 As 113/2012—133.

hoeren@uni-muenster.de

– Supreme Administrative Court 4 As 90/2013.
– Supreme Administrative Court 4 As 109/2013.
– Supreme Administrative Court 4 As 75/2012—28.
– Supreme Administrative Court 5 As 158/2012.
– Supreme Administrative Court 7 As 186/2012.
– Supreme Administrative Court 3 As 21/2005.
– Constitutional Court I. ÚS 517/10.
– Municipal Court in Prague 10 A 220/2013.
– Municipal Court in Prague 11 A 77/2012.

1.2 Definitions

Basic statutory definitions are contained in Art. 4 of the GDPR. Personal data are regarded as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Special categories of personal data (former 'sensitive personal data') whose processing is specifically restricted are defined in Art. 9(1) of the GDPR as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

The scope of the GDPR is limited to the domain of the EU law, so it does not cover *e.g.* processing of personal data for security or defence purposes. The GDPR also does not cover processing of personal data 'by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'—that area is legislated indirectly through the Directive (EU) 2016/680. However, if the aforementioned Czech Personal Data Processing Act, and the Amending Act are passed, there will apply analogical definitions and principles of protection according to the GDPR also in these areas.

1.3 Institutional Backing

The main responsible authority for administrative protection of personal data is the Czech Office for the Protection of Personal Data (*Úřad pro ochranu o sobních údajů*). We further refer to the Office also as to the Czech Data Protection Authority

hoeren@uni-muenster.de

(DPA). The English language website of the Czech DPA is at https://www.uoou.cz/en/.

The Czech DPA has a general administrative jurisdiction incl. the jurisdiction to investigate and sanction the processing of personal data. Providers of services of electronic communications are simultaneously under the administrative jurisdiction of the Czech Telecommunications Office (*Český telekomunikační úřad*—English website is available at https://www.ctu.eu) with regards to protection of privacy in electronic communications.

The scope of jurisdiction of the Czech DPA does not include processing of personal data in the judiciary and in the course of criminal investigation and prosecution. That is due to the principle of distinction of powers between the administration (part of which is also the Czech DPA) and the judiciary. The envisaged Personal Data Processing Act and the Amending Act (see above) lay down supervision powers over processing of personal data in criminal proceedings for the Supreme Public Prosecutor's Office. The same draft acts also establishes supervision over processing of personal data in the judiciary for superior courts and ultimately for all Czech supreme judicial institutions, *i.e.* the Supreme Court, the Supreme Administrative Court and the Constitutional Court.

1.4 Self-Regulation

The regulatory architecture of the GDPR is built on performance-based rules. It means that black-letter law lays down only basic principles and general requirements, while particular behavioural rules are set up autonomously by regulated subjects, *i.e.* controllers and processors. Controllers and processors have to document ways in which they process personal data and adopt efficient protective measures. In addition, controllers and processors are obliged to autonomously implement procedures for data subjects to exercise their rights.[1]

Relative vagueness of performance-based rules created demand for solutions that would provide controllers and processors with greater certainty as to compliance of their autonomously developed measures with legal requirements. The GDPR thus counts in Art. 42(1) with 'establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors.'

It is also expected that significant role in defining particular rules for typical forms of processing of personal data will be played by various specific instruments such as standard data protection clauses, binding corporate rules or codes of conduct. The adoption procedures of these instruments are legislated in the GDPR, but their mere

[1]For more particular explanation of use of behavioural rules in the Czech law, see Polčák et al. (2018), p. 13.

hoeren@uni-muenster.de

creation is solely a matter of initiative or controllers, processors or various professional associations or guilds.

2 Personal Data Processed by Electronic Means

The Czech law does not contain a specific legislative act covering the protection of personal data in the context of services provided at a distance, by electronic means, at the individual request of a recipient of services. These forms of personal data processing were until recently governed by the general statutory rules of the Act. No. 101/2000 Sb. on the Protection of Personal Data and on Amendment to Some Acts. The current general framework is provided by the GDPR. It shall further be supplemented by upcoming new Czech national personal data protection framework consisting of the 'Personal Data Processing Act' and the 'Act Amending Certain Statutes with Regards to the Adoption of the Personal Data Processing Act'. These legislative drafts reflect the coming into force of the GDPR and provide for transposition of the provisions contained in Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Police Directive 2016/680) and Directive (EU) 2016/681 on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. However, as of now, there are no indications, that even this new legislation should contain specific legislative provisions on the protection of personal data in the context of services provided at a distance, by electronic means, at the individual request of a recipient of services.

Aside from directly applicable general provisions of the GDPR, the Czech law currently does not provide for specific additional protection of data subjects in this context. The data controller is not required to have a consent for the electronic processing under circumstances divergent from the requirements set under the GDPR. There are no additional limitations of processing for specific purposes or for specific types of data or other particular requirements for the electronic processing of personal data. The increased protection of minors pursuant to the GDPR should be applicable to age threshold of 15 years of age, as implies from the proposal of the 'Personal Data Processing Act'. This provision is, however, subject to extensive political debate and it is currently unclear, if the threshold will not be moved further towards the minimal threshold of 13 years of age set by the GDPR.

Rules for the rectification and erasure of personal data were already previously found in the Act. No. 101/2000 Sb. as a transposition of the Directive No. 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. These were replaced by more extensive and detailed provisions in Articles 16 and 17 of the GDPR as well as parallel provision of Article 16 in the Police Directive 2016/680, which are to be transposed to Czech law by the

hoeren@uni-muenster.de

'Personal Data Processing Act'. Apart from these, there are no specific rules present in the Czech law for the rectification and erasure of personal data. In particular, the Czech law did not, as of now, pursue specific legal framework for personal data processing on social networks. There are therefore so far no tailored provisions regarding personal data protection in this context and the general data protection framework as introduced above applies.

Despite there is no specific legislation regarding electronic processing of personal data, it might be found relevant in this context that the Czech Republic has a specific legislation on cyber security—the Act No. 181/2014 Sb., on Cybersecurity. This Act does not contain any particular provisions on the protection of personal data, but it provides for a regulation of gathering and processing of specific dataset that consists of data collected by the Governmental Cybersecurity Incident Response Team (govCERT)[2] and might also include IP addresses. Given that the Court of Justice of the European Union (CJEU) confirmed through decision on 19th October 2016 in the case C-582/14, Breyer, that static as well as dynamic IP address has the capacity to be considered as personal data, the Czech legislation on cyber security can therefore be seen as relevant. From organisational perspective, it should be noted that the formal institutional assignment of govCERT was recently transferred from the Czech National Security Authority to the newly established National Office for Cybersecurity and Information Security.

2.1 Commercial Communication

The Sections 7 and 8 of the Act No. 480/2004 Sb., on Certain Information Society Services contain specific legislation on commercial communication constituting the transposition of the Articles 6 to 8 of the Directive (EU) 2000/31/EC on electronic commerce.[3] These provisions set conditions for dissemination of the commercial communication. Pursuant to Section 2 lit. f) of the Act No. 480/2004 Sb.; *"commercial communication" includes any form of communication, including advertisement or invitation to visit the website, designed to direct or indirect promotion of goods, services or image of a commercial entity, who or which is regarded as entrepreneur or exercising a regulated profession pursuant to the Czech law*.

The prior consent of the recipient of the communication is required, unless the contact details were obtained from the recipient during a conduct of sale of goods or services and in compliance with general personal data protection framework. In such a case, the contact details may be used for commercial communication to the recipient concerning similar products of the commercial entity in question, if the recipient is always provided by clear instructions to withdraw consent with such communication for free. The commercial communication through electronic mail is

[2]See in Czech: Maisner and Vlachová (2015), pp. 126–128.

[3]See in Czech: Maisner (2016), pp. 138–147.

hoeren@uni-muenster.de

not permitted, if it is not clearly marked as commercial communication; if the identity of the sender is concealed; or if the message is sent without a valid e-mail address, where the recipient may directly and effectively send a message that further commercial communication is undesirable.[4]

With regard to regulated professions, the commercial communication through electronic means is permissible under above described conditions, if it is further in compliance with the rules of conduct published by the commercial, professional or consumer organizations. An emphasis is given to advancement of professional independence, dignity, honour and honest conduct towards customers. The commercial communication of a regulated profession must further contain the name of the professional self-governing chamber established by law, where the entity is registered; link to the professional rules of conduct applicable in the member state of EU, where the entity is established; and a form of permanent public access to information about the respective professional self-governing chamber established by law.

The formerly applicable Act No. 101/2000 Sb. contained additional specific provisions covering personal data processing in the context of commercial communication. However, it did not differentiate between electronic and non-electronic communication. It is a little peculiarity, that these rather specific provisions were part of the same section, which enlisted the general duties of the controller. The text of Section 5 subsections 6 to 9 read as follows:

(5) If the controller or processor carries out personal data processing for the purpose of offering business or services to the data subject, the data subject's name, surname and address may be used for this purpose provided that the data were acquired from a public list or in relation to his activity of controller or processor. The controller or processor, however, may not further process the data specified above if the data subject has expressed his disagreement therewith. The disagreement with processing must be expressed in writing. No additional personal data may be added to the data specified above without the consent of data subject.

(6) The controller who processes personal data pursuant to paragraph 5 may transfer these data to other controller only under the following conditions:

   (a) the data on the data subject were obtained in relation to activities of the controller or the personal data in question were made public;
   (b) the data shall be used exclusively for the purpose of offering business and services;
   (c) the data subject has been notified in advance of this procedure of the controller and the data subject has not expressed disagreement with this procedure.

(7) Other controller to whom data pursuant to paragraph 6 have been transferred may not transfer these data to any other person.

(8) Disagreement with processing pursuant to paragraph 6(c) must be expressed by the data subject in writing. The controller shall be obliged to notify each controller to whom he has transferred the name, surname and address of the data subject of the fact that the data subject has expressed disagreement with the processing.

(9) To eliminate the possibility that the name, surname and address of the data subject are repeatedly used for offering business and services, the controller shall be entitled to

[4] See in Czech: Maisner (2016), pp. 15–27.

hoeren@uni-muenster.de

> further process the subject's name, surname and address in spite of the fact that the data subject expressed his/her disagreement therewith in accordance with paragraph 5.[5]

These provisions were in fact invalidated by coming into force of the GDPR, which also contains specification with regard to direct marketing in Article 21 concerning the right to object, in particular in subsections 2–4. The text of the provisions reads as follows:

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

Cookies and similar technologies are regulated in Section 89 subsection 3 of Act No. 127/2005 Sb., on Electronic Communications (Electronic Communications Act). This act incorporates into the Czech legal system the "cookie provision", as provided in the Article 5 subsection 3 of the Directive (EU) 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive).[6] As to the scope and substance of the national implementation of cookies and similar technologies, the Czech law uses the same definition as the e-Privacy Directive. Section 89 subsection 3 reads as follows:

> Anybody wishing to use, or using, the electronic communications network for the storage of data or for gaining access to the data stored in the subscribers' or users' terminal equipment shall inform those subscribers or users beforehand in a provable manner about the extent and purpose of processing such data and shall offer them the option to refuse such processing. This obligation does not apply to activities relating to technical storage or access and serving exclusively for the purposes of message transmission via the electronic communications network, nor does it apply to the cases where such technical storage or access activities are needed for the provision of an information society service explicitly requested by the subscriber or user.

The provision regulates all situations, where there is an intention to use an electronic communications network for the storage of data or for access to the data stored in the subscriber's or user's terminal equipment. However, there is a divergence between the wording of the Directive and the Czech implementation. Strictly speaking, the opt-in principle was not incorporated into the Czech provision. The

[5]Unofficial translation of the Czech Office for the Protection of Personal Data. Available online: https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1107&archiv=0&p1=1105.

[6]See in Czech: Chudomelová et al. (2016), pp. 295–298.

hoeren@uni-muenster.de

amending Act No. 468/2011 Sb. removed the words 'exclusively for the purposes' from the sentence "This obligation does not apply to activities relating to technical storage or access and serving exclusively for the purposes of performing or facilitating message transmission via the electronic communications network", while the wording of the first sentence remained the same as before the adoption of the Directive 2009/136/EC, which brought opt-in principle for cookies to the e-Privacy Directive. Thus, under the Czech law, the provider has only a duty to offer an option to refuse the use of cookies. Interestingly, the explanatory note of the amending act states that the opt-in principle is in fact introduced, which leaves space for confusion among both providers and users.

To prevent unintended operational breaches of the EU law, The Czech Data Protection Authority issued a guidance stating that the law should be interpreted in the light of European provisions,[7] so that the opt-in principle should be applied even though Czech law does not provide for such specific statutory obligation.

Pursuant to the coming into force of the GDPR, the Czech Data Protection Authority issued in May 2018 a draft Recommendation regarding processing of cookies and similar means of monitoring.[8] The document summarizes the applicable combination of obligations implied from the Section 89 of the Electronic Communications Act and the GDPR. It highlights the personal data protection by default and design pursuant to Article 25 GDPR; clear formulation of the purpose of processing and identification of legal basis; duty to assess the related risk; duty to inform the data subjects and provide them with an option to withdraw their consent. The draft recommendation distinguishes between technical cookies necessary for proper functioning of the website, which do not require user consent and other cookies, which require user consent through appropriate browser settings. The text further favours the less demanding requirements on cookies of third parties, as it accepts as sufficient a more general consent related to form of processing rather than specific consent with particular cookie on particular website. The content of the draft recommendation was open to comments and as of now, there is not final wording of the recommendation available. It is, however, probable that the recommendation will be further amended in light of the received feedback, as some of the wording is diverging from current academic view on the issue.

[7]Cookies: přechod z principu opt-out na opt-in [Cookies: transfer from the opt-out principle to opt-in], 2012, Available online (in Czech): http://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=1853&n=cookies-prechod-z-principu-opt-out-na-opt-in&query=cookie&p1=1099.

[8]Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018 [Recommendation regarding processing of cookies and similar means of monitoring following 25th May 2018], 2018. Available online (in Czech): https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=29966&n=cookies%2Da%2Dgdpr&p1=1099.

hoeren@uni-muenster.de

2.2 Processing of Personal Data in the Workplace

The processing of personal data of employees may take various forms, including, but not limited to geolocation; surveillance through CCTV cameras; performance monitoring; surveillance of the use of company's equipment or accounts and electronic mail addresses. These are situations, where balancing of the interests between the employer and the employee are of the essence. In the Czech Republic, there is case law available that concerned various forms of this aspect of employer-employee relationship. The processing of personal data of employees is subject to general data protection framework represented by the GDPR. Additionally, the Act No. 262/2006 Sb., Labour Code, covers in a specific provision of the Section 316 the requirements on protection of the employee's privacy.[9] The text of Section 316 subsections 2 and 3 of the Labour Code reads as follows:

> (2) Without a serious cause consisting in the employer's nature of activity, the employer may not encroach upon employees' privacy at workplaces and in the employer's common premises by open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee.
> (3) Where there is a serious cause on the employer's side consisting in the nature of his activity which justifies the introduction of surveillance (monitoring) under subsection (2), the employer shall directly inform the employees of the scope and methods of its implementation.[10]

The following court decisions deal with various aspects of intrusions into privacy of the employees and processing of their personal data.

The decision No. 6 Ca 227/2008-71 of the City Court in Prague, delivered on 27th September 2011, concerned the installation of CCTV cameras in the workplace. The Czech Office for the Protection of Personal Data fined Státní Tiskárna Cenin (STC) a state-owned company, which is the only authorised body for printing of banknotes, for monitoring its employees on the workplace by the system of CCTV cameras. The STC was found in breach of the obligations to sufficiently inform the employees about the monitoring and obtain their consent. STC then put a motion against the decision, but the Court ruled to uphold the decision of the Czech Data Protection Authority. Of relevance for this ruling was also that the monitored area did not concern printing of banknotes, but of food stamps and public transport tickets. There was therefore not found a sufficiently serious cause on the employer's side consisting in the nature of its activity which would justify the introduction of surveillance pursuant to Section 316 subsections 2 and 3 of the Labour Code.

The Czech Supreme Court was concerned with the monitoring of employee's computer activity in the decision No. 21 Cdo 1771/2011, delivered on 16th August 2012. The employer terminated the employment of the employee because the

[9] See in Czech: Kahle et al. (2015), pp. 641–643.

[10] Unofficial translation of the Ministry of Labour and Social Affairs. Available online: http://www.mpsv.cz/files/clanky/3221/Labour_Code_2012.pdf.

hoeren@uni-muenster.de

employee used employer's computer for personal matters without employer's consent. By that the employee breached a duty, which is stipulated in subsection 1 of the section 316 of the Labour Code.[11] The employer used a log of employee's account activity as evidence. The employee tried to defend himself stating that the employer breached the data protection law by unlawful monitoring of his activities, but the court sided with the employer, arguing that the employer must have a possibility to ensure that his assets (the work computer in this case) are used in accordance with his instructions and that the resulting intrusion into employee's privacy was marginal. Similar conclusion reached the Czech Supreme Court also in the decision No. 21 Cdo 747/2013, delivered on 7th August 2014.

The Czech Constitutional Court had to deal with an opposite situation in its decision on 9th December 2014, No. II. ÚS 1774/14. Here the matter related to permissibility of evidence obtained by the employee through secret recording of a discussion with his supervisor. The evidence was permitted with the justification, that the employee did not have any other means how to prove the content of the discussion. The legal permissibility was based on protection of the weaker party threatened by serious harm (loss of employment).

On 2nd September 2014, City Court in Prague decided another case concerning CCTV cameras at workplace. In the decision No. 8 A 182/2010 the court confirmed a fine, which was set by the Czech Data Protection Authority to a vendor for having CCTV cameras in the shop, because by that he unlawfully processed personal data of his employees working at the counter and in the shop. The main breaches of personal data protection obligations concerned lack of previous information about the monitoring, extensive duration of the data storage and lack of consent or sufficiently serious cause justifying the surveillance pursuant to Section 316 of the Labour Code.

Important is also the decision of the City Court in Prague from 5th May 2017, No. 6 A 42/2013, dealing with the monitoring of postmen through GPS trackers. The employer, Czech postal service, was recording the location in short intervals during the work routine of the postmen, whereas the identity could be inferred from separately held task schedule. The Czech postal service defended the system by special obligations to effective postal service derived from the specific Act on Postal Services. The Czech Office for the Protection of Personal Data, however, found the measures disproportionately in breach of employees' privacy. The main issue was the continuous recording, which stored all positions of the postman during his or her working routine, including entering shops or public toilet. As the GPS tracking was not based on previous consent of the postmen, court in its ruling sided with the Office and confirmed its decision.

Despite the number of cases discussed in Czech courts concerning the processing of personal data of employees and limits of their privacy in the workplace, we are not

[11] Without their employer's consent, employees may not use the employer's means of production and other means necessary for performance of work, including computers and telecommunication technology for their personal needs. The employer is authorized to check compliance with the prohibition laid down in the first sentence in an appropriate way.

hoeren@uni-muenster.de

aware of any specific decision that would provide orientation on the use of electronic means by the employees in respect to the nature of the information shared by employees through social networks. With respect to this aspect of the issue and the subsequent question of use of such information for evidence in disciplinary actions against the employee, the Czech courts are primarily guided by the interpretation provided by the European Court of Human Rights in the Grand Chamber decision from 5th September 2017 in the case *Bărbulescu v Romania*, Application No. 26713/05.

Also in the relevant legislation, there is no specific provision for the use of social media. The above mentioned Section 316 of the Labour Code contains merely a general provision concerning use of employer's assets (electronic as well as non-electronic) by the employees in subsection 1. This provision reads as follows:

> (1) Without their employer's consent, employees may not use the employer's means of production and other means necessary for performance of work, including computers and telecommunication technology for their personal needs. The employer is authorized to check compliance with the prohibition laid down in the first sentence in an appropriate way.

When it comes to the online (as well as offline) activity of the employee, it is further generally governed by the Section 301 of the Labour Code, which enumerates fundamental obligations of the employees as follows:

> Employees are obliged:
>
> (a) to work properly in accordance with their strength, knowledge and capabilities, fulfil instructions given by their superiors in compliance with the statutory provisions and cooperate with other employees;
> (b) to make full use of their working hours (working time) and capital equipment (means of production) for performance of the work assigned to them, to fulfil their working tasks properly and timely;
> (c) to observe the statutory provisions relating to the type of work carried out by them; to observe other regulations relating to the type of work performed by them provided that they have been duly acquainted therewith;
> (d) to properly use (manage) the resources (means) entrusted to them by the employer, to secure and protect the employer's property against damage, loss, destruction and misuse, and not to act contrary to legitimate interests of the employer.

Pursuant to the original decision in the case *Bărbulescu v Romania*, application no. 26713/05, delivered on 12th January 2016, the doctrinal interpretation of the obligations of the employee towards the employer with regards to use of the social networks indicates that in case, that the employee writes in the name of the employer on the social network, the employer can monitor the content and use the information as an evidence. It can further be deduced that in situation, when the employee writes defamatory or similarly infringing posts about his employer from his private profile using the employer's assets and the information is publicly available, he acts contrary to legitimate interest of employer and such action may constitute breach of the duty laid down, in case of Czech law, in particular in the above described Section 301 lit. d) of the Labour Code. The strength of these conclusions was, however, shaken by the Grand Chamber decision in the *Bărbulescu v Romania* case, application No. 26713/05, delivered on 5th September 2017, as the Grand Chamber

hoeren@uni-muenster.de

decided differently from the original decision, despite the fact that the main grounds for this deviation are not to be found in dismissal of the above stated conclusion, but rather in the procedural aspect of the insufficient depth of the analysis of the case carried out by the Romanian courts. In consequence, the question of permissibility of the information as evidence in disciplinary proceedings is currently not conclusively clarified.

2.3 *Personal Data Conveyed and Stored Through Electronic Means*

Sections 88–89 of the Electronic Communications Act lay down a general duty of providers of electronic communications to secure confidentiality of the electronic communications, including cases when personal data is conveyed.[12] However, there are no specific obligations for the confidentiality of messages containing personal data, which would differ from the messages, which do not contain personal data.[13] This can be seen as understandable, given the prohibition of general obligation to monitor content set down by Article 15 of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (eCommerce Directive) and implemented through Section 6 of the Act No. 480/2004 Sb., on Certain Information Society Services. This section reads as follows:

> The providers of services listed in Sections 3 to 5 are not obliged
>
> a) to monitor the content of information they convey or store,
> b) actively seek facts and circumstances indicating illegal content of the information.

From this follows that the provider is not obliged to be aware, if the content constitutes personal data, and shall not be legally bound to monitor for such quality of the content. Specific obligations related to this type of content would therefore contradict this framework of ISP liability.[14]

The Electronic Communications Act further contains obligation in Section 88 subsection 1, lit. c) for the undertaking providing publicly available electronic communications service to inform the subscribers concerned about the specific risk of the disturbance of network security in relation to data protection.[15] This provision is described in greater detail in the following chapter on Data protection in the electronic communications sector.

Apart from the above described, the Czech legal system currently does not contain any specific legislation or implemented self-regulation instruments on

[12] See in Czech: Chudomelová et al. (2016), pp. 290–298.

[13] See in Czech: Polčák et al. (2018), pp. 524–528.

[14] See in Czech: Maisner (2016), pp. 99–137.

[15] See in Czech: Chudomelová et al. (2016), pp. 290–293.

hoeren@uni-muenster.de

sectorial areas that have processing of personal data by electronic means as their core capacity. Despite of political or academic debate concerning specific regulation of home banking, unmanned aerial vehicles, mobile health, internet of things devices or artificial intelligence, there is as of now no draft of such legislation. This is generally in accordance with the concept of the Czech framework of personal data protection as being formulated in essentially technology neutral way.

3 Data Protection in the Electronic Communications Sector

In addition to the generally applicable GDPR, processing of personal data is regulated through specific provisions in the Electronic Communications Act and in the Act No. 480/2004 Sb. on Certain Information Society Services, which implement the Directive 2002/58/EC on privacy and electronic communications as amended through the Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. In the upcoming year 2019, it is expected that these provisions shall be replaced by the unified European specific legislation contained in the proposed Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), currently available in a form of the proposal COM/2017/010 final—2017/03 (COD).

As the Czech Republic is an EU Member State, the core case law concerning the specific issues of personal data protection in the electronic communication sector is originated by the Court of Justice of the European Union, in particular:

- case C-461/10, *Bonnier Audio AB et al. v Perfect Communication Sweden AB*;
- case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH*;
- case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*;
- joint cases C-293/12 and C-594/12, *Digital Rights Ireland*; or ¨
- joint cases C.203/15 and C-698/15, *Tele2 Sverige*.

On the national level, the most significant case law concerns the constitutional permissibility of data retention legal framework as formerly implemented pursuant to now invalid Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (for details, please refer to the decision of CJEU in joint cases C-293/12 and C-594/12, Digital Rights Ireland). This legal framework was brought into the Czech law by the Act

hoeren@uni-muenster.de

No. 247/2008 Sb., amending the Act No. 127/2005 Sb., on the Electronic Communications and the relevant provision of the Act No. 141/1961 Sb., Criminal Procedural Code. In the decision Pl. ÚS 24/10 (concerning the constitutional validity of the relevant provision of the Act No. 127/2005 Sb., on the Electronic Communications) and later in the decision Pl. ÚS 24/11 (concerning the constitutional validity of the relevant provision of the Act No. 141/1961 Sb., Criminal Procedural Code), the Czech Constitutional Court discussed at length the aspects of constitutional permissibility of data retention and invalidated the respective provisions implementing the form of data retention based on the Directive 2006/24/EC. The provisions were later replaced by provisions that took the conditions and requirements expressed in these judgements into consideration.

3.1 Definition of Entities Subject to Obligations and Core Terms

Subject to the specific obligations under the Electronic Communications Act is a legal entity or a natural person, who is an entrepreneur in electronic communications. Under the object of business in the electronic communications area is understood either the provision of public communications networks or the provision of electronic communications services (Section 8 Subsection 1 of the Electronic Communications Act).[16] The applicable law also operates with the term "*communications activities*" under which are understood: provision of electronic communications networks; provision of electronic communications services; and operation of apparatus (defined in Section 73 of the Electronic Communications Act).[17] Provision of public communications network, provision of publicly available electronic communications services and the provision of electronic communications networks for the purposes of the security of the State are regarded as of public interest.

Pursuant to the definition of the term in Section 2 lit. a) of the Act No. 480/2004 Sb. on Certain Information Society Services; "*information society service*" means any service provided through electronic means on individual request of the user delivered through electronic means, whereas the provision of the service is in principle remunerated.[18] A service is provided through electronic means, if it is delivered over the network for electronic communication and received by the user on an electronic device capable of data storage. The "*electronic means*", as used in the previous definition, are further specified in lit. c) of the same section; as in particular a network for electronic communication, electronic communication devices, automated call and communication systems, end-user telecommunication devices and electronic correspondence.[19]

[16]See in Czech: Vlachová (2016), pp. 28–31.

[17]See in Czech: Chudomelová et al. (2016), pp. 240–243.

[18]See in Czech: Maisner (2016), pp. 5–9.

[19]See in Czech: Maisner (2016), pp. 11–12.

hoeren@uni-muenster.de

The term "personal data" is understood in the context of the electronic communications sector pursuant to the general definition contained in Article 4 no. 1 of the GDPR as any information relating to an identified or identifiable natural person. The communications data are further specified as traffic data and location data.

Traffic data and location data are terms primarily used in the Electronic Communications Act. The respective definitions in Section 90 Subsection 1 and Section 91 Subsection 1 are in accordance with the definitions adopted in Article 2 Subsections b) and c) of the Directive 2002/58/EC on privacy and electronic communications, respectively.[20] Their wording is as follows:

> Section 90
>
> Traffic Data
>
> (1) Traffic data mean any data processed for the purposes of the transmission of a message via the electronic communications network or for the billing thereof.
>
> (. . .)
>
> Section 91
>
> Location Data
>
> (1) Location data mean any data that are processed within the electronic communications network and that define the geographical location of the terminal equipment of a user of publicly available electronic communications service.
>
> (. . .)

3.2 Specific Rules for the Electronic Communications Sector

One of the core values protected through the specific provisions contained in the above mentioned legislation is the confidentiality of communication data. The confidentiality obligations cover data transmitted via public communications network or the publicly available electronic communications services as well as related traffic and location data. Subject to these obligations are the respective providers of public communications networks or publicly available electronic communications services.

The following Section 89 of the Electronic Communications Act contains specific rules about confidentiality of communications data in accordance with the Directive 2002/58/EC on privacy and electronic communications:

> Section 89
> Confidentiality of Communications
>
> (1) The undertakings providing public communications networks or publicly available electronic communications services shall ensure the technical and organisational measures to safeguard the confidentiality of the messages and the related traffic and location

[20] See in Czech: Chudomelová et al. (2016), pp. 299–306.

hoeren@uni-muenster.de

data, which are transmitted via their public communications network and the publicly available electronic communications services. In particular, such undertakings shall not admit any wiretapping, message storage, or any other types of interception or monitoring of messages, including the data contained therein and related thereto, by any persons other than the users, without the consent of the users concerned, unless otherwise provided in laws [Section 88 of Act No. 141/1961 on criminal procedure (Code of Criminal Procedure), as subsequently amended.]. This shall not be to the prejudice of the technical storage of data as needed for message transmission without affecting the confidentiality principle.

(2) Message means any information being exchanged or transmitted between a finite number of subscribers or users via the publicly available electronic communications service, except for the information transmitted as part of the public audio or television broadcasting via the electronic communications network, unless it can be allocated to an identifiable subscriber or user receiving that information.

(3) Anybody wishing to use, or using, the electronic communications network for the storage of data or for gaining access to the data stored in the subscribers' or users' terminal equipment shall inform those subscribers or users beforehand in a provable manner about the extent and purpose of processing such data and shall offer them the option to refuse such processing. This obligation does not apply to activities relating to technical storage or access and serving exclusively for the purposes of performing or facilitating message transmission via the electronic communications network, nor does it apply to the cases where such technical storage or access activities are needed for the provision of an information society service explicitly requested by the subscriber or user.

(4) The undertakings providing public communications networks or publicly available electronic communications services shall upon request of the subscriber provide such subscriber free of charge and in a form allowing further electronic processing with the traffic and location data, which it has at its disposal following this law, if such subscriber was not able to intercept or storage such data pursuant to a device failure caused by a cyber security incident [as defined in the Section 7 Subsection 2 of the Act No. 181/2014 Sb. on the Cybersecurity and Change of Related Acts]. The undertaking shall transmit the data, if technically possible, without due delay, latest within three days following the delivery of the request or, in case of continuous communication, following the day of its realization.

The related aspect of electronic communications regulation, that to a certain degree ensures the protection of confidentiality of the communications data, is the requirement for adequate security measures to be implemented by the electronic communications providers in order to protect transmitted data, and obligations in case of risk of a breach of data security. The specific legal rules include obligation to implement adequate technical and organisational measures to protect personal data as well as traffic and location data and the confidentiality of the communication and obligation to prepare internal technical and organisational regulations to provide data protection and communications confidentiality.

The following Sections 88 and 88a of the Electronic Communications Act contain specific rules about the implementation of security measures by electronic communications providers in order to protect personal data including traffic and location data, and obligations in case of risk of a breach of security in accordance with the implementation of the Directive 2002/58/EC on privacy and electronic communications:

hoeren@uni-muenster.de

> Section 88
>
> Securing the Protection of Personal, Traffic and Location Data and the Confidentiality of Communications
>
> (1) The undertaking providing publicly available electronic communications service is obliged to:
>
> a) take technical and organisational measures to safeguard the security of the service in respect of the protection of natural persons' personal information in accordance with a special legal regulation [currently referring to the respective unified obligations pursuant to the GDPR], protection of the traffic and location data, and confidentiality of the communications of natural persons and legal entities in providing the service; if necessary, the provider concerned shall upon written agreement also co-operate with the undertaking providing the communications network to provide the protection,
>
> b) prepare internal technical and organisational regulations to provide data protection and communications confidentiality in accordance with Clause a) above; secure data protection and communications confidentiality with respect to the existing technical capabilities and the costs needed to provide protection at a level adequate to the risks of compromising the protection,
>
> (. . .)
>
> Section 88a
>
> (1) The undertakings providing public communications networks or publicly available electronic communications services shall secure that the traffic and location data collected pursuant to Section 97 Subsection 3 have equal quality and underlay equal security and protection from unauthorized access, modification, deletion, loss or theft or other unauthorized processing or use as do the data pursuant to Section 88; this provision does not preclude obligations under special legal regulation [currently referring to the respective unified obligations pursuant to the GDPR].
>
> (2) The undertakings providing public communications networks or publicly available electronic communications services shall prepare an internal technical and organisational regulation in order to assure the protection of the data pursuant to the Subsection 1; data protection shall be secured with respect to the existing technical capabilities and the costs needed to provide protection at a level adequate to the risks of compromising the protection. For the protection of data under this provision shall accordingly apply the provisions in Section 88 Subsections 2 to 7.

Further obligation can be derived from Section 88 subsection 1, lit. c) of the Electronic Communications Act. It lays down that the undertaking providing publicly available electronic communications service is obliged to inform the subscribers about the specific risk of the disturbance of network security in relation to data protection. If the risk is beyond the scope of the measures taken by the undertaking providing publicly available electronic communications service, the undertaking shall also inform the subscribers about all the possible ways of remedying the situation, including the costs associated therewith.[21] Pursuant to the technical provisions contained in the Regulation (EU) 611/2013 on the notification of personal data breaches in the electronic communication sector (Regulation 611/2013), such

[21] See in Czech: Chudomelová et al. (2016), pp. 290–293.

hoeren@uni-muenster.de

notification must be made without undue delay, no later than 24 h after the detection of the personal data breach. The Regulation 611/2013 further specifies uniformly for all EU member states in particular the circumstances to be taken into account when assessing whether there is a likely adverse effect, which constitutes the obligation to notify. Such circumstances are, namely, the nature and content of the personal data concerned; the likely consequences of the breach; and the circumstances of the breach.

The following subsections of the Section 88 of the Electronic Communications Act contain specific rules about data breaches in accordance with the implementation of the Directive 2002/58/EC on privacy and electronic communications:

> Section 88
>
> Securing the Protection of Personal, Traffic and Location Data and the Confidentiality of Communications
>
> (1) The undertaking providing publicly available electronic communications service is obliged to:
>
> (. . .)
>
> c) inform the subscribers concerned about the specific risk of the disturbance of network security in relation to data protection in accordance with Clause a) above, and if the risk is beyond the scope of the measures taken by the undertaking providing publicly available electronic communications service, the undertaking shall also inform the subscribers about all the possible ways of remedying the situation, including the costs associated therewith.
>
> (. . .)
>
> (4) In the event a breach of security occurs concerning the personal data of a natural person, the undertaking providing a publicly available electronic communications service is obliged to notify the Office for Personal Data Protection of this fact without undue delay. This notification shall contain a description of the outcome of the breach of security and the technical protection measures the undertaking has adopted or proposes adopting.
>
> (5) In the event the breach of security concerning a user's personal data pursuant to Subsection 4 above may affect the privacy of a natural person in a particularly serious manner, or if the undertaking providing a publicly available electronic communications service has failed to adopt measures that would remedy this situation and which would be sufficient to protect the personal data at risk in accordance with the assessment made by the Office for Personal Data Protection, it shall also notify the natural person concerned and the Office for Personal Data Protection. In this notification, the undertaking shall describe the nature of the breach of security concerning personal data, a recommendation to carry out interventions to mitigate the impact of the breach of security concerning personal data and a contact information site.
>
> (6) After investigating the situation that has occurred after the breach of security pursuant to Subsection 4, the Office for Personal Data Protection is entitled to impose on the undertaking providing a publicly available electronic communications service an obligation to inform the natural person affected of the breach of security regarding his data, if it has not already done so itself.
>
> (7) An undertaking providing a publicly available electronic communications service shall make a summary of breaches of security concerning personal data, including information on the circumstances of the breach, its impact and measures adopted to remedy the situation, only for the purposes of the investigation into compliance with its obligations, in accordance

hoeren@uni-muenster.de

> with Subsections 4 and 5. An implementing legal regulation may lay down more detailed conditions under which an undertaking providing a publicly available electronic communications service is obliged to notify any breach of personal data protection, the format of such a notification and the manner in which the notification is to be made.

Concerning the personal data breach reporting, electronic communication services were until recently the only area, where such obligation was established on the European harmonized level. Since May 2018 it was complemented by general mandatory personal data breach notification and communication obligations contained in Articles 33 and 34 of the GDPR respectively. Pursuant to these provisions, the data controller shall notify the personal data breach to the competent data protection authority without undue delay and, where feasible, not later than 72 h after having become aware of it.

However, as the specific notification obligation for undertakings providing publicly available electronic communications service pursuant to Section 88 of the Electronic Communications Act lays down stricter requirements than the general personal data breach notification obligation pursuant to Article 33 of the GDPR, and as the supervisory authority to which such notification shall be made is in the Czech Republic in both cases the Office for Personal Data Protection, the specific notification obligation absorbs the general notification obligation with regard to these specifically obliged undertakings.

The similarity between the concept of personal data breach notification for the electronic communication sector and the general personal data breach notification contained in the GDPR can be mostly traced to the fact, that the specific provisions for the electronic communication sector presented a template later adapted during the preparation of the GDPR.

To complete the description of relevant notification obligations of entities operating in the electronic communications sector, the duty to inform about cyber security incidents pursuant to Act No. 181/2014 Sb., on Cybersecurity (Act on Cybersecurity) shall be shortly introduced. The obligations relevant to operators of electronic communications pursuant to the Act on Cybersecurity depend on their classification. Such entity may either be a controller or operator of communication system included in the critical information infrastructure[22] (Section 3 lit. d) of the Act on Cybersecurity); or, in case that the Section 3 lit. d) is not applicable, an entity securing an important network[23] (Section 3 lit. b) of the Act on Cybersecurity); or a provider of electronic communications service or an entity securing a network for

[22]Pursuant to Section 2 lit. b) of the Act on Cybersecurity, "*critical information infrastructure*" is to be perceived as an element or system of elements of the critical infrastructure in the communication and information systems sector in the field of cybernetic security (as classified pursuant to the Section 2 of the Act No. 240/2000 Sb., on Crisis Management and Amendment of Certain Acts in in the Governmental Regulation No. 432/2010 Sb., on Criteria for Classification of an Element of the Critical Infrastructure).

[23]Pursuant to Section 2 lit. h) of the Act on Cybersecurity, "*important network*" means an electronic communications network securing a direct connection of the public communication networks with abroad or securing direct connection to the critical information infrastructure.

hoeren@uni-muenster.de

electronic communications, if neither lit. d), nor lit. b) of the Section 3 is applicable (Section 3 lit. a) of the Act on Cybersecurity).[24]

If an entity operating in electronic communications sector is classified as either the first or the second above described category, it is subject to specific notification obligation pursuant to Section 8 of the Act on Cybersecurity. This provision states that such entities are obliged to report cyber security incidents[25] without undue delay after their detection. In case of classification as an entity operating an important network (Section 3 lit. b) of the Act on Cybersecurity), such incident is reported to the administrator of the national CERT.[26] In case of a controller or an operator of communication system included in the critical information infrastructure (Section 3 lit. d) of the Act on Cybersecurity), such notification is made to the National Office for Cybersecurity and Information Security (govCERT).

The aforementioned data breaches must be reported regardless of presence or absence of personal data in the breached dataset. However, this obligation of notification is without prejudice to any other duty to report data breaches. That means that entities obliged to notify data breach to CERT unit are, in case that such breach affected the processed personal data, also obliged to notify the Czech Office for the Protection of Personal Data as data controllers, either pursuant to Article 33 of the GDPR or, in case of undertakings providing publicly available electronic communications service, pursuant to Section 88 Subsection 4 of the Electronic Communications Act.

3.3 Supervision of the Personal Data Processing in the Electronic Communication Sector

As implies from Section 87 Subsection 3 of the Electronic Communications Act, supervision over compliance with the obligations in processing personal data in the electronic communications sector is provided by the Czech Office for the Protection of Personal Data in accordance with Act No. 101/2000 Sb., on the Protection of Personal Data and on Amendment to Some Acts.[27] For future reference, the provisions regarding the competent data protection authority in the Czech data

[24]See in Czech: Maisner and Vlachová (2015), pp. 74–76.

[25]Pursuant to Section 7 Subsection 2 of the Act on Cybersecurity, "cybernetic security incident" is defined as a breach of the security of the information in the information systems or a breach of security of the services or of the security and integrity of the electronic communications networks due to cybernetic security event. "Cybernetic security event" means, pursuant to Section 7 Subsection 1 of the Act on Cybersecurity, an event, which may cause a breach of security of the information in the information systems or a breach of security of the services or of the security and integrity of the electronic communications networks.

[26]The national CERT is currently administered by the Czech domain name authority CZ.NIC.

[27]See in Czech: Chudomelová et al. (2016), pp. 287–290.

hoeren@uni-muenster.de

protection legal framework shall be contained in the upcoming new Czech Personal Data Processing Act.

Providers of services of electronic communications are at the same time in most other aspects under the administrative jurisdiction of the Czech Telecommunications Office.[28] This supervisory body may become involved in the control of the processing of personal data in the context of electronic communications due to its supervisory activity on the technical level, *e.g.* in case of wiretapping, as well as with regard to the security and integrity of the provided publicly available electronic communications services and public communications networks.

Data protection in the electronic communications sector is, however, as indicated above, within the jurisdiction of the data protection authority, the Czech Office for the Protection of Personal Data. Pursuant to the above described specific legislation enshrined in the Electronic Communications Act is this supervisory body vested with additional sanctioning powers for personal data processing in the electronic communications sector, contained in the following excerpts of the Section 118:

> Administrative Offences
>
> Section 118
>
> (14) The undertaking providing public communications networks or publicly available electronic communications services commits administrative offence if it:
>
> (. . .)
>
> k) endangers the confidentiality of messages and the associated traffic and location data by breaching an obligation under Section 89 Subsection 1, or Section 91 Subsections 2, 3 or 4;
>
> (. . .)
>
> *(15)* The undertakings providing public communications networks or publicly available electronic communications services shall further commit an administrative offence by failing to fulfil any obligation for securing personal data protection pursuant to Section § 88a Subsections 1 or 2.
>
> (. . .)
>
> (22) For an administrative offence referred to in Section 118 shall the imposed fine be up to
>
> (. . .)
>
> b) CZK 10,000,000, in cases of administrative offence referred to in Subsection 1 Clause m), Subsection 2 Clauses c) to e), Subsection 3 Clause a), Subsection 8 Clause d) to m), Subsection 10 Clauses j) to r), Subsection 12 Clauses f) to o), Subsection 13 Clauses i) to m), Subsection 14 Clauses k) to ad) or Subsection 15,
>
> (. . .)

The presented specific provision on administrative sanctions with regard to the personal data processing in the electronic communications sector needs to be, however, perceived in light of the general supervisory capacity and the respective

[28]English website of the Czech Telecommunications Office can be found under https://www.ctu.eu.

hoeren@uni-muenster.de

sanctioning powers of the Office for Protection of Personal Data pursuant to the provisions contained in Article 83 and 84 of the GDPR.

4 Data Protection and Digital Forensics

The regulatory substance of the draft Personal Data Processing Act (see above) is divided into three parts. The first part covers national legal harmonisation with General Data Protection Regulation. The second part implements the Police Directive[29] and the third part stipulates general data protection framework for areas which are outside of the scope of the EU law like security, intelligence or defence. Specific rules for processing of personal data in criminal procedure are laid down in Act No. 141/1961 Sb. Code of Criminal Procedure.

The Code of Criminal Procedure is a dated act that has been amended numerous times. Nevertheless, up until today, there are no specific provisions on access to data and their use. Therefore, the police, state prosecutors and other law enforcement authorities ("LEA") must rely on legal instruments which were originally used for different purposes (*e.g.* seizure of assets). A common framework for accessing and collecting digital evidence was established only after several years of interpretation process of these rules by different institutions. Apart from court decisions, the most influential document is Opinion No. 1/2015 of the Supreme Public Prosecutors Office,[30] which unified processes of accessing and collecting digital evidence.

There are several provisions in the Code of Criminal Procedure that allow LEA to collect and access digital evidence. These provisions contain both substantive and formal prerequisites of the collection. The digital evidence may be basically divided into three categories: i) data that are stored in computer systems or storage devices that can be seized (hard drives, flash drives, mobile phones, computers, and similar); ii) data that are can be accessed via networks; and iii) data that are transferred as telecommunication traffic.

The computer systems and storage devices may be seized following provisions on Seizure of property (section 79 of the Code of Criminal Procedure) or during a house or personal searches (section 82 of the Code of Criminal Procedure). Section 79 of the Code of Criminal Procedure reads as follows (informal translation from ASPI system):

§ 79 Seizure of Property

[29]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework.

[30]In Czech online: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

hoeren@uni-muenster.de

(1) If the tangible property important to the criminal proceedings is not released when those who have it in their possession are prompted, it may be removed from their possession on the warrant of the presiding judge, and in preliminary hearing, the public prosecutor or police authority. The police authority needs to have the prior approval of the public prosecutor for the issue of such warrant.
(2) If the authority that issued the warrant for the seizure of the tangible property does not seize such property themselves, the police authority shall do so on the basis of the warrant.
(3) Without the prior consent referred to in Subsection 1 the warrant may be issued by the police authority only if prior approval cannot be achieved and the matter cannot be delayed.
(4) A person who is not involved in the matter shall take part in seizing the tangible property.
(5) The transcript of the release and seizure of the tangible property must also contain a sufficiently accurate description of the released or seized property that would make it possible to determine its identity.
(6) The authority that performed the action shall immediately issue a written confirmation of the receipt of the property or a copy of the transcript to the person who released the tangible property or from whom the tangible property was removed, together with a written instruction that they must not transfer the released or removed tangible property to another party or encumber it and that any legal action made contrary to such prohibition is invalid.
(7) Removed tangible property that was not taken into custody by a law enforcement authority in order to take evidence shall be governed accordingly by Section 78 Subsection 4 through 8.

A lawful seizure of property is conditioned by prior approval of the public prosecutor.[31] Data stored in seized devices can be accessed and used as evidence without further consent from the judge or public prosecutor. There is currently ongoing a discussion, whether the law enforcement authorities can also seize sole data following provisions in section 79 of the Code of Criminal Procedure, but there is no conclusive case-law on that mater.[32]

The Code of Criminal Procedure does not contain any specific provisions which would allow LEA to access the digital evidence which is stored in cloud services or computer systems connected to the network. Therefore, LEA must follow procedures defined in more general provisions. As was stated in the Opinion of the Supreme Public Prosecutors Office No. 1/2015, for this purpose, it is applicable procedure mentioned in the section 158d of the Code of Criminal Procedure that covers the Surveillance of Persons and Items (informal translation from ASPI system):

§ 158d Surveillance of Persons and Items

(1) The surveillance of persons and items (hereinafter referred to as "surveillance") means acquiring knowledge about persons and items performed in a classified manner by technical or other means. If the police authority finds during the surveillance that the

[31] In a case of a house search, there must be issued a previous warrant by a judge. For more information see in Czech: Šámal (2013), pp. 1111–1120.

[32] See in Czech *e.g.* Polčák et al. (2015), pp. 100–115: Hlaváčová and Chorvát (2016), pp. 3–24.

hoeren@uni-muenster.de

accused communicates with their defence counsel, they are required to immediately destroy the records with the content of the communication, and the information that they learned in this context they are not allowed to use in any way.

(2) Surveillance during which audio, video or other records are to be obtained may be performed only upon the written authorisation of the public prosecutor.

(3) If the surveillance is to interfere with in the inviolability of residence, the confidentiality of correspondence, or finding the contents of other documents and records kept in private with the use of technology, then it may be performed only with the prior authorisation of a judge. When entering a residence, no actions other than those that lead to the planting of technical equipment can be performed.

(4) The authorisation referred to in Subsection 2 and 3 can only be issued upon written request. The request must be justified by a suspicion of specific criminal activity and, if known, with the information about the persons or items that are to be surveilled. The authorisation must state the period during which the surveillance will be carried out and this must not be longer than six months. This period may be extended by those who authorised it on the basis of a new written request, but still not exceeding six months.

(5) If the matter cannot be delayed and it is not a case referred to in Subsection 3, the surveillance may be initiated even without prior authorisation. However, the police authority is obliged to additionally request the authorisation without undue delay and if it is not received within 48 hours they are required to cease the surveillance, destroy any records, and not to use any information found in this context.

(6) Without compliance with the conditions referred to in Subsection 2 and 3, the surveillance may be performed only if the person whose rights and freedoms are to be interfered with by surveillance gives their express consent. If such consent is subsequently withdrawn, surveillance shall immediately terminate.

(7) If the record of the surveillance is to be used as evidence, it is required that the transcript is attached with the particulars referred to in Section 55 and 55a.

(8) If no facts important to the criminal proceedings were found, it is necessary to destroy the records in the prescribed manner.

(9) Operators of telecommunications activity, their employees, and other persons who participate in the operation of telecommunications activity, as well as the post office or the person performing the transport of the consignments are obligated to provide the police authority performing the surveillance with the necessary assistance free of charge and in accordance with their instructions. At the same time, they may not claim the obligation of professional confidentiality imposed by special Acts.

(10) In a criminal matter other than that which the surveillance was performed for under the conditions referred to in Subsection 2, the records obtained through surveillance and the attached transcript may be used as evidence only if there is, in this case, a pending criminal proceeding on an intentional criminal offence or if the person whose rights and freedoms the surveillance interfered with, gives their consent.

It allows LEA to acquire knowledge about persons and items, including "*records kept in private*", in a classified manner by technical or other means.[33] Therefore, this provision allows LEA to access and store online data in a clandestine way. The stored data can be accessed during investigation of any crime, but only with written authorisation of the public prosecutor.

Additionally, if the data is considered to be "kept in private", which is essentially any data stored in private computer systems and storage devices or cloud environ-

[33]For more detailed explanation in Czech see Šámal (2013), pp. 2006–2007.

hoeren@uni-muenster.de

ments, prior authorisation of a judge is required,[34] unless the person whose rights and freedoms are to be interfered with gives their express consent.[35] However, there might arise a problem with future investigation in such cases, because the withdrawal of the consent will result in immediate discontinuation of the surveillance and access to data. Furthermore, authorisation of the judge allowing the surveillance of the content covers only access to the data that was stored before the first access.

A different situation is in the cases when access to "in-traffic data" is necessary. Examples of such data are emails and other data that are received thanks to the automatic synchronisation after the device is seized, or a data which are added to the cloud storage after the police gained access to it. In such cases, LEA must follow a procedure defined in Section 88 of the Criminal procedure code, which deals with interception and recording of telecommunications.[36] Apart from that, if LEA need access to the traffic and location data held by electronic communication service providers (so-called "data retention"), they must follow another specific provision—section 88a of the Code of Criminal Procedure.[37]

Finally, in cases, when none of the abovementioned provisions is applicable, LEA can try to get the data through the application of a general provision covering obligation of cooperation with public authorities in criminal investigation. Section 8 subsection 5 of the Code of Criminal Procedure states that in situations when there is not applicable any special law, information may be requested for criminal proceedings upon the prior consent of the judge. Example of such information might be location and traffic data held by other persons than electronic communication service providers. For example, information service providers can have and often do have information which would, by their nature, fall within a definition of location and traffic data, but proceedings following section 88a of the Code of Criminal Procedure in such cases cannot apply, because it is by its scope limited to electronic communication service providers.

4.1 Interception of Communication Data

In the Czech Republic, interception of communication is seen as a serious breach of protection of the right to privacy.[38] Therefore, the law contains relatively rigorous

[34]See section 158d, subsection 3 of the Code of Criminal Procedure.

[35]See section 158d, subsection 6 of the Code of Criminal Procedure. Should the collected data be used as an evidence during the criminal proceedings, a proper protocol should be prepared, which contains an information how the access was granted as well as the written consent of the person. The Constitutional Court confirmed this approach in its decision No. III. ÚS 3844/13.

[36]See in Czech: Polčák et al. (2015), pp. 121–137.

[37]Both interception of electronic communication and data retention is discussed in more detail bellow.

[38]See *e.g.* decision of Czech Constitutional Court No. II. ÚS 502/2000, followed by Decision No. II. ÚS 615/06-1 in which the Court formulated and interpreted necessary conditions for

hoeren@uni-muenster.de

provisions on wiretapping and similar investigative activities. The Code of Criminal Procedure in its section 88 allows interceptions of communication once the criminal proceedings have started and only when it is done for investigation of a "crime for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, for a criminal offence of machinations in insolvency proceedings, violation of regulations on rules of competition under, negotiating advantages during public procurement, tender and auction, machinations during public procurement and tenders, machinations at a public auction, misuse of powers of an official person or . . . any other intentional criminal offence for which prosecution is stipulated in a declared international treaty". The strict nature of this exception was confirmed by the Constitutional Court in decision No. II. ÚS 615/06 in which the court stated (paras 13–16):

> The right to protection of the secrecy of messages arising from Art. 13 of the Charter of Fundamental Rights and Freedoms, together with personal freedom and other constitutionally guaranteed fundamental rights, comprises the personal sphere of an individual, whose individual integrity, as an essential condition for a dignified existence and the development of human life generally, must be respected and thoroughly protected as a token of respect for the rights and freedoms of people and citizens.
>
> If the constitutional order permits a breach of this protection, it does so solely and exclusively in the interests of a democratic society, or in the interest of the constitutionally guaranteed fundamental rights and freedoms of others. . . . Therefore, there may be only such infringement of the fundamental rights and freedoms by the state power, which is necessary for this sense.
>
> It should be emphasised that an effective judicial review of the use of any operative means, with an overlap into the area of fundamental rights and freedoms, is absolutely crucial to a fair trial in criminal proceedings.[39]
>
> In terms of the constitutional order, a violation of the secrecy of messages is possible only in cases and manner prescribed by law. Statutory regulation interfering with this right must be formulated so that it does not deny this fundamental human right and it must also be interpreted this way. . . . A court order for interception and recording of telecommunication operations must be written and reasoned. It must therefore be issued in respect to a person against whom criminal proceeding is conducted. If the proceedings are conducted on the basis of reasonable suspicion, it must be explained in a recital what evidence supports such conclusion. The mere criminal complaint itself, if it does not include explanation, is not sufficient for court order. . . . The order may therefore be issued only in duly commenced criminal proceedings for a legally qualified crime, and must be supported by relevant clues from which we can derive a reasonable suspicion of committing such a crime. The order must be individualized in a relation to the specific person who is the user of intercepted telephone device. . . . Finally, the order must provide at least a minimal indication of what facts relevant for the proceeding are to be thus identified, and what is inferred from that.

The object of interception is broadly specified as "telecommunications traffic". Neither legislature nor case law defines this term. Traditionally, this term means

allowing the interception. See also Interception of electronic communications in the Polčák et al. (2016) and Wagnerová (2012).

[39] *Ibidem*, para. 15.

hoeren@uni-muenster.de

communication between persons via landlines, mobile phones, fax, radio or similar devices. However, thanks to the technological development, the interpretation of this term evolves. Nowadays it covers all sorts of communication transferred via telecommunications and electronic communications networks including communication between computers or other communication devices, as well as any kind of IP traffic regardless of whether it was generated by persons or computers. Even content data transferred while surfing the web via electronic communications networks may be an object of interception.

When defining the term "telecommunications traffic", literature usually refers to the Act on electronic communications.[40] This act itself doesn't contain definition of the term, but we may understand it as content transferred via electronic communications networks, which are defined by the act as transmission systems and, where applicable, switching or routing equipment and other facilities, including network elements which are inactive, and which permit the conveyance of signals.[41] Furthermore, section 89 of the Act on electronic communications, which deals with the confidentiality of communication, provides a helpful hint of what telecommunications traffic means. It reads as follows:

> §89 Confidentiality of Communication
>
> (1) Undertakings providing a public communications network or a publicly available electronic communications service shall implement technical and organisational measures to safeguard the confidentiality of the messages and the related traffic and location data, which are transmitted via their public communications network and the publicly available electronic communications services. In particular, such undertakings shall not admit any tapping, message storage, or any other types of interception or monitoring of messages, including the data contained therein and related thereto, by any persons other than the users, without the consent of the users concerned, unless otherwise provided in an Act. This shall not be to the prejudice of the technical storage of data as needed for message transmission without affecting the confidentiality principle.
> (2) A message means any information being exchanged or transmitted between a finite number of subscribers or users via the publicly available electronic communications service, except for the information transmitted as part of the public radio or television broadcasting service via the electronic communications network, unless it can be allocated to an identifiable subscriber or user receiving that information.

Interception of electronic communications may be conducted only after an interception order is issued. The interception order is a decision *sui generis*, for which can apply in preliminary proceedings only a public prosecutor, usually after a consultation with respective police investigator.[42] Before applying, the public prosecutor usually verifies whether the criminal proceedings are conducted for a crime, for which the interception can be ordered. The public prosecutor particularly

[40]For example, see Šámal (2013).

[41]Section 2 letter h) of the Act no. 127/2005 Sb., on electronic communications.

[42]Opinion No. 1/2018 of the Supreme Public Prosecutors Office elaborated more on the necessary requirements of interception request. It focuses heavily on the required argumentation of the request, so it cannot be too general or blank. See in Czech online: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2018/1_SL_719-2017.pdf.

hoeren@uni-muenster.de

assesses whether the offence described in the record of the commencement of the criminal proceeding or in the resolution to initiate the criminal prosecution corresponds with respective legal classification. The prosecutor also assesses whether it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained during the interception if there is no other way to achieve such purpose or if its achievement would be otherwise significantly reduced. A reasoned application is then presented to a judge, who can authorise the interception by issuing an order, according to Section 88 subsection 2 of the Code of Criminal Procedure that reads as follows (informal translation from ASPI system):

> The presiding judge and, in preliminary proceedings upon the petition of the public prosecutor, the judge, is entitled to warrant the interception and recording of telecommunications. [. . .] The order for the interception and recording of telecommunications shall immediately be forwarded to the police authority. In the preliminary hearing, the judge shall send a copy of the order for the interception and recording of telecommunications to the public prosecutor without undue delay.

This procedure is described in more detail in Section 32 subsection 2 of the instruction of the Ministry of Justice ref. No. 505/2001-Org as follows:

> The judge shall decide on the application of the public prosecutor for interception and recording of telecommunications traffic in accordance with section 88 para. 2 of the Code of Criminal procedure (hereinafter "interception") without delay or within the period agreed with the public prosecutor; on the proposal of the public prosecutor to extend duration of the interception (section 88 para. 4 of the Code of Criminal Procedure) will the judge decide no later than the last working day before the expiry of the previously issued interception order, if the public prosecutor filed the proposal at least 3 working days before expiry of the interception order.

An order is then forwarded to the investigator and the Unit for Special Activities, which carries out the interception.[43]

The maximum length of an interception order is 4 months. Based on the assessment of the current course of the interception, the judge of a superior court and, in a preliminary hearing upon a petition of the public prosecutor, deputy county court judge may extend the duration of the interception even repeatedly, however, always only for a maximum period of 4 months.

Basic formal requirements for interception orders are defined in section 88 para. 2 of the Code of Criminal Proceedings that reads as follows:

> The order for the interception and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the justification of the order must include the specific facts that justify the issuance of such order as well as its period. [. . .]

An order for interception or recording of telecommunications may be issued if it may be reasonably assumed that facts relevant to the criminal proceedings will be

[43]Unit for Special Activities of Criminal Police and Investigation is a Police division divisions with a countrywide authority which assists other police divisions as well as other authorities like *e.g.* Customs service. It conducts all interception and surveillance operations.

hoeren@uni-muenster.de

obtained in this way and if there is no other way to achieve such purpose or if its achievement would be otherwise significantly reduced. The investigator, the public prosecutor and most importantly the judge should, therefore, consider whether the evidence relevant for criminal proceedings cannot be obtained by other less intrusive means of investigation referred to in the Code of Criminal Procedure. This approach is based upon basic principles of criminal proceedings defined in the section 2 of the Code of Criminal Procedure, especially on the principle of proportionality and principle of moderation formulated in the Section 2 subsection 4 as follows:

> [. . .] Criminal cases shall be dealt with a full investigation of rights and freedoms guaranteed by the Charter of Fundamental Rights and Freedoms and by international treaties on human rights and fundamental freedoms that the Czech Republic is bound by; when conducting acts of criminal proceedings, the rights of persons that such acts affect may be intervened only when justified by law and to the extent necessary to ensure the purpose of criminal proceedings. [. . .]

The Constitutional Court was dealing with formal requirements of interception orders in decision No. II. ÚS 615/06 mentioned above.

There are a few rules that protect data subjects affected by an interception. Firstly, the communication between the defence counsel and the accused should be excluded from the interception. Such communication is generally inadmissible in criminal proceedings, and if the police authority finds during the interception that the accused has communicated with his or her defence counsel, they are obliged to immediately destroy the interception record and not to use the acquired information in any way.[44] These rules are in some sources deemed rather problematic. The reason is that most interceptions are conducted before the commencement of the criminal prosecution, and in this stage, the person against whom the criminal proceedings are conducted is not regarded as the accused. Therefore, *stricto sensu* interpretation of the provision would mean, that before the commencement of the criminal prosecution, the police would be able to access and use even the communication between the person against whom the criminal proceedings are conducted and her attorney. Some sources see this as a disproportionate breach of the right for a fair trial.[45]

In any case, the protection of the communication between the defence counsel and the accused is not absolute. In particular, when the communication relates to a crime, which is committed by the defence counsel in cooperation with the accused, then the protection does not apply. This approach is supported in the decision of Constitutional Court No. I. ÚS 1638/14, which states[46]:

[44]Section 88 subsection 1 of the Act no. 141/1961 Sb., the Code of Criminal Procedure. See commentary in Czech Šámal (2013), pp. 1192–1206.

[45]For example, in Czech see Vantuch, 2008, no. 10, p. 29.

[46]Para. 25 of the decision no. I. ÚS 1638/14. Provided excerpt translated by the authors. This approach was followed later by Opinion No. 1/2018 of the Supreme Public Prosecutors Office. See in Czech online: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2018/1_SL_719-2017.pdf.

hoeren@uni-muenster.de

> [. . .] However, as is clear from the case law of the European Court of Human Rights and of the Supreme Court, the protection of communication between solicitor and his client is not absolute, inviolable and under certain circumstances may be limited. Possible criminal activity of the solicitor, both to the detriment of the client or to the detriment of others in complicity with the client, can't be considered as the provision of legal services, and in such a case it is impossible to provide any protection of such activity. [. . .]

Secondly, the data subject has a right to be informed of the interception. The public prosecutor or the police authority, by whose decision the case was finally concluded, or the presiding judge in the first instance after the final conclusion of the matter, shall inform the affected person, if known, on the ordered interception.[47] As is clarified in Opinion No. 1/2018 of the Supreme Public Prosecutors Office, this information should be delivered as a separate announcement, which must be served directly to the hands of the intercepted person.[48] The information should include the designation of the court that issued the order for the interception and recording of telecommunications service, the duration of the interception and the date of the conclusion. The information about the interception is not provided to the affected person in cases when criminal proceedings are conducted for specific crimes, the criminal offence involved more people, and in relation to at least one of them the criminal proceedings have not yet been finally concluded, or when it could lead to threats to national security, life, health, or the rights and freedoms of individuals.[49]

The affected person may afterwards file a petition to review the legality of the order for the interception and recording of telecommunications service to the Supreme Court.[50]

In a case when the data subject provides his or her consent prior to the interception, the interception may also be conducted without a court order. This is however limited to several criminal offences such as human trafficking, unlawful delegation of custody of a child to someone else, restriction of personal freedoms, extortion, kidnapping of a child and persons suffering from a mental disorder, violence against a group of people or an individual, dangerous threats, or dangerous persecution.[51] This approach can be problematic because it infringes telecommunications secrecy of the other party to the communication who did not provide for the consent. For that reason the Supreme Public Prosecutor included in the General Instruction No. 8/2009 the rule that the public prosecutor must assess the suitability and legality of an interception order issued by the police without a proper court order.[52]

Finally, Opinion No. 1/2018 of the Supreme Public Prosecutors Office brought an interesting limitation following principle of data minimisation. It states that public

[47] Section 88 subsection 8 of the Act no. 141/1961 Sb., the Code of Criminal Procedure.

[48] See in Czech: Opinion No. 1/2018 of the Supreme Public Prosecutors Office, online: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2018/1_SL_719-2017.pdf.

[49] See Section 88 subsection 9 of the Act no. 141/1961 Sb., the Code of Criminal Procedure.

[50] Section 88 subsection 8 of the Act no. 141/1961 Sb., the Code of Criminal Procedure.

[51] See Section 88 subsection 5 of the Act no. 141/1961 Sb., the Code of Criminal Procedure.

[52] Section 45 of the General Instruction of the Supreme Public Prosecutor no. 8/2009, on criminal proceedings.

hoeren@uni-muenster.de

prosecutor should control that originals of the telecommunication interception are being kept outside of the prosecution file. Only parts of the communication that are relevant as evidence should be present in the file.

4.2 Data Retention

A legal regulation of collection and storage of location and traffic metadata for further criminal investigation and other uses is present both in the Act on Electronic Communications, where is set a duty for electronic communication service providers to store the data and to provide the data to the Police or other LEA, as well as in the Code of Criminal Procedure, where is enacted the power of LEA to request such data. The full-scale data retention framework was introduced in 2005 as a part of the act No. 127/2005 Sb., on electronic communications. Subsequently, the old wording was abolished by the Constitutional court[53] and consequently re-enacted in a constitution conformal way.[54] Recent Section 97 para. 3 of the Act on Electronic Communications states that electronic communication service providers have to retain for 6 months traffic and location data which are created or processed during the operation of their public communications networks and during the provision of their publicly available electronic communications services. Section 97 subsection 4 of the Act on Electronic Communications defines traffic and location data as follows:

> The traffic and location data pursuant to Subsection 3 above are primarily data leading to the tracing and identification of the source and address of the communication, and also data leading to the identification of the date, time, method and duration of the communication.

More detailed list of categories of data that are to be retained is in section 3 of the decree no. 357/2012 Sb., on storing, handing over and liquidation of traffic and location data, which is not available in English.

After 6 months, the data must be deleted, unless a special act states otherwise. Data relating to an unsuccessful call attempts do not need to be stored, unless these data are created or processed and at the same time stored or recorded. Furthermore, electronic communication service providers must make sure that any content data are not stored as well.

The same provision gives a list of public authorities which can request access to such data. It reads as follows:

- criminal law enforcement authorities for the purposes of and under the conditions laid down in special legal regulation,

[53]Decision of the Constitutional Court No. Pl. ÚS 24/10, 94/2011 Sb., N 52/60 SbNU 625. English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=c574142df486769e0b435954fead08c3.

[54]See Myška (2013), pp. 267–285.

hoeren@uni-muenster.de

- the Police of the Czech Republic for the purposes of initiating a search for a specific wanted or missing person, for the identification of persons of unknown identity or the identity of a corpse that has been discovered, for the prevention or detection of specific terrorist threats or for the verification of a protected person, while complying with the conditions set out in a special legal regulation,
- the Security Information Service, for the purposes of and under the conditions laid down in a special legal regulation,
- the Military Intelligence service for the purposes of and under the conditions laid down in a special legal regulation,
- the Czech National Bank for the purposes of and under the conditions laid down in a special legal regulation.

Conditions for the access of law enforcement authorities to retained data are formulated in § 88a of Code of Criminal Procedure. This provision specifies types of criminal offences for which the retained traffic and location data could be requested as follows (informal translation from ASPI system):

> [. . .] an intentional criminal offence for which the law sets out a prison sentence with an upper penalty limit of at least three years; for the criminal offence of violating the confidentiality of messages; for the criminal offence of fraud; for the criminal offence of unauthorised access to computer systems and information media; for the criminal offence of procuring and possessing access devices and computer system passwords and other such data; for the criminal offence of dangerous threats; for the criminal offence of dangerous persecution; for the criminal offence of spreading alarming news; for the criminal offence of encouraging a criminal offence; for the criminal offence of approving a criminal offence; or for an intentional criminal offence for which prosecution is stipulated in a proclaimed international treaty binding on the Czech Republic.

The general requirement is that the prosecuted crime should be an intentional one for which the law provides for imprisonment with an upper limit of the penalty of at least 3 years. This, however, does not apply on the crimes that cannot be practically prosecuted without the traffic and location data, *i.e.* crimes committed by means of electronic communication. As the Explanatory Memorandum to the Act on electronic communications explains "should the police during the investigation of these crimes had no chance to get traffic and location data, one could consider the decriminalisation of such conduct, as these crimes would be virtually inexplicable".[55] Finally, the data could also be requested for the purposes of criminal proceedings for an intentional crime, which the Czech Republic is required to prosecute under an international treaty that is binding on the Czech Republic. The supra cited provision also states that the order can be issued only in case there is no other way to achieve the pursued purpose or if its achievement would be otherwise significantly harder.

An application for a court order to request traffic data is prepared in preliminary proceedings by a prosecutor and is usually based on a reasoned proposal from the police. Before a prosecutor submits the application, she must assess whether the order is necessary to obtain facts relevant to the criminal proceedings, whether there is no other way to achieve the pursued purpose, whether the criminal proceedings are

[55]See in Czech: Šámal (2013), pp. 1222–1237.

hoeren@uni-muenster.de

conducted for adequate criminal offence and whether there is enough information about the case to properly determine which data are to be obtained. The prosecutor should mention these facts in the application that should also indicate the scope of required data and proper justification. Finished application is then forwarded to the judge, who issues an order to request traffic data. The order usually contains generally the same information as the application. The order is then forwarded to the public prosecutor.[56]

5 Data Protection and Electronic Surveillance for Security and Defence Purposes

General legal framework for processing of personal data for security and defence purposes will be laid down by the draft Personal Data Processing Act. The third substantive part of the act is dedicated to data protection in areas outside the scope of the EU law like intelligence, defence or security and provides for *mutatis mutandis* application of regulatory principles of the GDPR.

5.1 Surveillance by Intelligence Services

There are three intelligence services in the Czech Republic that are strictly separated: The Office for Foreign Relations and Information (foreign intelligence service), the Security Information Service (interior counter-intelligence service) and the Military Intelligence. *Lex generalis* covering these services is Act No. 153/1994 Sb. on intelligence services of the Czech Republic; the special acts are Act No. 154/1994 Sb. on the Security Information Service and Act No. 289/2005 on Military Intelligence. Rules for communication interception conducted by intelligence services are included in these acts. A very specific case is the National Security Authority, which is responsible for personnel and facility security clearance procedures. Section 107, subsection 3 of the act No. 412/2005 Sb. on the protection of secret information and security gives National Security Agency a power to ask an intelligence service to carry out an examination of possible security risks in the candidate's surroundings for clearance purposes. This examination may include surveillance and interception of communications.

The conditions which are needed to be fulfilled by an intelligence service in order to legally carry out interception of electronic communication are much less strict than in the case of interception for criminal purposes. Acts No. 154/1994 Sb. on the Security Information Service and No. 289/2005 on Military Intelligence are

[56]The problematic of data retention and use of traffic and location data is in detail elaborated in Interception of electronic communications in the Polčák et al. (2016), pp. 83–88.

hoeren@uni-muenster.de

practically identical when it comes to the authorisation to conduct communication interception. Both services are authorised to i) the interception or recording of telecommunications, radio communication or other similar operation, or surveying data about this operation[57]; ii) monitoring of telecommunications, radio communication or other similar operations without tapping its content, or collecting data on the traffic.[58] Probably the most important provision is Section 9 subsection 5 of the act No. 289/2005 on Military Intelligence[59] which reads as follows:

> Military Intelligence/the Security Information Service is entitled to the extent required for the performance of a specific operation, request a legal or natural person providing a public communications network or publicly available electronic communications service
>
> a) the establishment or security interface for connecting the terminal telecommunications equipment for the interception or recording messages at specified points of their network, and
> b) the provision of operational and localization data, in the form and to the extent determined by special legislation.

The Office for Foreign Relations and Information is not expressly authorised by law to conduct communication interception. However, section 9 of the act No. 153/1994 Sb. on intelligence services of the Czech Republic allows general cooperation between the services based on an agreement between them.

Although a judicial approval is needed before an intelligence service starts with communication interception, the threshold is much lower because it is not limited to specific criminal offence. The Constitutional Court noted this difference in its decision No. I. ÚS 3038/07, when it stated that information obtained from communication interception by an intelligence service could not be freely used in criminal proceedings. The Constitutional Court formulated that there are two frameworks for communication interception.

The first one is criminal proceedings framework. Its sole purpose is to solve the crime and the entire process is contained within the judiciary branch of state power. The interception to obtain the evidence is done by the Police in accordance with the Code of Criminal Procedure and it is subject to a closer judicial review. On the other hand, the purpose of the second one, the intelligence framework, is to ensure national security. It is heavily rooted in the executive branch of state power and the judicial review is much less extensive than in the case of criminal proceedings.[60]

[57]Section 8 subsection 1 letter b of both acts. This is considered as intelligence technology.

[58]Section 8 subsection 2 letter d of both acts. This is not considered as intelligence technology.

[59]The same wording has section 8a of act No. 154/1994 Sb. on the Security Information Service.

[60]For more information see Interception of electronic communications in the Polčák et al. (2016), pp. 19 and 95–101.

hoeren@uni-muenster.de

5.2 Cybersecurity and Information Transfer

The Act No. 181/2014 Sb., on Cybersecurity requires controllers of important systems and critical information infrastructure to share data on cyber security incidents with the Governmental CERT (Computer Emergency Response Team) that is operated by the National Cyber and Information Security Agency. Section 8 of the Cybersecurity Act states that:

> Public authorities and natural and legal persons set out in § 3 b) to e) are obliged to report cyber security incidents in their important network, critical information infrastructure information system, critical information infrastructure communication system or important information system immediately after their detection.

This data may also contain personal data, which is why the National Cyber and Information Security Agency and its employees are required to keep it confidential, as is prescribed by section 10 as follows:

> (1) Employees of the Czech Republic working for the Agency, taking part in solving cyber security incident, are bound by confidentiality about incidents record data. Confidentiality lasts even after the termination of the labour law relationship towards the Agency.
> (2) The director of the Agency may waive incidents evidence data confidentiality of persons set out in paragraph 1, together with determination of the data and waiver extent.

Incident data can be only shared with other public authorities if it is necessary for fulfilling tasks within their authority.[61]

The National CERT generally falls within the application of the private law. Therefore, General Data Protection Regulation applies for any data processing conducted by it. This situation is not so clear in the case of the Government CERT. The wording of section 41 of the proposal of Personal Data Processing Act states that the provisions in question are to be used when there is processing of personal data for "*the purpose of defence and security interests of the Czech Republic*". However, the explanatory report to the proposal mentions only duties of intelligence services, the army and during crises. Therefore, it is not entirely clear whether processing of personal data conducted by the Government CERT during fulfilling of its duties should be covered by the third part of the proposed act.

6 Remedies and Sanctions

The overall regulatory philosophy of the GDPR has changed, compared to previous legislation, from liability to compliance. The GDPR lays down, besides mere protective obligations, a system of various regulatory instruments designed to

[61] Section 9 subsection 3 of the act No. 181/2014 Sb., on Cybersecurity. The relationship of data protection and cybersecurity was in analysed in *e.g.* Harašta and Míšek (2015), pp. 21–42 (in Czech). For more information on Czech legislative approach to cybersecurity see (in Czech) *e.g.* Polčák 2015, pp. 95–149.

hoeren@uni-muenster.de

prevent breaches of protection of personal data. Consequently, sanctions are available not only for actual breaches of protection of personal data but also for breaches of various compliance obligations.

The sanctioning policy of the GDPR uses pragmatic assessment of a number of practically relevant facts related to respective breach of obligations. In particular, imposing fines is subject to assessment of the following criteria laid down in Art. 83 (2) of the GDPR:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Direct administrative sanctions for breaches of obligations laid down in the GDPR are fines. Breaches in obligations listed in Art. 83(4) of the GDPR, *i.e.* mostly compliance obligations, are subject to fines amounting up to 10 mil. EUR or 2% of worldwide turnover. Breaches of obligations listed in Art. 83(5) of the GDPR, *i.e.* mostly protective obligations related to rights of data subjects, are subject to fines amounting up to 20 mil. EUR or 4% of worldwide turnover.

The GDPR also lays down powers of DPAs to impose corrective administrative measures to recover lack of compliance or breaches of protection. These measures listed in Art. 58(2) of the GDPR can be imposed upon controllers or processors, depending on circumstances of particular cases, solely or along fines.

Maximum fines in the GDPR are substantially higher than those laid down in the Act No. 101/2000 Sb. The past limit for fines under the Act No. 101/2000 Sb. was 10 mil. CZK (approx. 400,000 EUR) and there was even no possibility to charge a fine based on corporate turnover. Moreover, the sanctioning policy of the Czech DPA had been, compared to other DPAs of the EU member-states, very modest, as regular fines amounted mostly to hundreds or single thousands EUR.

hoeren@uni-muenster.de

The reason for such modesty in charging was mostly that the breaches of protection that the Czech DPA was able to fully investigate were of minor relevance. It was also not rare that the Czech DPA was often, mostly for being understaffed and subject to political pressures in appointing senior officials (the Inspectors), not able to establish solid cases against controllers or processors acting in breach of obligations. Low fines were in these cases used to avoid respective decisions being challenged in judicial review, as it was not economically reasonable for affected controllers or processors to invest in court litigation against fines worth near to nothing.

The same are the reasons for which there had been for long time almost missing relevant Czech court case law. As there had been neither real fear of sanctions nor reasons for establishment of court cases, there also had been almost missing professional legal expertise. That led to critical shortage of legal experts in the wake of the GDPR when there emerged a massive market of compliance solutions.

Member states are allowed by Art. 83(7) of the GDPR to legislate specific limitations of fines charged to public sector bodies. In that respect, it is questionable whether there applies current limitation of 10 mil. CZK laid down in Czech Act No. 101/2000 Sb. that is still in force (despite it was substantially materially derogated by the GDPR—see above). In any case, the same limit of max. 10 mil. EUR for public sector bodies is now drafted in the pending Personal Data Processing Act (see above).

Distinction of fines between public sector bodies and other controllers and processors have been recently broadly debated in the Czech Republic. Especially smaller self governing units, such as towns, feel threatened by limits specified in Art. 83 of the GDPR. At the same time, specific limitations for public sector bodies might create unreasonable inequalities and might lead to paradoxical situations, *e.g.* in cases when a private establishment acts as a personal data processor for a controller who is a public sector body. In such cases, that are not rare in the practice of Czech public sector bodies of all sizes, a controller who sets the purpose of processing of personal data and gives orders to the processor would be subject to sanctions theoretically amounting only to a fraction of limits that would apply to the processor.

Besides administrative fines and corrective measures, there are also available standard court remedies for material damage or immaterial harm. Material damage is covered with damages (*náhrada škody*), while immaterial harm is covered with satisfactory damages (*zadosti učinění*).

The court procedure of claiming damages or satisfactory damages depends on the nature of respective controller or processor. If a controller or processor causes damage or harm as a public authority acting in its public law capacity, remedies might be sought through administrative court procedure (Act No. 150/2002 Sb.) upon the liability for illegal acting of a public body (Act No. 82/1998 Sb.) In all other cases, data subjects can sue upon standard rules of civil procedure (Act. No. 99/1963

hoeren@uni-muenster.de

Sb.), and upon the general civil law liability for damage or harm (Act No. 89/2012 Sb.)

No fines or other direct sanctions are available for breaches of obligations that fall outside the scope of jurisdiction of the Czech DPA, *i.e.* when personal data are processed for security and defence purposes or in cases when data are processed for exercise of juridical powers. However, subsequent sanctions are available in these cases against responsible staff upon general disciplinary liability. Also, there still applies the liability for illegal acting of a public body and there is available respective court claim under the rules of administrative court procedure.

In addition to above administrative sanctions and remedies for recovery of damage or harm, serious misuse of personal data might be subject to criminal law sanctions. The Czech Criminal Code (Act No. 40/2009 Sb.) uses specific type of criminal conduct indicated as 'Unauthorised Use of Personal Data' and laid down in Section 180 (informal translation):

§ 180 Unauthorised Use of Personal Data

(1) Whoever, even out of negligence, publishes, discloses, makes available, or otherwise processes or appropriates personal data that was collected on another person in connection with the execution of public authority without authorisation, and thus causes serious harm to the rights or legitimate interests of the person whom the personal data concerns, shall be punished by a prison sentence of up to three years or punishment by disqualification.
(2) Whoever, even out of negligence, violates the State imposed or recognised obligation of confidentiality by publishing, disclosing, making available, or otherwise processing or appropriating personal data that was collected on another person in connection with the execution of their employment, profession, or function without authorisation, and thus causes serious harm to the rights or legitimate interests of the person whom the personal data concerns, shall be similarly punished.
(3) An offender shall be punished by a prison sentence of one to five years, monetary penalty, or punishment by disqualification, if,

    a) they committed an act referred to in Subsection 1 or 2 as a member of an organised group,
    b) they committed such act by the press, film, radio, television, publicly accessible computer networks, or other similarly effective means,
    c) they caused substantial damage by committing such an act, or
    d) they committed such an act with the intention of gaining a substantial benefit for themselves or someone else.

(4) An offender shall be punished by a prison sentence of three to eight years, if,

    a) they caused large-scale damage by committing an act referred to in Subsection 1 or 2, or
    b) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

hoeren@uni-muenster.de

7 Private International Law Rules

The territorial scope of application of data protection rules is laid down in Art. 3 of the GDPR that reads as follows:

> Article 3 Territorial scope
>
> 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
>   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
>
> 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

The above relatively broad reach of the GDPR raises a number of questions namely as to enforcement. To put it short, the GDPR also theoretically applies to cases when data are processed by offshore entities and processing takes place on foreign soil and so it is questionable to which extent can the EU or its member-states provide for truly efficient investigation and sanctions of data compliance or data breaches.

Due to overall lack of case-law and past lack of investigative activity of the Czech DPA in cases with cross-border outreach, there is no substantial Czech case-law on data transfers. Most relevant case-law of the CJEU on cross-border processing of personal data includes:

- C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.*
- C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmiés Információszabadság Hatóság*.
- C-498/16 *Maximilian Schrems v Facebook Ireland Limited*.

For the sake of efficiency, the GDPR contains limitations to data transfers. Data are allowed to be transferred for processing in a third country or an international organisation (incl. making them available for access from a third country) only under conditions specified in Art. 45 and 46 of the GDPR. The general rule for data transfers to third countries is laid down in Art. 44 that reads as follows:

> Article 44 General principle for transfers
>
> Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward

hoeren@uni-muenster.de

> transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Art. 45 contains a procedure for the Commission to declare protective regime of personal data in a third country "adequate" with the rules applicable in the EEA. Adequacy decisions constitute per se a valid reason for transferring data to a third country without a need for any further safeguards. The same procedure of declaring adequacy of protection applied even before the GDPR came into effect and one adequacy decision had already been taken down by the CJEU in a broadly medialised case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, joined by Digital Rights Ireland Ltd.

Besides adequacy decisions, the GDPR formulates a handful of further legal titles for transfers of personal data to third countries. They are listed in Art. 46 of the GDPR that reads as follows:

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

   (a) a legally binding and enforceable instrument between public authorities or bodies;
   (b) binding corporate rules in accordance with Article 47;
   (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
   (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
   (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
   (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

   (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
   (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

The GDPR also lays down procedural principle of one-stop shop for cases when data processing takes place in multiple EU jurisdictions at the same time. In that case, the GDPR constitutes the "lead supervisory authority" that coordinates investigation and issues a decision that is "directed towards the main or single establishment of the controller or processor" (see Para 126 of the Recital to the GDPR).

hoeren@uni-muenster.de

Decisions on sanctions or other remedies made in such cases shall be mutually agreed between the lead supervisory authority and other involved DPAs.

If processing of personal data falls within the scope of the GDPR and neither controller nor processor(s) are established in the EU (or EEA respectively), they are obliged to appoint a representative in the EU. In that case, the representative "shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are, and it shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation"—see Art. 27(3),(4).

The mechanism of legal representatives that existed also under the previous statutory regime demonstrates the above concerns over efficiency of cross-border reach of EU data protection rules. It turns out that entities that process personal data outside the EU and have no presence in the EU hesitate to appoint their representatives pursuant to Art. 27(1) of the GDPR or previously Art. 4(2) of the Directive 95/46/EC. In such cases, EU member states struggle to find measures to motivate offshore controllers and processors to comply with this obligation.

The GDPR provides for liability claims in Art. 82(1) and (2) of the GDPR that read as follows:

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Basic procedural provision, including jurisdictional rules, is laid down in Art. 79 of the GDPR that reads as follows:

Article 79 Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

In addition to the GDPR, the Czech Civil Code contains traditional liability provisions for infringements of personality protection, whereas privacy is considered a component of the concept personality. Consequently, certain cases of breaches of

hoeren@uni-muenster.de

the GDPR can at the same time fall under remedies laid down in the Civil Code. Data subjects would in those cases have a choice as to whether they litigate under the GDPR or the Civil Code (or both—see above).

However, neither the draft Czech Data Processing Act nor the Amending Act contain any provisions regarding procedure for GDPR-based court cases. That means there will arise substantial uncertainty as to whether such cases fall under the general civil procedure, special civil procedure under Head V. of the Civil Code (this procedure is for certain cases of judicial review of authoritative decisions) or administrative court procedure (this procedure is generally used for judicial review of administrative decisions).

In any case, the above implies that cross-border court claims made by data subjects under the GDPR will be from jurisdictional perspective based on above statutory dichotomy of Art. 79(2) that consists of place of establishment of the controller or processor, and place of residence of the data subject. The same applies also for damages or other remedies pursuant to Art. 82(6) of the GDPR.

Contrary to that, determination of forum and law applicable in cross-border court cases for personality protection remedies under the Civil Code will be made pursuant to Regulation (EC) No. 864/2007 and subsequently according to Act No. 91/2012 Sb. (Act on Private International Law) where the key criterion is, besides the place of establishment of the defendant, *locus delicti* and *locus damni* (the place of delict or the place of damage). In that regards, there will mostly probably continue to apply jurisdictional interpretations made in joined cases C-509/09 and C-161/10 eDate *Advertising GmbH and Others v X and Société MGN limited*. As to civil law damages, there will probably apply, *per analogiam*, rules laid down in C-170/12 Peter Pinckney v. KDG Mediatech AG that give respective court of a member state "jurisdiction only to determine the damage caused in the Member State within which it is situated".

References

Chudomelová Z, Beran M, Jadrný V, Němečková Š, Novák J (2016) Zákon o elektronických komunikacích: Komentář. Wolters Kluwer, Praha

Harašta J, Míšek J (2015) IP adresy v kybernetické bezpečnosti. Revue pro právo a technologie 6 (12):21–42

Hlaváčová K, Chorvát O (2016) Přístup orgánů činných v trestním řízení k datům uloženým v cloudu. Revue pro právo a technologie 7(14):3–24

Kahle B, Vysokajov M, Hůrka P, Randlová N, Doležílek J (2015) Zákoník práce: Komentář. 5. Aktualizovanévydání. Wolters Kluwer, Praha

Maisner M (2016) Zákon o některých službách informační společnosti: Komentář. C.H. Beck, Praha

Maisner M, Vlachová B (2015) Zákon o kybernetické bezpečnosti: Komentář. Wolters Kluwer, Praha

hoeren@uni-muenster.de

Myška M (2013) Data retention in Czech Republic: past, present and future. Masaryk Univ J Law Technol 7(2):267–285
Polčák R (2015) Kybernetická bezpečnost jako aktuální fenomén českého práva. Revue pro právo a technologie. 6(11):95–149
Polčák R et al (2015) Elektronické důkazy v trestní mřízení [online]. Masarykova Univerzita, Brno
Polčák R et al (2016) Interception of electronic communications in the Czech Republic and Slovakia. Masaryk University, Brno
Polčák R et al (2018) Právo informačních technologií. Wolters Kluwer, Praha
Šámal P (2013) Trestní řád: Komentář. C. H. Beck, Praha. 4720 p
Vantuch P (2008) Nová úprava odposlechu v trestním řádu od 1. 7. 2008. Bulletin advokacie, no. 10, p. 29
Vlachová B (2016) Zákon o elektronických komunikacích: Komentář. C.H. Beck, Praha
Wagnerová E et al (2012) Listi na základních práv a svobod: Komentář. Wolters Kluwer, Praha. 931 p

hoeren@uni-muenster.de

Data Protection in the Internet: French Report

Laurence Nicolas-Vullierme

1 General Data Protection

The legal framework surrounding personal data protection is provided primarily by the *Loi du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés* (LIL),[1] as amended successively and principally by the *Loi du 6 août 2004*,[2] *Loi du 7 octobre 2016*[3] and *Loi du 20 juin 2018*.[4] This legislation is supplemented by the *Décret du 29 mai 2019*.[5]

While the *Loi pour la République Numérique* (LRN) of 2016 had anticipated the entry into force of the General Data Protection Regulation (GDPR), it had not sufficiently adapted French law to the new European rules. A draft legislative act

[1] Act no 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (LIL), JORF *(Journal Officiel de la République Française)* 7 January 1978 – *corrigendum* – JORF 25 January 1978. Consolidated version on: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460. (Accessed 21 September 2018).

[2] Act no 2004-801 of 6 August 2004 relative to the protection of individuals with regard to the processing of personal data *(Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel)*, JORF 7 August 2004.

[3] Act no 2016-1321 of 7 October 2016 (*Loi pour une République numérique* – LRN), JORF 8 October 2016.

[4] Act no 2018-493 of 20 June 2018 (*Loi relative à la protection des données personnelles*), JORF 21 June 2018. Desgens-Pasanau (2018a); Dossier Dalloz IP/IT (2018), p. 458; Debet (2018), p. 907; Viney (2018), p. 366.

[5] Decree no 2019-536 of 29 Mai 2019, JORF 30 Mai 2019, No16.

L. Nicolas-Vullierme (✉)
Centre de Droit Européen, Université Panthéon-Assas (Paris 2), Paris, France
e-mail: laurence.nicolas-vullierme@u-paris2.fr

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_6

hoeren@uni-muenster.de

was therefore tabled on 13 December 2017[6] and fast-tracked through Parliament. After an appeal brought before the *Conseil Constitutionnel* indicative of the tension between the two houses,[7] the bill was enacted and then published on 21 June 2018.[8]

The Act of 20 June 2018 not only adapts French law to the GDPR, but it also transposes Directive 2016/680 on the processing of personal data into criminal law. The French legislature has not systematically implemented the provisions of the GDPR, but has adopted the policy of cross-referencing, which hardly facilitates their proper applicability.[9] This explains why the Ordinance of 12 December 2018 was made to improve the legibility of the act and its consistency.[10] This lack of foresight, which is not conducive to legal certainty, is to be regretted.

The wording of the LIL currently in force bears little resemblance to the initial text but it is still tremendously symbolic.[11] Article 1 is unchanged: "Information technology should be at the service of every citizen". The adaptation of the French law to the European package effects a "paradigm shift"[12]: *ex-ante* supervision with prior declarations is replaced by *ex-post* supervision. The responsibility of actors (accountability principle) and the protection of natural and legal persons are reinforced.[13]

These basic texts are supplemented by *other legislation* (*e.g.* article 9 of the Civil Code on the protection of privacy, legislation on unfair clauses in the Consumer Code), *other regulations* (*e.g.* the three decrees of 29 September 2017 on the obligation for on-line platform operators to provide truthful information[14]) and *soft*

[6]Assemblée Nationale, No 490, Draft law relative to the personal data protection: http://www.assemblee-nationale.fr/dyn/15/dossiers/alt/donnees_personnelles_protection. (Accessed 21 September 2018). See also: CNIL, Deliberation no 2017-299 of 30 November 2017, CNILTEXT000036195647. *Conseil d'État*, Opinion of 7 December 2017, no 393836, NOR: JUSC1732261L.

[7]*Conseil Constitutionnel*, Decision no 2018-765 DC of 12 June 2018, JORF 20 June 2018: NOR: CSCL1816349S.

[8]Act no 2018-493 of 20 June 2018, JORF 21 June 2018; Dossier (2018).

[9]See, for example, a critical article: Martial-Braz (2018), p. 459.

[10]Act no 2018-493 of 20 June 2018, Art. 32. Ordinance no 2018-1125 of 12 December 2018, JORF 13 December 2018. See in particular CNIL, Deliberation no 2017-299 of 30 November 2017, CNILTEXT000036195647. See also Fauvarque-Cosson and Maxwell (2018), p. 1034; Martial-Braz (2018), p. 459.

[11]Le Gouvernement a fait le choix symbolique de ne pas abroger la loi fondatrice du 6 janvier 1978, Explanatory Note to Act no 2018-493, p. 7.

[12]See, for example, Hébert (2018), p. 9.

[13]Desgens-Pasanau (2018b), p. 25.

[14]Decrees nos 2017-1434, 2017-1435 & 2017-1436 of September 29, 2017, JORF 05 October 2017: entry in force on 1 January 2018 except the Decree no 2017-1435 which came into force on 1 January 2019.

hoeren@uni-muenster.de

law. This latter has already been greatly developed by the action of the *Commission Nationale de l'Informatique et des Libertés* (CNIL)[15] and is bolstered by the Act of 20 June 2018, which creates new instruments "whose rule-making character is graduated"[16]: drafting and publication of guidelines, recommendations, or benchmarks to facilitate compliance and prior risk-evaluation by processors' controllers, and publication of reference methodologies for processing activities.

Alongside this legislation there are numerous *legal rulings*: those of the CNIL, and of French and European courts of law (the European Court of Human Rights (ECHR) and the European Court of Justice (ECJ)).

Before the Ordinance of 12 December 2018, the article 2(2) LIL provided that: "personal data means any data relating to a natural person who is identified or may be identified directly or indirectly by reference to an identification number or to one or more elements specific to that person. In determining whether a person is identifiable, consideration should be given to all means for enabling their identification that are available to the controller or any other person, or to which they may have access."

This definition derives from the LIL as amended by the Act of 2004. Initially, the text covered "nominative information". The lawmaker subsequently replaced that expression by "nominative data" before coming to refer to "personal data".

With the Ordinance, the LIL includes now a cross-reference to the definition of "personal data" contained in the GDPR.

Further to the judgment of the ECJ of 19 October 2016, which held that an IP address referred to an identifiable natural person,[17] the *Cour de Cassation* in turn found on 3 November 2016 that an IP address was personal data.[18] The same applies to a MAC address.[19]

For want of any right to personal data protection being enshrined in the French Constitution of 1958,[20] the *Conseil Constitutionnel* recognized such a right on the basis of the right to respect of privacy.[21] This right is guaranteed by article 2 of the Declaration of the Rights of Man and the Citizen of 1789. Several decisions take up the same grounds:

[15]Falque-Pierrotin (2013), p. 239; Bourgeois (2017), pp. 15 ff.

[16]See for example the baseline methodology in the matter of health: MR-001. Explanatory statement, p. 8.

[17]ECJ 19 October 2016, C 582/14, ECLI:EU:C:2016:779.

[18]Decision of the first Civil Chamber of Court of Cassation, 3 November 2016, *pourvoi* no 15-22595, ECLI:FR:CCASS:2016:C101184. Fauchoux et al. (2017), no 333.

[19]CNIL, Deliberation no 2016-053 of 1 March 2016: CNILTEXT000032168674.

[20]See Martial-Braz (2018), p. 459.

[21]*Conseil Constitutionnel*, Decision no 2012-652 DC of 22 March 2012, no 8. ECLI:FR:CC:2012:2012.652.DC.

hoeren@uni-muenster.de

> The freedom proclaimed by article 2 of the Declaration of the Rights of Man and the Citizen of 1789 implies the right to privacy. Consequently, the collection, recording, storage, consultation and disclosure of personal data must be warranted by a ground of general interest and implemented in a manner that is suitable and proportionate to this purpose.[22]

The LIL includes provisions specific to certain data: *e.g.* sensitive data, data relating to offences, convictions and security measures.[23]

Adaptation of the current framework to the GDPR has widened the range of *sensitive data*. Apart from data on racial or ethnic origin, political opinions, etc. the LIL now mentions "genetic" and "biometric" data.[24] The Act of 20 June 2018 adds controlled access using biometric data in working relations, the re-use of public information featuring in judgments, and processing required for public information and research. Similarly, it is no longer a question of sex life but of sexual orientation.

In principle, such data cannot be processed.

> I. - It is prohibited to process data of a personal character that reveal the supposed racial origin or ethnic origin, political opinions, religious or philosophical convictions or trade-union membership of a natural person or to process genetic or biometric data for the purposes of identifying a natural person individually, data concerning health or data concerning sex life or sexual orientation of a natural person.[25]

However, there are exceptions in criminal law (processing relating to criminal convictions), research (for archival, research, and statistical purposes), and health.

The Act of 20 June 2018 introduces amendments surrounding *the use of algorithms* in individual legal decisions and administrative decisions. Decision no 2018-765 DC of the *Conseil Constitutionnel* of 12 June 2018 provides useful clarification on this last point.[26] It held that the new provisions surrounding the use of algorithms are consistent with the Constitution because "use of the algorithm alone as a basis for an individual administrative decision is subject to compliance with three conditions" (No 70):

(1) The decision "shall state explicitly that it has been adopted on the basis of an algorithm". Moreover, the main characteristics for implementing the algorithm shall be disclosed to the data subject on request. Consequently, it shall not infringe any of the secrets or interests stated in subsection 2 of article L 311-5 of the Code on relations between the public and the administration,
(2) The individual administrative decision based on the algorithm alone "shall be subject to administrative appeal procedures",
(3) It shall not pertain to any sensitive data.

---

[22]For example: *Conseil Constitutionnel*, Decision no 2012-652 DC of 22 March 2012, no 8 and Decision no 2016-745 DC of 26 January 2017, no 25. NOR: CSCL1702669S.

[23]LIL, Article 6.

[24]See Bourgeois (2017), no 362.

[25]LIL, Article 6 I.

[26]*Conseil Constitutionnel*, Decision no 2018-765 DC of 12 June 2018, JORF 20 June 2018: NOR: CSCL1816349S. Nicolas-Vullierme (2018), https://audeladudroit.fr/algorithme-droits-fondamentaux/. (Accessed 21 September 2018). Rochfeld (2018), p. 474.

hoeren@uni-muenster.de

The algorithm shall remain under the controller's supervision. Therefore a "self-learning" algorithm cannot be used.

The question came under debate in France because of the use of such algorithms for first-year university registrations. The previous "Admission Post Bac" system or APB was replaced by a new "Parcours Sup" system because of a lack of transparency and of recourse to drawing lots for university places.[27]

Lastly, the Act of 20 June 2018 introduces into the area of healthcare a general regime for processing health data and a specific regime for processing data for research purposes.[28]

Although the LIL was initially enacted to protect citizens from the administration, it applies to both public and private entities. Subsequently, specific or sector-wide legislation has supplemented the personal data protection arrangements in areas as diverse as the fight against terrorism,[29] archives,[30] or healthcare.[31]

In France, the CNIL,[32] an independent administrative authority, is tasked with data protection. Although it is not a legal entity, it does have *locus standi*.[33] It is composed of 18 members who are elected or designated by assemblies or courts and tribunals.[34] Since February 2019 the CNIL has been chaired by Madame Denis. There is a five-member select committee with a separate chair from the chair of the CNIL (currently Mr. Linden).

The tasks of the CNIL[35] are to inform, advice, especially through advisory opinions and recommendations, supervise, and sanction.[36] Until now the CNIL supervised processing both *ex ante* (via a system of declaration and authorisation) and *ex post*. With the entry into force of the GDPR, the *ex ante* authorisation system has all but vanished. It still holds for processing health data for research work and in the absence of standard regulations, benchmarks or reference methodologies.

The entry into force of the GDPR went along with increased competences for the CNIL. For example, the CNIL may carry out supervision under a borrowed identity.[37] The CNIL must also list the criminal files that may present a high risk for individual rights and freedoms. The penalties it may order are heavier and more

[27]Nicolas-Vullierme (2018), https://audeladudroit.fr/algorithme-droits-fondamentaux/. (Accessed 21 September 2018).

[28]Bossi-Malafosse (2018), pp. 58 ff.

[29]Act no 2006-64 of 23 January 2006, JORF 24 January 2006.

[30]Act no 2008-696, 15 July 2008, JORF 16 July 2008.

[31]Act no 2016-41 of 26 January 2016, JORF 27 January 2016.

[32]Website: https://www.cnil.fr/.

[33]Bourgeois (2017), No 39.

[34]LIL, Article 9. Fauchoux et al. (2017), p. 58 ff.

[35]LIL, Article 8.

[36]Bourgeois (2017), pp. 22 ff.

[37]LIL, Article 19 III.

hoeren@uni-muenster.de

systematic. There is no need for prior notice to be issued, as was the case before—apart from in serious instances—to impose penalties.[38]

The CNIL has become the national supervisory authority within the meaning of the GDPR.[39] Apart from the CNIL (see above), the Act of 6 August 2004 had created a new position: that of data protection correspondent (*correspondant "informatique et libertés"* (CIL)),[40] "tasked with independently ensuring compliance with obligations" laid down in the LIL. Whenever there was a correspondent, there was no need to file declarations unless personal data were to be transferred to a non EU member state. The CIL could be held accountable in criminal law in some instances. However, the presence of a CIL did not in any way dispense with requests for authorisation.

With the coming into force of the GDPR, the CIL has become the data protection officer (DPO).[41] The DPO assists the controller and its processor. While the designation of a CIL was optional, it has become mandatory to designate a DPO in three cases: for the public authority or public body, for large-scale processing, and for sensitive data and criminal offences.

Although the status of the CIL and the DPO are similar, the requirements as to qualifications and training are specified and tasks reinforced, particularly in terms of advice and cooperation with the supervisory authority.[42] Lastly, the DPO must be afforded the resources necessary for the task.

The CIL was in charge of all processing by the body or just a part of it. The position had been created to avert administrative or criminal sanctions for the body. The role was to ensure the body complied with personal data protection rules. It has now been replaced by the data protection officer (DPO) who is assigned specific tasks by the regulation.

The CIL had no power of sanction and could only make recommendations to the controller.

Under the GDPR the DPO is responsible for reporting any breach of personal data. The CNIL has already published a number of documents explaining the role of the new officer.[43] No doubt the "compliance" function will develop further within business organizations.[44]

Although Directive 95/46 is designed to promote self-regulation instruments, these are little developed in France.[45]

[38]Debet et al. (2015), no 2-10.

[39]LIL, Article 8.

[40]JORF 7 August 2004, 14063. LIL, Article 22 III. Decree no 2005-1309 of 20 October 2005 (amended by Decree no 2007-451 of 25 March 2017), Article 42 ff.

[41]LIL, Article 57. Desgens-Pasanau (2018b), p. 25; Carrera Mariscal (2018), p. 233.

[42]https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees.

[43]https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo.

[44]Fauvarque-Cosson and Maxwell (2018), p. 1033.

[45]See *Conseil d'État* (2014), pp. 274 ff.

hoeren@uni-muenster.de

Under article 11-I-3°b of the LIL, "at the request of professional organizations or of institutions essentially comprising controllers" the CNIL "makes an appraisal of the guarantees provided by professional rules that it has previously recognized to be consistent with the provisions of this Act, in terms of adherence to fundamental personality rights". However, no clarification has been made by the legislator as to the procedure.

The CNIL has not been the driving force in this domain.[46] Under this article, two codes of professional ethics for marketing by electronic means have been recognized as complying: one presented by the *Syndicat National de la Communication Directe* (SNCD)[47] and one by the *Union Française du Marketing Direct* (UFMD).[48] To promote their development, the *Conseil d'État* in its 2014 study recommended adopting an approval procedure.[49] On 11 December 2014, the CNIL passed a resolution to issue an accreditation.[50] This resolution was modified on 13 July 2017 to adapt it to the GDPR[51]: it supposes that the body meets 25 requirements concerning the internal organization and management of personal data, the procedure for testing compliance, and the management of complaints and incidents.[52] Professional actors have not contributed further to the development of these self-regulation systems.

The GDPR should therefore further the development of such instruments. The CNIL shall have to strengthen its production of reference standards in the future because its practical information sheets are not specific enough.[53]

2 Data Protection in the Internet

In the case of data processing by electronic means, apart from the LIL, the Civil Code[54] and the Postal and Electronic Communications Code (CPCE) are applicable. There are also simplified norms adopted by resolution by the CNIL.

[46]Debet et al. (2015), pp. 193 ff, see in particular p. 195.

[47]CNIL, Deliberation no 2005-047 of 22 March 2005: CNILTEXT000017653290.

[48]CNIL, Deliberation no 2005-051 of 30 March 2005. https://www.cnil.fr/sites/default/files/typo/document/projet-codeUFMD.pdf.

[49]*Conseil d'État* (2014).

[50]CNIL, Deliberation no 2014-500 of 11 December 2014, JORF 10 January 2015. Fauchoux et al. (2017), no 327.

[51]CNIL, Deliberation. No 2017-219 of 13 July 2017, JORF 20 September 2017.

[52]Perray (2018), pp. 19 ff.

[53]Desgens-Pasanau (2018a), p. 211.

[54]Code civil, Article 1125 to Article 1127-4 (since the reform of the law of obligations from 10 February 2016) and CPCE, Article L 100 (electronic registered mail).

hoeren@uni-muenster.de

Provisions specific to agreements entered into by electronic means do not contain any specific rules for personal data protection because they are only the transposition of European Directive no 2000/31/EC on electronic commerce.

Under article 1127-1 (1) of the Civil Code, "Anyone offering on a professional basis by electronic means the supply of goods or services shall make the applicable contractual provisions available in a way that enables them to be stored and copied". Paragraph 2 of the same article lists everything a contractual offer must contain and especially the technical means for identifying any errors made in capturing data and for correcting them.

Generally, French law on electronic communications has taken up the European rules. However, there is a number of specifics.

The LIL recalls the rights of the "data subject" protected by GDPR.[55]

The data subject must also be informed about the purpose of the processing and the means they have to object to it.[56]

Initially there was no need for a basis for processing in the LIL. It was only when Directive 95/46 EC was transposed by the Act of 6 August 2004 that consent became one of the bases for processing.[57]

A reading of the former article 7 of the LIL might suggest that it is always necessary to secure the consent of the data subject to set about processing personal data.[58] However, this was not the case if the processing resulted from any of the following five conditions:

1. Compliance with a statutory duty incumbent on the controller (*e.g.* to enable the identification of content creators).[59]
2. Saving the life of the data subject (*e.g.* data processing in healthcare).
3. Performing a public service mission incumbent on the controller or recipient (*e.g.* laboratories[60]; *Comédie Française*[61]).
4. Performance either of a contract to which the data subject is party or of pre-contractual measures taken at the request of the data subject.[62]
5. Accomplishment of the legitimate interest pursued by the controller or recipient, provided it does not disregard the interest or the fundamental rights and freedoms of the data subject (*e.g.* a site for rating teachers does not constitute a legitimate interest).[63]

[55]LIL, Article 1, Article 48 to Article 56.

[56]LIL, Article 5 & Article 48.

[57]Debet (2018), p. 37.

[58]CNIL 23.07.2009, Deliberation no 2009-474 of 23 July 2009, JORF 19 August 2009, Text No 27, NOR: CNIA0900018X.

[59]CE 20 November 2013, no 347349 about the Decree no 2011-219 of 25 February 2011.

[60]For example: CNIL, Deliberation no 2012-408 of 22 November 2012. Decree no 2013-406 of 16 May 2013, "*Outils de recherche de contamination ADN*" (ORCA), JORF 18 May 2013, p. 8324.

[61]CA Paris 19 June 2008, Juris-Data no 2008-370803.

[62]CNIL, Deliberation no 2012-214 of July 19, 2012, Fnac Direct.

[63]TGI Paris 3 March 2008, RG no 08/51650, Note 2 be, *D.* 2008, p. 288, note Manara; *Comm., com. électr.* 2008, *Comm.* 58, Lepage.

hoeren@uni-muenster.de

The Act of 20 June 2018 added a cross-reference to articles 4(11) and 7 of the GDPR. The Ordinance of 12 December 2018 simplifies and retains now only a cross-reference to GDPR.

Consent is in actual fact one basis among other legitimate bases allowing personal data to be processed.[64] It should be observed, however, that the restrictive interpretation of the other bases has led to pride of place being given to consent.[65] Moreover, these various bases are not mutually exclusive. Several of them may justify the existence of one and the same processing. Lastly there is no criminal penalty for the absence of any of the conditions of article 7.[66]

Where required, the data subject's consent to the processing of their data must be prior,[67] simple and specific: it cannot be limited to acceptance of general terms and conditions of use.

There are specific rules for sensitive data, which were amended by the Act of 20 June 2018 (see above). Although the processing of such data is prohibited in principle, there are many exceptions to this prohibition (*e.g.* medical reasons, research, and statistics). The processing of sensitive data has required the data subject's consent from the outset.

The LIL notably contains special provisions for health law.[68] New article 63 LIL provides "where research requires genetic characteristics to be examined, the informed and express consent of data subjects shall be obtained before data processing is implemented".

There are also specific rules *e.g.* for on-line publications, journalists,[69] data transfers, marketing,[70] and criminal matters.[71] In this last area, the scope of application of the LIL is broader than that of the GDPR.[72]

Contrary to what was provided in the draft legislative act on personal data protection, the legislator used the possibility afforded by article 8 of the GDPR to lower the age of consent of minors for the provision of information society services to 15 years.[73] A "strong educational and awareness policy" must be introduced because of the dangers of the Internet for minors.[74] Controllers must provide minors with information about the processing of their data "in plain language that is easy to understand".[75]

[64] See Debet et al. (2015), p. 298.

[65] Debet (2018), p. 39.

[66] Debet et al. (2015), p. 304.

[67] For example: CA 21 September 2017, no 15/23732.

[68] LIL, Articles 64 ff.

[69] LIL, Article 80.

[70] *Code des postes et des communications électroniques* (CPCE), Article L 34-5.

[71] LIL, Article. 46 & Article 87 ff.

[72] Bourgeois (2017), no 413.

[73] LIL, Article 45.

[74] Charrier (2018), p. 335 ff.

[75] LIL, Article 45.

hoeren@uni-muenster.de

Minors aged 15 years may first "object to the holders of parental authority having access to data concerning them collected during research, study or evaluation".[76] In this case the minor exercises his or her rights of access, rectification, and right to object alone. Second, the minor may also "object to the holders of parental authority being informed of the treatment of data if participating in it leads to revealing information about a preventive action, testing, diagnosis, treatment or operation".[77]

Since the LRN, minors also have a specific right to erasure: data collected from minors on line and in particular data they may have published on the social networks when minors may be erased.[78] If the controller fails to comply with the application within one month, the matter may be referred to the CNIL. The CNIL must deal with the claim within three weeks. This possibility is set aside, though, whenever the treatment is necessary for complying with freedom of expression and information, statutory obligations, public policy grounds or for the purposes of research or the exercise of legal rights.

When under 15 years of age, consent must be given "jointly by the minor who is the data subject, and the holder(s) of parental authority with respect to the minor".[79] The recipients of the information concerning the processing and exercise of rights deriving from the LIL are disclosed in this case to the holders of parental authority. They may consult the data concerning the minor and exercise the right to erasure. The LIL provides that if it is impossible to inform one of the two title holders, it is possible to proceed regardless in the context of medical research.[80] The second holder of parental authority may nonetheless subsequently exercise the rights of access, rectification, and the right to object.

Everyone has the right to object [81]: this right to object can be exercised both *ex ante* and *ex post*.[82] In parallel to it there is a right of erasure.[83] Such modifications must be possible free-of-charge. Moreover, if the data has been passed on to a third party, the controller must pass on to that party the changes made. The right to rectification does not apply to literary, artistic, and journalists data.[84]

There are besides specific provisions in the event of death of the rights holder since the LRN.[85] Anyone may draft instructions concerning the provisions to be erased after their death.[86] These directives may be recorded with a digital trustee certified by the CNIL.[87]

[76]LIL, Article 70.
[77]LIL, Article 70.
[78]LIL, Article 51 II. Foret (2018), p. 350.
[79]LIL, Article 45.
[80]LIL, Article 70.
[81]LIL, Article 56.
[82]Foret (2018), p. 350.
[83]LIL, Article. 51 I.
[84]CNIL: https://www.cnil.fr/fr/le-droit-de-rectification. (Accessed 21 September 2018).
[85]LIL, Article 84 ff.
[86]LIL, Article 85.
[87]LIL, Article 85-I.

hoeren@uni-muenster.de

See above for the right of erasure of data of minors.

Apart from the LIL, the following provisions are applicable to marketing by electronic means: article L. 34-5 and article R 10-1 of the CPCE, articles 226-1 *et seq.* and 226-16 *et seq.* of the Criminal Code[88] and a simplified standard no 48 of the CNIL.[89]

The protection covers natural persons only. The general rules on data processing apply[90]: data collection must be fair[91] and done for specific purposes.

The data subject must have consented to treatment,[92] and the controller must be pursuing a legitimate interest. There cannot be one single act of consent for two separate instances of data processing.[93] Sensitive data are excluded from processing.

Files must respect the rights of persons in accordance of GDPR: information, the right to object, the right of access, the right of rectification.

The rules applicable to individuals (BtoC) offer more protection than those applicable to professionals (BtoB).

In BtoC relations, anyone in principle may object to marketing. The principle is that it is prohibited to send marketing material by electronic means without the addressee's prior consent.[94] By consent the Act means "any display of free, specific and informed wishes by which a person accepted that personal data concerning them be used for direct marketing purposes"[95] (direct marketing is "the sending of any message intended to promote directly or indirectly goods, services, or the image of a person selling goods or providing services"). This opt-in principle includes two exceptions: if the person is already a customer and the products or services proposed are similar to those initially supplied and if the marketing is not commercial.[96] In any event, the person concerned must be able at any time during collection to object simply and free-of-charge to the use of their data.

The legislator has sought to strike a balance between knowledge of consumer behaviour and protection of the private data of those same consumers.

In 2008, "the CNIL took the view that sending advertising messages to mobile phones via Bluetooth technology should be tantamount to directing marketing by electronic mail".[97] This is not the solution that the Commission adopted.

---

[88]CNIL, La publicité par voie électronique, October 2016: https://www.cnil.fr/sites/default/files/atoms/files/_commerce-donnees_perso_publicite_electronique.pdf.

[89]CNIL, Norme simplifiée no 48: adopted in 2005, modified in 2012 and 2016: Deliberation no 2016-264 of 21 July 2016: CNILTEXT000026268805. See Debet et al. (2015), pp. 938 ff.

[90]LIL, Article 5 & Article 6.

[91]CNIL, Decision of 21 September 2011: https://www.cnil.fr/sites/default/files/typo/document/D2011-203_Pages_Jaunes.pdf. (Accessed on 21 September 2018).

[92]See Bretonneau (2015), p. 1112.

[93]CNIL, Decision No MED 2018-043 of 8 October 2018.

[94]CPCE, Article L 34-5 § 1er.

[95]CPCE, Article L 34-5 § 2.

[96]CPCE, Article L 34-1-1, § 4.

[97]Debet et al. (2015), p. 940.

hoeren@uni-muenster.de

In BtoB relations, marketing material may be sent to the business address of the person or entity without their prior consent if it is directly related to their business activity.[98] The professional has only a right of information and a right to object.

In point of fact it is a mixed system. Although the opt-in system seems to be promoted *a priori*, it includes many exceptions.

The data subject must be able to object simply and free-of-charge to the use of their data. Moreover, data cannot be stored for more than three years.

The principles of purpose and security must be complied with.

There are general provisions in the Civil Code,[99] the LIL, the Labour Code,[100] the Criminal Code[101] and many simplified standards of the CNIL[102] and one-off authorisations concerning biometrics.[103] The Act of 20 June 2018 has added clarifications about biometric data required for controlling access to workplaces and to devices and applications used as part of missions entrusted to employees, agents, trainees, or service providers.[104]

Employees must be informed beforehand of any surveillance system for places that are not open to the public.[105] All surveillance camera systems are subject to CNIL supervision.[106] It is in the context of this jurisdiction that it has called for a democratic debate on the new uses of CCTV cameras.[107]

Data processing is aimed at different domains: apart from surveillance cameras, geolocation of vehicles, intercepting and recording calls, access to premises and time-keeping supervision, work tools and personnel recruitment and management.[108]

Such surveillance systems are authorised if they are justified for billing services, ensuring the safety of people and property, monitoring working time; for complying

[98] Debet et al. (2015), p. 942.

[99] *Code civil*, Article 9.

[100] *Code du travail*, Article L 1121-1, Article L 1221-9, Article L 1222-3, Article L. 1222-4 and Article L. 2323-32.

[101] *Code pénal* (CP), Article 226-1 ff. and Article 226-16 ff.

[102] NS-051: CNIL, Deliberation no 2015-165, 04.06.2015: CNILTEXT000030750827; NS-057: CNIL, Deliberation no 2014-474, 27.11.2014: CNILTEXT000030048118; NS-042: CNIL, Delib. No 02-001, 08.01.2002: CNILTEXT000017653507. NS-046: CNIL, Delib. No 2005-002, 13.01.2005 *modifié par* Deliberation no 2005-277, 17.11.2005: https://www.cnil.fr/sites/default/files/atoms/files/ns-046-consolidee.pdf.

[103] AU-052 - CNIL, Deliberation no 2016-186, 30.06.2016: JORFTEXT000033156742 et AU-053 - CNIL, Delib. No 2016-187, 30.06.2016: JORFTEXT000033156699.

[104] LIL, Article 44-4°.

[105] *Code du travail*, Article L.1221-9 and Article L.1224-4.

[106] See the factsheets established by the French-CNIL: https://www.cnil.fr/sites/default/files/atoms/files/videosurveillance.pdf. (Accessed 21 Sept. 2018).

[107] https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-video. (Accessed 21 Sept. 2018).

[108] https://www.cnil.fr/sites/default/files/atoms/files/travail-vie_privee.pdf.

hoeren@uni-muenster.de

with a statutory or regulatory duty and supervising compliance with rules; for adapting resources. The processing must be necessary and proportionate.

Employees' e-mails are for work-use by default and may as such be consulted by the employer. However, employers may not have ready access to their employees' personal e-mails. Such access should be gained in the presence of the employee or after calling the employee or in the event of serious incidents. There are no longer any such restrictions when a legal investigation is underway.

Files on computer are for work purposes by default.

Messages sent by the employee via Facebook or the MSN messaging site are protected because such messages are "accessible only to those persons accredited by the interested party, in a very limited number" and form "a community of interests".[109] The absence of authorisation from users to share contents they publish on their profile make them private: accordingly employers cannot rely on such messages as a basis for dismissal.[110] Case law in this domain is prolific.[111]

Identifiers and passwords are confidential and are not to be passed on to the employer unless the absent employee has essential information on his/her workstation for continuing the business activity. In this case, the employer may demand the codes be disclosed if the network administrator is unable to provide access to the workstation.

The LIL contains specific provisions on the transfer of personal data to states that do not belong to the European Union.[112] It requires users to give consent before storing information on their equipment or when there is access to information already stored unless such data are required to ensure the best possible access to the information transmitted.[113]

In the event of a breach of personal data, the service provider must alert the CNIL "promptly".[114] The service provider must also alert the interested party unless protective measures are considered appropriate by the CNIL, that is, the provider has made the data incomprehensible to anyone not authorised to have access to them.

Self-regulation is little developed as yet (*cf.* above).

[109]Cass. Civ., 1, 10 *avr.* 2013, *pourvoi* no 11-19.530.

[110]Bourgeois (2017), pp. 376 ff.

[111]Bourgeois (2017), p. 377.

[112]LIL, Article 112ff.

[113]CNIL, Deliberation no 2013-378 of December 5, 2013, cookies and others technologies JORFTEXT000028380230.

[114]LIL, Article 83 II.

hoeren@uni-muenster.de

3 Data Protection in the Electronic Communications Sector

Apart from the European rules and opinions of the G20 group, the provisions on electronic communications have been integrated into the LIL (see *Titel II Chapter IV*). This Act includes general provisions on the processing of personal data and special provisions on the protection of privacy on line. Some of these have been the subject of CNIL resolutions or court rulings.

Then there are provisions in the special Acts such as the Act of 9 July 2004 on electronic communications and audio-visual communication services[115] taken up by articles L 32 *et seq.* of the CPCE.

The obligations are incumbent primarily on the controller and processor.[116] The LIL further covers the recipient, which is the person or entity authorised to receive the data other than the data subject, the controller, the processors and the persons or entities tasked with processing the data because of their positions. Currently, French law requires that the recipient be clearly identified.[117]

Under the CPCE, "Data relating to traffic means all data processed with a view to channelling a communication over an electronic communications network or for its invoicing".[118]

Under the same code, "Electronic communications means broadcasting, transmitting or receiving signs, signals, writing, images or sounds by electromagnetic means"[119] and "electronic communications network means any installation or any set of installations for transporting or disseminating and, as the case may be, other means of channelling electronic communications, especially means of switching and routing".[120]

French law generally makes a distinction between two types of communication: direct and indirect communication.[121] In the first instance, collection is directly from the person or entity holding the data; and in the second the data collected are transmitted to a recipient who in turn becomes the controller. This distinction notwithstanding, for indirect collection French law confines itself to referring to the rules for direct collection. With the entry into force of the GDPR, the deadlines for transmitting information is more precise and the nature of the information amended slightly.[122]

The rules on the confidentiality of correspondence in the context of electronic communications have been specified by the LRN of 7 October 2016 which has amended article L 32-3 CPCE. This article was supplemented by a decree of

[115] Act no 2004-669 of July 9, 2004, JORF 10 July 2004, 12483.
[116] LIL, Article 81 ff. Bourgeois (2017), pp. 39 ff.
[117] Bourgeois (2017), p. 48.
[118] CPCE, Article L 32-18°.
[119] CPCE, Article L 32-1°.
[120] CPCE, Article L 32-2°.
[121] Bourgeois (2017), pp. 139 ff.
[122] Bourgeois (2017), pp. 155 ff.

hoeren@uni-muenster.de

28 March 2017[123]: Operators and members of their personnel are bound to abide by the secrecy of correspondence. Secrecy covers the contents of the correspondence, the identity of the correspondents and, as the case may be, the heading of the message and the documents enclosed with the correspondence.

The aim is to protect the individual against infringements by the state and its agents (*C. pén.*, art. 432-9) and against infringement by any other person or entity (*C. pén.*, art. 226-15). The correspondence covered is any that is "emitted, transmitted or received". The message must be correspondence and be "personal", that is, addressed to one or more individualized persons.

For example, the CNIL fined Darty €100,000 for failing to ensure the security of data of customers having made an online request for after-sales service.[124] The sanction is generally imposed after a warning has been given. Sanctions have changed with the entry into force of the GDPR.

Article 34bis of the LIL includes specific rules for the public provision of electronic communications services over electronic communications networks open to the public.

Breach of personal data applies to "any breach of security entailing accidentally or unlawfully the destruction, loss, deterioration, disclosure of or unauthorised access to personal data processed in the context of the supply to the public of electronic communications services".[125]

In the event of any breach, the supplier must alert the CNIL promptly. The data subject need only be alerted if the breach infringes their personal data or private life.

For failure to comply with these obligations, the supplier is liable to five years' imprisonment and a fine of €300,000.[126]

The CNIL is the competent authority for data protection. It may request an advisory opinion of the others regulators (*e.g. Autorité de Régulation des communications électroniques et des postes*—ARCEP).

In addition to the possibility of issuing advisory opinions, the CNIL has a power of supervision over controllers and subcontractors. Before imposing administrative fines, the CNIL may issue a warning to the controller or processor and/or may issue a notice to amend the processing. It may also issue a call to order or an enjoinder to render compliant or limit, interrupt or even prohibit the processing, withdraw or refuse certification, suspend data flow to foreign countries, certifications and approvals.

The CNIL may also file observations or develop them verbally in criminal or civil proceedings, which may lead to penalties.

[123]Decree no 2017-428 of 28 March 2017 relative to the confidentiality of private electronic correspondence: JORF 30 March 2017.

[124]CNIL, Deliberation no SAN-2018-001 of January 8, 2018: CNILTEXT000036403140.

[125]LIL, Article 83 I.

[126]*Code pénal* (CP), Article 226-17-1 § 1er.

hoeren@uni-muenster.de

4 Data Protection and Digital Forensics

The Act of 20 June 2018 inserted a *new chapter XIII in the LIL*. Since the Ordinance of 12 December 2018 it is a new *title III*. There are also specific rules in the *Code of Criminal Procedure* (CCP) in articles 100 to 100-8 and in the Title on the procedure applicable to organized crime and delinquency,[127] in articles 706-95 to 706-95-10, and articles 706-102-1 to 706-102-9. These provisions were amended for the most part by the Act of 3 June 2016 reinforcing the fight against organized crime, terrorism and their financing and improving the effectiveness and safeguards of criminal procedure.[128]

All of the rules allow the interception of e-mails, the use of "MSI catchers", the interception of correspondence; access in all places to stored computer data that are displayed on screen, are captured, received or issued, and their recording, safeguarding and transmission.[129] The capture, fixing, transmission and recording of words spoken privately in private or public places or vehicles and the image of natural persons in a private place are also possible but obey different rules.[130]

A distinction must be made between remote access to stored data and real-time access.

In the case of remote access, the magistrate (*juge de la liberté et de la détention* (JLD)), to whom the case is referred by the public prosecutor (*procureur de la République*), and the examining magistrate (*juge d'instruction*) have jurisdiction. The ordinance authorising the measure must state the grounds for doing so.[131] Under penalty of invalidation, the data can be for no other purpose than investigating and finding that offences have been committed.[132]

In the case of real-time access to data, the examining magistrate may order such access since the Act of 14 March 2011[133] and the magistrate (JLD) since the Act of 3 June 2016 for expedited or preliminary investigations.[134] This makes it possible, then, to record, safeguard, and transmit computer files hosted on hard drives or removable discs. In both instances, under penalty of invalidity, the magistrate or examining magistrate must specify the offence in question, the exact location or detailed description of the systems of automated data processing and the duration of the operations.[135] The operations are conducted under the authority and supervision of the magistrate or examining magistrate.[136]

[127] Infringements in the scope of *Code de procédure pénale* (CPP), Article 706-73 and Article 706-73-1.

[128] Act no 2016-731 of 3 June 2016, JORF 4 June 2016.

[129] CPP, Article 706-102-1 to Article 706-102-3.

[130] CPP, Article 706-96, Article 706-96-1, Article 706-97, Article 706-98, Article 706-98-1, Article 706-99, Article 706-101 and Article 706-101-1 (new articles).

[131] CPP, Article 706-95-1 and Article 706-95-2.

[132] CPP, Article 706-95-3.

[133] Act no 2011-267 of March 14, 2011, JORF 15 March 2011, p. 4582. CPP, Article 706-102-1.

[134] CPP, Article 706-102-1 to Article 706-102-3.

[135] CPP, Article 706-102-3, §1.

[136] CPP, Article 706-95-4.

hoeren@uni-muenster.de

The interception of data relates to electronic communications. However, it does not cover the capture of speech or images,[137] operations for tracing mobile phones covered by articles 230-32 *et seq.* CPP on geolocation, the identification of subscribers on a confidential list, or the consultation of detailed invoices.

Interceptions may only be made in cases of serious offences when the maximum penalty is two years' imprisonment or more.[138]

Interceptions are possible in the context of an expedited or preliminary enquiry relating to one of the offences listed under article 706-73 of the Code of Criminal Procedure (especially offences relating to organized delinquency and crime) and under article 706-73-1 of the Code of Criminal Procedure (fraud as part of an organized ring, money laundering, etc.) Interception must be used exceptionally only: it may be used "when the inquiry so requires".

The examining magistrate (*juge d'instruction*) and the magistrate (*juge des libertés et de la détention* (JLD)) alone are authorised to order such interceptions.[139] The public prosecutor may ask them of the magistrate (JLD). The decision is not of a judicial character and is not subject to appeal.

For judicial investigations, the duration of these interceptions is 4 months, renewable under the same conditions as to form and duration.[140] Since the Act of 3 June 2016, the total duration of the interception cannot exceed one year, or two years for offences under articles 706-73 and 706-73-1 of the Code of Criminal Procedure.

When the examining magistrate is tasked with an inquiry to determine the causes of death or disappearance,[141] he or she may also order interceptions. These may not then exceed three months, which may be renewed.[142]

In the case of an expedited or preliminary inquiry, the magistrate (JLD) may authorise them for a maximum duration of one month. The authorisation is renewable once, under the same conditions as to form and duration.

Special provisions are applicable to lawyers, members of the judiciary, journalists and members of parliament.

Correspondence must be retained in full to safeguard the possibility of subsequent adversarial examination.

Recordings are placed in bags under judicial seal,[143] other than for data stored by the national platform for judicial interceptions (*Plateforme nationale des interceptions judiciaires* (PNIJ)).[144] Persons under investigation may request the

[137]Dourneau-Josette (2016), No 53.

[138]CPP, Article 100, §1. Dourneau-Josette (2016).

[139]See 21.1.

[140]CPP, Article 100-2. Judgement of the Criminal Chamber of the French Supreme Court of 10 May 2012, Appeal No 11-87.328, *Bull. crim.* No 116.

[141]CPP, Articles 74 and 74-1.

[142]CPP, Article 80-4.

[143]CPP, Article 100-4, §2.

[144]CPP, Article 230-45, §3.

hoeren@uni-muenster.de

cancellation of the recordings under judicial seal, independently of an appeal directed against an order refusing further expert examination of the interception CD-ROMs.[145]

Recordings are destroyed when the matter becomes time-barred.[146] A report is made out concerning the destruction,[147] except when the data is stored by the PNIJ.[148]

5 Data Protection and Electronic Surveillance for Security and Defence Purposes

The Ordinance of 12 December 2018 insert a new Title IV in the LIL. The LIL details the information the data subject should be made aware of by the controller or its representative. The data subject shall therefore be informed of:

1. The identity of the controller and, as applicable, the identity of its representative;
2. The purpose of the processing for which the data are intended;
3. The mandatory or optional character of the responses;
4. Any consequences, for the data subject, of not responding;
5. The recipients or categories of recipients of the data;
6. The rights the data subject has under the provisions of section 2 of the present chapter including the right to lay down instructions as to what will become of their personal data after their death;
7. Where applicable, any transfer of personal data to a non-member state of the European Community;
8. The time the categories of data processed are stored or, if impossible, the criteria used to determine such a time limit.[149]

The Act of 20 June 2018 specifies that "when such data are collected by means of questionnaires, the questionnaires must indicate the requirements in numbers 1, 2, 3 and 6".

"The controller is bound to take all proper precautions with respect to the character of the data and the risks with processing, to ensure the security of the data and especially to prevent them from being deformed, or damaged, or accessed by unauthorised third parties."[150]

Although the Code of Criminal Procedure contained provisions for electronic surveillance,[151] these have been broadened under the state of emergency and incorporated into the Code of Internal Security and Defence.

[145]Crim. 8 November 2011, *Bull. crim*. No 228.

[146]CPP, Article 100-6, §1.

[147]CPP, Article 100-6, §2.

[148]CPP, Article 230-45, §3.

[149]LIL, Article 116.

[150]LIL, Article 121.

[151]Enderlin (2015).

hoeren@uni-muenster.de

The *Code of Criminal Procedure* has specific rules for developing automated files and for placing people under electronic surveillance. Its scope has been gradually extended and clarified.[152] Placement under electronic surveillance may be fixed[153] or mobile.[154] Implementation of placement under electronic surveillance is approved by the Justice Minister and must "ensure respect for the dignity, integrity and privacy of the person".[155] A memorandum (*Circulaire interdirectionnelle*) of 28 June 2013 from the Justice Minister provides guidelines for placement under electronic surveillance.[156]

The *Code of Internal Security* includes provisions about the electronic surveillance of persons for whom there are good grounds to believe that their behaviour is a particularly serious threat to security and to law and order.[157] This is an alternative to the person periodically reporting to the police introduced by the Act of 30 October 2017.[158] In this event, it is the Minister of the Interior who proposes the measures after having informed the public prosecutor for Paris and the locally competent public prosecutor. The person must necessarily give their written consent. Placement under mobile electronic surveillance is decided on for the duration of the measure. It may be ended at the request of the person concerned.

"The person concerned is subject for the duration of the placement to wearing a technical device enabling the administrative authority at all times to ensure remotely that they have not left the area defined under paragraph 1 of the same article L. 228-2. The technical device cannot be used by the administrative authority to locate the person unless they have left the area or in the event of malfunction of the said technical device." The arrangement is applicable until 31 December 2020.

The practical modalities are determined by a decree of the *Conseil d'État*.[159] The administrative authority must ensure that the person has been informed about how the device operates. The decision to place someone under mobile electronic surveillance must state the grounds for doing so.

The Act of 24 July 2015 on intelligence authorises correspondence to be intercepted where of necessity for public interest.[160] A decree of 29 June 2018 authorises certain departments of the police force to intercept correspondence exchanged over electronic communication networks to counter illegal immigration.[161]

[152]CPP, Article 142-5 to Article 142-13; Article 723-7 to Article 723-13-1 and Article R 57-10 to Article R 57-30-10.

[153]CP, Article 132-26-1 to Article 132-26-3 and CP, Article 132-26 will apply as of 24 Mars 2020.

[154]CP, Article 131-36-9 to Article 131-36-13.

[155]CPP, Article 723-8, §2.

[156]NOR: JUSD1317006C. This circular replaces the previous circular of December 23, 2005.

[157]*Code de la sécurité intérieure* (CSI), Article L 228-3.

[158]Act no 2017-1510 of 30 October 2017, JORF 31 October 2017.

[159]Decree no 2018-167 of 7 March 2018, JORF 9 March 2018, text no 5.

[160]CSI, Article L 801-1.

[161]Decree no 2018-543 of 29 June 2018, JORF 30 June 2018, text no 2.

hoeren@uni-muenster.de

Alongside this new measure, the Act of 30 November 2015 on surveillance measures for international electronic communications[162] has introduced into the Code of internal security a chapter on "Surveillance measures for international electronic communications".[163]

It should be added that the *Defence Code* has provisions designed to ensure the security of state and operator information systems.[164]

6 Remedies and Sanctions

Failure to comply with the rules for personal data protection is a matter of public policy. There are administrative, criminal, and civil law sanctions.

Victims may file a complaint with the CNIL but they may also seek remedy via the public prosecutor's office and the fraud office (DGCCRF).

Should rules on data protection be disregarded, the CNIL may impose administrative penalties.[165] Appeals against its decisions may be made to the *Conseil d'État* within one month. More specifically, the CNIL may impose penalties after issuing notice that is not acted on, issuing warnings, fines, injunctions, after withdrawal of CNIL authorisation, and the lockdown of data for three months. These penalties have been gradually increased. The maximum penalty, which was raised from €150,000 to €3 million by the LRN, has been raised again. It may now come to €10 million or 2% of the total worldwide annual turnover for the preceding financial year[166] and in cases covered by the GDPR €20 million or 4%.[167] Moreover the select committee may now impose penalties without prior notice.[168]

Under articles 226-16 to 226-24 of the Criminal Code, the various offences may give rise to up to five years' imprisonment and a €300,000 fine. The usual appeals in criminal law may be made.

By way of civil law penalties, the data transfer operation may be cancelled if the formalities are not observed.[169] A first class action was created by the Act of 20 January 2017 to enable associations to force compliance. A second for remedy for damage arising from a breach of personal data was introduced by the Act of 20 June 2018.[170]

[162] Act no 2015-1556 of 30 November 2017, JORF 1 December 2015, p. 22185.

[163] CSI, Article L 854-1 to Article 854-9.

[164] Code de la défense, Article L 2321-3 and Article L 2321-4.

[165] LIL, Articles 20 ff; Decree No 2019-536, Article 38 ff.

[166] LIL, Article 20 III.

[167] LIL, Article 20 III and GDPR, Article 83, §§ 5 & 6.

[168] CNIL, Deliberation no SAN-2017-012 of 16 November 2017.

[169] Judgement of the Commercial Chamber of the French Supreme Court of 25 June 2013, Appeal No 12-17037.

[170] LIL, Article 37.

hoeren@uni-muenster.de

In the event of misuse of personal data for marketing purposes, the CNIL complaints department may be seized as may the public prosecutor's office. The victim may also take the matter to a national platform for combatting spam.[171]

Employees may object to the installation of devices that fail to comply with the statutory conditions set out in the legal texts or by the CNIL. Should rules on data protection be disregarded, employees may take the matter to the CNIL, the work inspectorate or the public prosecutor's office.

In the event of fraudulent access to a system, other rules of the Criminal Code apply.[172] There are also a number of offences under general law (*e.g.* data theft is punishable by a €75,000 fine and five years' imprisonment). Forgery may be punished in both criminal and civil law.

7 Private International Law Rules

The CNIL has jurisdiction whenever the controller is based on French soil, or if not based in France whenever the controller implements means of processing located in France.

The Act of 3 June 2016 strengthening the fight against organized crime, terrorism and their financing and improving the effectiveness and safeguards of criminal procedure introduced a new article 113-2-1 to the Criminal Code, which reads:

> Any serious offence committed using an electronic communications network, where it is attempted or is effected to the prejudice of a natural person residing in the territory of the Republic or a legal entity whose head office is in the territory of the Republic, is deemed to be committed in the territory of the Republic.

Whenever a company based outside the European Union uses means of processing located on French soil, then French law applies, as in a recent example involving WhatsApp.[173]

Where data transfer is concerned, European rules were introduced by the Act of 6 August 2004 and others by the Act of 20 June 2018.

Data may only be transferred to a state not belonging to the European Union if the level of protection of the recipient state is adequate.[174] However, an exception is provided whenever the data subject has expressly consented to the transfer of their data or because of the nature of the data.[175] The CNIL may also decide to authorise the transfer.

[171] Association "Signal Spam": www.signal-spam.fr or Service 33700 (www.33700-spam-sms.fr).

[172] CP, Articles 323-1 ff.

[173] CNIL, Dec. no MED-2017-075 of 27 November 2017.

[174] LIL, Article 123.

[175] LIL, Article 124.

hoeren@uni-muenster.de

In addition, there are transfers of data or authorisations to transfer data already transmitted to a state not belonging to the European Union. In this event, a new transfer cannot in principle be made, saving exceptions.

Whenever any act constituting an offence is committed in France, then French criminal law applies in principle.[176]

References

Bossi-Malafosse J (2018) Le traitement des données de santé et le Règlement européen sur la protection des données du 27 avril 2016, Comm., com. électr., Dossier: Article 12, 58–61

Bourgeois M (2017) Droit de la donnée. LexisNexis, Paris

Bretonneau A (2015) Prospection commerciale: le consentement de l'utilisation doit être exprès. AJDA 19:1112–1115

Carrera Mariscal A (2018) Le CIL: modèle type du futur délégué à la protection des données? Dalloz IP/IT, no 4, 233–239

Charrier B (2018) Le consentement exprimé par les mineurs en ligne, Dalloz IP/IT, no 6, 333–337

Conseil d'État (2014) Étude annuelle du Conseil d'État – Le numérique et les droits fondamentaux. La Documentation française, Paris

Debet A (2018) Le consentement dans le RGPD: rôle et définition. Comm., com. électr., Dossier: Article 9, 37–44

Debet A, Massot J, Metallinos N (2015) Informatique et Libertés – Protection des données à caractère personnel en droit français et européen. Lextenso éditions, Paris

Desgens-Pasanau G (2018a) La protection des données personnelles. LexisNexis, Paris

Desgens-Pasanau G (2018b) Le délégué à la protection des données, pierre angulaire du principe de responsabilité (accountabiliy), Comm., com. électr. No. 4, Dossier: Article 6, 25–29

Dossier Dalloz IP/IT (2018) L'adaptation de la Loi informatique et libertés au RGPD, Dalloz IP/IT no 9, 458–484

Dossier Entrée en vigueur du Règlement général sur la protection des données: quels changements pour les responsables de traitement (Debet, Anne, Metallinos, Nathalie, Perray, Romain) (2018), Comm., com. électr., no 4, 7–96

Dourneau-Josette P (2016) Interceptions de correspondances émises par la voie des télécommunications électroniques. Rép. Proc. Pén., Dalloz, Paris

Enderlin S (2015) Placement sous surveillance électronique fixe ou mobile. Rép. Proc. Pén., Dalloz, Paris

Falque-Pierrotin I (2013) Le droit souple vu de la CNIL: un droit relais nécessaire à la crédibilité de la régulation des données personnelles. Conseil d'État, Étude annuelle 2013 - Le droit souple, 239–256

Fauchoux V, Deprez P, Dumont F, Bruguière J-M (2017) Le droit de l'internet. LexisNexis, Paris

Fauvarque-Cosson B, Maxwell W (2018) Protection des données personnelles (décembre 2016-mai 2018), D., no 19, 1033–1050

Foret O (2018) Le droit à l'oubli des mineurs, Dalloz, IP/IT no. 6, 350–352

Hébert P (2018) RGPD et projet de loi Informatique et Libertés, Comm., com. électr., no. 4 Dossier: Article 2, 9–10

Martial-Braz N (2018) L'abus de textes peut-il nuire à l'efficacité du droit?, Dalloz IP/IT, no. 9, 459–463

[176] CP, Article 113-2 ff.

hoeren@uni-muenster.de

Nicolas-Vullierme L (2018) Algorithme et orientation des bacheliers: avancée ou recul des droits fondamentaux? Published on 26 June 2018, https://audeladudroit.fr/algorithme-droits-fondamentaux, ISSN no. 2607-5881
Perray R (2018) La gouvernance, Comm., com. élec. 2018, no. 4, Dossier: Article 5, 19–24
Rochfeld J (2018) L'encadrement des décisions prises par algorithme, Dalloz IP/IT, no. 9, 474–479
Viney F (2018) La loi relative à la protection des données personnelles, AJ fam. 366–367

hoeren@uni-muenster.de

Data Protection in the Internet: National Report Germany

Christina Breunig and Martin Schmidt-Kessel

1 General Regulatory Framework on Data Protection

1.1 The Dual Basic Structure of the German Data Protection Law: European and National Origins

The protection of personal data is a fundamental right, both under EU and German legislation. It is rooted in Art. 8 European Convention on Human Rights ("ECHR")[1] and Art. 7 and 8 EU Charter of Fundamental Rights ("Charter").[2] The Charter became legally binding with the entry into force of the Treaty of Lisbon in 2009. In Germany, the right to data protection falls within the scope of the right to individual self-determination with respect to information; this fundamental right is not explicitly mentioned in the constitution but was drawn from Art. 2 para. 1 GG and Art. 1 para. 1 GG by the Federal Constitutional Court ("BVerfG").[3]

On 14th of April 2016, the EU has adopted the General Data Protection Regulation ("GDPR")[4] within its Digital Single Market Strategy.[5] The GDPR replaces the

[1]Convention for the Protection of Human Rights and Fundamental Freedoms.

[2]Charter of Fundamental Rights of the European Union, 2012/C 326/02.

[3]BVerfG, judgment of 15 December 1983—Volkszählungsurteil—BVerfGE 65, 1 = NJW 1984, 419; commented from a current point of view by Kühling (2017), p. 3069; see infra Sect. 1.2.

[4]Regulation (EU) 2016/679 (GDPR).

[5]See for more information: A Digital Single Market Strategy for Europe, COM(2015)192 final.

C. Breunig (✉) · M. Schmidt-Kessel (✉)
University of Bayreuth, Centre for Consumer Law, Bayreuth, Germany
e-mail: Martin.Schmidt-Kessel@uni-bayreuth.de

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_7

hoeren@uni-muenster.de

outdated Data Protection Directive[6] from 1995 and shall apply from 25 May 2018.[7] It is directly applicable in all Member States and guarantees a wide range of rights of the persons affected.[8] Member states may provide for more specific rules in respect of specific processing situations such as the involvement of minors, in the employment sector and in context with the right of freedom of expression and information.[9]

Besides, the EU data protection framework contains specific rules for data processing in the communication sector,[10] by prosecution authorities[11] and by EU entities.[12] All provisions have to be interpreted in light of the fundamental right to protection of personal data.

German legislation implements the EU standards. The former version Federal Data Protection Act ("old BDSG")[13] contained general aspects and basic principles of data processing while there was (and still is) specific legislation especially in the telemedia, communications and public sector.[14] Because the GDPR will largely invalidate the provisions of the old BDSG from the date of its application, an entirely new act, the "new BDSG", making use of the opening clauses was established in summer 2017.[15] Alongside, each region (federal state) has its own regional data protection act. They are, however, not introducing any new standards and mainly apply to public institutions and organize the regional data protection authorities.

This national report is written on the basis of the GDPR considering German particularities.

1.2 Basic Notions

1.2.1 Notion of Personal Data and General Perspective of Protection

Personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more

[6]Directive 95/46/EC.

[7]Art. 99 para. 2 GDPR.

[8]Art. 99 para. 2 GDPR; cf. Art. 288 para. 2 Treaty on the Functioning of the European Union (TFEU).

[9]Art. 8 para. 2, Art. 85 *et seq*. GDPR.

[10]ePrivacy directive 2002/58/EC, adapted by directive 2009/136/EC; new proposal: ePrivacy regulation COM(2017) 10 final, is discussed.

[11]Framework decision 2008/977/JI; replaced by directive 2016/680.

[12]Regulation (EC) No. 45/2001; new proposal, COM(2017) 8 final is discussed.

[13]Bundesdatenschutzgesetz.

[14]*E.g.* Telemedia Act (TMG), Telecommunications Act (TKG), tax regulation (AO, EStG) and regional and federal police regulation Acts (PAG, BPolG).

[15]Established by article 1 of the Act of June 30, 2017, Federal Official Journal 2017, I, 2097.

hoeren@uni-muenster.de

factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person", Art. 4 para. 1 GDPR. The ECJ decided in *Dynamic IP addresses*,[16] that dynamic IP addresses are personal data and thus data protection rules apply on the processing of them.[17]

Personal data protection is recognized as a specific fundamental right in Art. 8 of the EU-Charter of fundamental rights and must be ensured by the EU institutions and by all Member States of the EU (as far as applying EU law). In Germany, the right to personal data protection is not explicitly laid down. The Federal Constitutional Court has derived the right to individual self-determination with respect to information from Art. 2 para. 1 GG and Art. 1 para. 1 GG in the pioneering census verdict in 1983.[18] Therefore, German law is focusing data protection as a particular personality right and is not based on a separation between private data in the literal sense of *privacy* and public data.

1.2.2 Categories of Personal Data

Personal data is classified in *personal data* in general, *special categories of personal data* and *personal data relating to criminal convictions and offences*. *Special categories of personal data* are "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation", Art. 9 para. 1 GDPR. On the processing of these particular data stricter requirements apply.[19]

1.2.3 Scope of Application of the Several Instruments on Data Protection

The GDPR is in general applicable to the processing of personal data by any entity, also public entities. However, whereas the basic principles are identical for private and public bodies, the GDPR contains a row of particular rules for public bodies.

[16]ECJ, judgment of 19 October 2016—Breyer—C-582/14 = EuZW 2016, 909.

[17]The decision was followed by the German Federal Supreme Court für Civil Law and Criminal Law, the Bundesgerichtshof (BGH), in BGH, judgment of 16 May 2017, VI ZR 135/13 = NJW 2017, 2416.

[18]BVerfG, judgment of 15 December 1983—Volkszählungsurteil—BVerfGE 65, 1 = NJW 1984, 419.

[19]The processing of special categories of personal data shall generally be prohibited, Art. 9 para. 1, if no exception applies, Art. 9 para. 2 GDPR. Personal data relating to criminal convictions and offences shall generally be carried out only under the control of official authority, Art. 10 GDPR. See for stricter requirements *e.g.* Art. 22 para. 4, Art. 30 para. 5, Art. 35 para. 3 lit. b), Art. 37 para. 1 lit. c) GDPR.

hoeren@uni-muenster.de

Moreover, the GDPR is not applicable on police and judicial cooperation in criminal matters and data processing by EU entities. The BDSG (in the new as well as in the old version) distinguishes between data processing by federal public bodies and data processing by private bodies and public-law enterprises participating in competition, but usually does not apply to regional public bodies. Data processing by regional (state) public bodies is as a rule regulated on the state level by state data protection law.

1.3 German Supervisory Authorities for Data Protection

Member States of the European Union shall provide for one (or more) independent public supervisory authority responsible for monitoring the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to data processing, Art. 51 para. 1 GDPR. The Federal Commissioner for Data Protection and Freedom of Information monitors data processing by public entities of the federal government, also by such participating in competition, *de jure* under old legislation (old BDSG) and the new Act (new BDSG). The Federal Commissioner is an independent supreme federal authority.[20] Regional public entities and non-public entities are monitored by state representatives.[21]

Moreover, data processing by private entities is controlled by consumer associations that can file a move for an injunction in case of data protection violations in (unfair) terms and conditions,[22] if data is illegally used for commercial purposes[23] or in case of violations of unfair competition law.[24] Additionally, data processing is *de facto* monitored by new Watchdog institutions, the so-called *Marktwächter*, mainly financed by the government and mainly ran by the most important consumer associations, which can inform the general public and the state representatives for data protection in case of data protection shortcomings.[25] Within enterprises, internal data protection officers are usually established to monitor all aspects of data processing. Also, works councils exert influence on the data processing of employees through their right to codetermination.

[20]Sec. 22–26 old BDSG, Sec. 8–16 new BDSG.

[21]Sec. 38 old BDSG, Sec. 40 new BDSG.

[22]Sec. 1 Injunctions Act (UKlaG).

[23]Sec. 2 para. 2 no. 11 UKlaG.

[24]Sec. 3a Unfair Competition Act (UWG).

[25]The exact legal status of these Marktwächter institutions is under discussion.

hoeren@uni-muenster.de

1.4 Tasks and Powers of the Different Supervisory Authorities

The federal structure of Germany excludes the possibility of one single supervisory body, see Art. 83 GG. Instead, administrative supervision of private bodies is usually organized by the regional agencies in the federal states. Only federal public bodies (and public enterprises) are controlled by the federal agency. Beyond the split between public and non-public bodies as well as between federal and regional entities, there is a (federal) sectorial supervisory body in the communication sector, the Federal Network Agency.[26]

The powers of supervisory authorities are laid down in Art. 58 para. 1 to para. 3 GDPR. Supervisory authorities shall have investigative, corrective and authorization as well as advisory powers. Member states may provide for additional powers, Art. 58 para. 6 GDPR. Sec. 16 new BDSG specifies the provisions of Art. 58 GDPR for the federal agency; for the regional agencies the state laws do or will do it similarly.

Under the GDPR administrative fines have increased tremendously in Germany. While the scope was formerly under German law up to 300,000 Euros,[27] supervisory bodies can now impose fines up to 20 million Euros or 4% of the annual group turnover, Art. 83 GDPR. Key element thereby is their independence and being subject only to the law, Art. 52 GDPR.

1.5 The Role of Self-Regulation Instruments

The GDPR introduces self-regulation instruments.[28] Enterprises shall be encouraged to the drawing up of codes of conduct to promote the implementation of data protection provisions, Art. 40 GDPR. Moreover, the GDPR seeks the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with data protection rules, Art. 42 GDPR. The adherence to such measurements may be used as an element by which to demonstrate compliance with the obligations under the GDPR, Art. 24 para. 3 GDPR and can thus lead to privileged treatment.

[26]Sec. 116 *et seq*. TKG. For the constitutional basis see Art. 87 *et seq*. GG.

[27]Sec. 43 para. 3 old BDSG.

[28]For more information on self-regulation instruments see Spindler (2016), p. 407; Kranig and Peintinger (2014), p. 3.

hoeren@uni-muenster.de

2 Data Protection in the Internet

2.1 Personal Data Processed by Electronic Means

2.1.1 Particular Legislation

The GDPR does, as a starting point, apply on the protection of personal data in the context of services provided at a distance, by electronic means, at the individual request of a recipient of services. However, it does not contain any specific rules. More rules that are specific are established by the ePrivacy Directive 2002/58/EC ("ePD") which probably will soon be replaced by a new ePrivacy Regulation ("ePR").[29]

The German Telemedia Act ("TMG") contains specific rules covering the protection of personal data in the internet sector, which would be applicable to services provided at a distance, by electronic means, at the individual request of a recipient of services. These rules also apply to social networks if not communication in itself is concerned. The rules established by the TMG will most likely to a large extent be overridden by the GDPR as of May 2018. Art. 95 GDPR, concerning the relation between the GDPR and national legislation based on the ePD,[30] states that the GDPR shall not impose additional obligations in relation to processing in relation to matters which are subject to specific obligations with the same objective set out in the ePD. Recital 173 GDPR clarifies that national legislation adopted to implement the ePD shall be given priority of application over contrary rules laid down in the GDPR. It is therefore essential to distinguish in a very accurate way between national rules, that have only been adapted to implement the requirements of the ePD and those that have not been adapted for precisely that reason. In the first case, but not in the second, national legislation exceptionally prevails; in the second case, the respective rule will be overridden by the GDPR.[31]

The rules of the TMG, in particular the ones relevant for the situation at hand, sec. 11 *et seq*. TMG, are not based on the ePD. Therefore, they do not fall within the scope of Art. 95 GDPR. From May 2018, the GDPR prevails over the relevant provisions of the TMG. If however, the new proposal for an ePR will be adopted, that regulation will prevail the national rules, which are not replaced by the GDPR (the rules that have been based on the ePD).

The ePR aims to complement the GDPR and modernize data protection in the specific field of electronic communications.[32] The GDPR would then be the general

[29]See the Proposal by the European Commission for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

[30]ePrivacy directive 2002/58/EC, adapted by directive 2009/136/EC.

[31]For the relation between GDPR and TMG see: Keppeler (2015), pp. 779 *et seq.*; Nebel and Richter (2012), pp. 407 *et seq*.

[32]See Schmitz (2017), p. 172 concerning the ePR.

hoeren@uni-muenster.de

data protection framework, subsidiary to the more specific rules of the ePR. Any data processing in context to electronic communications not being within the scope of the ePR, would be subject to the rules laid down in the GDPR.[33] There would be no room left for specific national legislation. We will answer the following questions assuming this scenario. The processing of personal data in context of services provided at a distance, by electronic means, at the individual request of a recipient of services, would then be regulated by the ePR and subsidiarily by the GDPR. None of those regulations provides for any specific legislation concerning services provided at a distance.

2.1.2 Particular Rules Applicable

Specific Protection for the Data Subject

The proposed ePR protects data subjects by regulating the use of tracking and third party cookies in Art. 8 and 9 ePR. The (amending) rules of the GDPR do not contain specific protection for the data subject in the context of services provided at a distance. The GDPR establishes general information duties, Art. 12–14 GDPR. The information has to be given in a transparent easily accessible form, using clear language. The information can be provided in writing, or by other means, including electronic means, where appropriate, Art. 12 GDPR. Besides the principles of data protection laid down in Art. 5 para. 1 GDPR apply.[34]

An additional point to be noted is the existence of specific consumer protection by contract law[35] in the situation at hand, introduced in transposition of the Consumer Rights Directive.[36] On the one hand, such rules are without direct effect on the legality of data processing. On the other hand, they might produce significant consequences as to the legitimation of the responsible person.

The Role of Previous Consent of the Data Subject

Electronic processing of personal data is subject to general data processing rules on consent.[37] A general principle of data protection both on EU and national level is the prohibition of processing of personal data without permission. The processing of

[33]Pohle (2017), p. 05452.

[34]The principles of data protection include the principle of lawfulness, fairness and transparency, the principle of purpose limitation, the principle of data minimization, the principle of accuracy, the principle of storage limitation, the principle of integrity and confidentiality and the principle of accountability, Art. 5 para. 1 GDPR.

[35]Especially sec. 312 *et seq*. of the German Civil Code deal with consumer protection in context with services provided by distance.

[36]Directive 2011/83/EU.

[37]These rules do not differentiate between electronic or non-electronic processing of personal data.

hoeren@uni-muenster.de

personal data is thus generally prohibited unless permitted by law or the previous consent of the data holder, Art. 6 GDPR. In case of permission by the law, no consent is necessary as far as the data processing is covered by that legal permission.

Conditions of previous consent are named in Art. 7 GDPR and by the definition in Art. 4 para. 11 GDPR. Art. 9 para. 1 of the proposed ePR refers to the understanding of consent in terms of the GDPR. Art. 9 para. 2 of the proposed ePR offers the possibility of expressing consent by using appropriate technical settings of a software application.

The GDPR contains a comprehensive set of rules under which processing without previous consent is allowed, Art. 6 para. 1 lit. b)–f) GDPR. A major role in the internet sector play Art. 6 para. 1 lit. b) and f) GDPR. Art. 6 para. 1 lit. b) allows the processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Art. 6 para. 1 lit. f) permits the processing necessary for the purposes of the legitimate interest pursued by a private body as controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Moreover, in the last case the data subject has a right to object the data processing under certain conditions, Art. 21 GDPR.

Processing of Personal Data Limited to Specific Purposes

As the electronic processing is determined by general rules,[38] it is not generally limited to specific purposes or specific types of data. However, consent has to be given only for specific and specified purposes[39] and under all legal permissions procession is only allowed for the purposes for which the data processing is permitted, so-called principle of purpose limitation.[40]

Import criteria, if the processing is lawful, are the *necessity* of the processing, so called principle of data minimization.[41] This is even more significant in the context of electronic processing as risks and interests of the data subjects are affected somewhat stronger. The processing shall consequently always be proportional to the concrete purpose of the processing.

[38] See the section "The Role of Previous Consent of the Data Subject".

[39] See Art. 6 para. 1 lit. a) GDPR.

[40] The principle of purpose limitation is laid down in Art. 5 para. 1 lit. b) GDPR.

[41] The principle of data minimization is laid down in Art. 5 para. 1 lit. c) GDPR; see also the wording of Art. 6 para. 1 lit. b)–f) GDPR.

hoeren@uni-muenster.de

Protection for Minors

Art. 8 para. 1 GDPR states that a child must at least be 16 years old to give valid consent in the processing of its personal data in relation to the offer of information society services. Where the child is younger, the consent of a legal representative is necessary. Member states may lower down that age, nonetheless not below 13 years, Art. 8 para. 2 GDPR. The fundamental rights and freedoms of a child being a data subject have explicitly to be considered in determining the necessity of processing for purposes of the legitimate interests of the controller, Art. 6 para. 1 lit. f) GDPR.

Minors are furthermore protected by general rules of contract law. Under German law, legal capacity and thus the ability to enter into a valid contract starts from the age of 18, sec. 104 *et seq*. German Civil Code. There are, of course, exceptions but these do mainly only work combined with the consent of a legal representative. Whether these contract law rules apply to consent of the minor, was subject to discussion under the old BDSG.

The "Right to Be Forgotten"

The *right to be forgotten* is explicitly guaranteed in Art. 17 GDPR. It comprises two rights. First, the data subject has the right to obtain erasure of its personal data without undue delay if a special ground, *e.g.* withdrawal of consent, applies. The controller has the corresponding obligation to erase its personal data without undue delay, Art. 17 para. 1 GDPR. Second, if the personal data has been made public, reasonable steps have to be taken by the controller to inform other controllers that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data, Art. 17 para. 2 GDPR. The *right to be forgotten* is limited to the extent that the processing is necessary for specific reasons like for the right of freedom of expression and information, Art. 17 para. 3 GDPR.

The ECJ hold in *Google vs. Spain*, that an internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties. Thus the data subject may approach the operator directly in order to obtain the removal of a link to a web page, which contains information on the data subject, from the list of results.[42]

2.1.3 Electronic Communications for Marketing Purposes

There is general legislation covering the protection of personal data in the context of electronic communications for marketing purposes. Recital 47 of the GDPR states that direct marketing purposes may be regarded as carried out for a legitimate interest. Marketing purposes may thus be a legitimate interest in terms of Art.

[42]ECJ, judgment of 13 May 2014—Google vs. Spain—C-131/12 = EuZW 2014, 541.

hoeren@uni-muenster.de

6 para. 1 lit. f) GDPR[43] and consequently may provide a legal basis for the processing of personal data.

The protection of personal data in the context of electronic communications for marketing purposes is also specifically addressed in Art. 13 ePD. The requirements laid down in the directive are mainly implemented by the Telecommunications Act ("TKG") and the TMG. Advertising issues are also addressed in the Unfair Competition Act ("UWG"),[44] where in particular cold calling is prohibited and sanctioned in § 7 UWG. The ePR would, in case of its adoption, introduce new rules concerning direct marketing.[45] The Federal Court of Justice ("BGH") dealt with the protection of personal data in the context of advertising. The Court held that the unsolicited forwarding of advertisement by e-mail and of electronic newsletters is inadmissible under the rules of unfair competition.[46]

2.1.4 Particular Protective Mechanisms for Electronic Marketing Communications

The GDPR generally establishes an opt-in system to the extent that personal data may only be processed if the consent of the data subject has been obtained, Art. 6 para. 1 lit. a) GDPR. If, however, the requirements, as set out in Art. 6 para. 1 lit. f) GDPR, are met, there is an opt-out system, because processing in accordance with these requirements is allowed. How far one could analyze this situation in terms of a mixed system depends on the interpretation and concretization of the general clause of the legitimate interests pursued by the controller within Art. 6 para. 1 lit. f) GDPR. Particularly for marketing purposes, § 7 of the German UWG prohibits certain practices typically based on personal data as far as not legitimized by previous consent of the data subject. This prohibition transposes rules from the ePD.

Following these lines, the ePR will (probably) state that electronic communications services may be used for the purposes of sending direct marketing communications to end-users who are natural persons if those persons have given their consent, Art. 16 para. 1 ePR. This constitutes principally an opt-in system. However, member states can provide for an opt-out system concerning direct voice-to-voice calls, Art. 16 para. 4 ePR.

In case of an existing customer relationship, the obtained contact details may be used for direct marketing of similar products or services. Nonetheless, the customer shall clearly and distinctly be given the right of objection at any time, Art. 16 para.

[43] See the section "The Role of Previous Consent of the Data Subject" for the wording of Art. 6 para. 1 lit. f) GDPR.

[44] It is disputed in literature if the requirements of the Cockie directive are implemented in its entirety, see Auer-Reinsdorff and Conrad (2016), § 36, paras. 9 *et seq*.

[45] See Sect. 2.1.1.

[46] BGH, judgment of 20 May 2009, I ZR 218/07 = NJW 2009, 2958; BGH, judgment of 11 May 2004, I ZR 81/01 = GRUR 2004, 517.

hoeren@uni-muenster.de

2 ePR. Therefore, concerning the specific situation of an existing customer relationship, there is an opt-out system for direct marketing of similar products or services.

Additional protection for the data subject in the context of electronic communications for marketing purposes will be granted by Art. 16 para. 3 ePR. Accordingly, in the context of direct marketing calls, the phone number has to be displayed or a special pre-fix, that indicates a marketing call, has to be used. Additional protection for data subjects is guaranteed by general contract law. The BGH on the basis of § 7 UWG held that it is unlawful to obtain the data subject's consent in the reception of advertising e-mails by signing general terms and conditions.[47]

2.1.5 Employees as Data Subjects

The GDPR does not contain legislation regulating the processing of personal data of employees through electronic means. It contains an opening clause allowing member states to provide for specific rules to ensure the protection of rights and freedoms in respect of the processing of personal data in the context of employment, Art. 88 para. 1 GDPR.

The old BDSG regulates data processing of employees' personal data specifically in sec. 32. Germany made use from the opening clause in Art. 88 para. 1 GDPR, and included sec. 26 in the new BDSG dealing with employee data protection. The new rules are inspired by sec. 32 BDSG. In 2010 there have been efforts to introduce an Employee Data Protection Act but the proposal[48] has never been approved.

2.1.6 Particular Rules for Personal Data of Employees

The rules do not concern a special type of processing of personal data of employees through electronic means. They have to be applied depending on the individual case and situation like geolocation and performance monitoring.

Sec. 26 new BDSG allows data processing for employment-related purposes and for the detection of crimes. Employment-related purposes are given if the processing is necessary for hiring decisions, for carrying out the employment contract or for the termination of the employment contract, sec. 26 para. 1 s. 1 new BDSG. The processing for the detection of crimes is legally if there is a documented reason to believe the data subject has committed a crime while employed, sec. 26 para. 1 s. 2 new BDSG.

The processing must maintain the principle of proportionality. The general right of privacy of the employee has to be weighed against the legitimate interests of the employer in the processing of the employee's data for the purposes outlined above.

[47] BGH, judgment of 16 July 2008, VIII ZR 348/06 = MMR 2008, 731.

[48] BT-Drs. 17/4230.

hoeren@uni-muenster.de

There is no discussion so far on the question, to whom the values drawn from the employees' personal data shall be attributed under German labour law. Following general rules such questions might be dealt with by collective agreements.

2.1.7 Use of Electronic Means by Employees and Disciplinary Proceedings

The use of electronic means (also of social networks) by employees is not subject to particular legislation. The usage of such means is governed by general sources of employment law, namely collective employment law, including tariff agreements and works agreements, and individual employment law, determined by the employment contract. It thus depends on the individual case whether and to what extent the (private) use of electronic means by employees is allowed.

Due to his right of freedom of speech, Art. 5 para. 1 GG, the employee may criticize the employer on social networks. However, he also has a duty of loyalty to the employer and may deal out criticism only in an appropriate way. The Federal Labour Court held that a termination without notice due to a gross affront on Facebook can be justified.[49] Information gained from social media may be used within disciplinary proceedings. Even if it was gained infringing data protection rules, there from does not necessarily result an exclusion of that evidence.[50]

2.1.8 Obligations in Order to Protect Personal Data Conveyed and Stored Through Electronic Means

There are additional obligations in order to protect personal data conveyed and stored through electronic means laid down in the Act on the Federal Office for Information Security ("BSIG") adopted in 2015. The BSIG has been adapted to implement the provisions of the NIS-Directive.[51] It now contains increased demands on technical and organizational security measures to protect customer data and IT-systems used by them. A general digital product security law has not been established yet.

The GDPR also foresees the implementation of appropriate technical and organizational measures like pseudonymisation and encryption to ensure a high level of security, Art. 32 GDPR. Furthermore, it provides a set of rules concerning processors to safeguard that a high security level is also guaranteed where the processing is to be carried out on behalf of a controller, Art. 28 GDPR. The introduction of the principles of data protection by design and by default, Art.

[49]Federal Labour Court (BAG), judgment of 10 December 2009, 2 AZR 534/08 = NZA 2010, 698.

[50]Further elaboration on the use of social media by employees: Kort (2012), p. 1321; Bauer and Günther (2013), p. 67.

[51]Directive on security of network and information systems (EU) 2016/1148.

hoeren@uni-muenster.de

25 GDPR, strengthens the protection of personal data stored and conveyed through electronic means additionally as they minimize the personal data stored at all from the very beginning.

2.1.9 Particular Obligations to Inform About Data Breaches or Incidents Concerning the Security of Personal Data

In case of data breaches or incidents concerning the security of personal data processed by electronic means there might be an obligation to inform the supervisory authority and the data subject. Obviously, there may be additional duties under tort law and contract law.

The supervisory authority has to be informed if the data breach is not unlikely to result in a risk to the rights and freedoms of natural persons. The notification shall be given without undue delay and, where feasible, not later than 72 h after having become aware of the breach, Art. 33 GDPR.

A data breach is to be communicated to the data subject under the following presuppositions: First, the breach is likely to result in a high risk to the rights and freedoms of natural persons. Second, the controller has not implemented appropriate technical and organizational protection measures, such as encryption, or has not taken subsequent measures which ensure that the high risk is no longer likely to materialize. Third, the communication wouldn't involve disproportionate effort, Art. 34 GDPR.

2.1.10 Specific Sectorial Rules for the Processing of Personal Data by Electronic Means

There is specific legislation regarding the processing of personal data by electronic means in the health sector. The Social Security Code, Part V, specifies the requirements of a valid consent, coherent information duties and the withdrawal of the same in connection with the electronic health card. It also provides for technical precautions to guarantee protection from unauthorized access.[52]

The principle of legal prohibition, reserving the right of permission and the comprehensive but general set of rules, under which processing without consent is allowed, offers a wide legal basis of data processing.[53] This leads in an indirect way to sectorial special legislation.

[52]See sec. 291 lit. a) Social Security Code, Part V (SGB V).

[53]Concerning the principle of legal prohibition reserving the right of permission See the section "The Role of Previous Consent of the Data Subject".

hoeren@uni-muenster.de

2.2 Data Protection in the Electronic Communication Sector

2.2.1 Legislation for the Communications Sector

There are specific legal rules regarding the processing of personal data in the electronic communications sector.

First of all, the right to secrecy of telecommunications, which is a fundamental one, shall be pointed out. On EU level it is granted by Art. 7 EU of the Charter and Art. 8 ECHR.[54] The ePR nominates the confidentiality of electronic communications data in Art. 5. The German constitution guarantees the right to secrecy of telecommunications in Art. 10 GG. It is specified in sec. 88 para. 1 TKG.

The ePR contains specific legal rules regarding the processing of personal data in the electronic communications sector. So does the TKG on national level. If the ePR is adopted, all national legislation, including the TKG, concerning the communications sector will lose its legal ground. If the Regulation is not adopted, data processing in the communications sector will be subject to the GDPR and to the rules of the TKG intending to implement the ePD.[55] The following explanations are based on the assumption that the ePR is adopted.

2.2.2 General Structure of Data Protection in the Communications Sector

Personal Scope of Application

Subject to the rules of the ePR are entities providing electronic communications services publicly available.[56] According to the technical progress, the ePR has a broader scope of application than the ePD. It extends its application scope on over-the-top services ("OTTs") as carrier networks such as Facebook and on data transfer between machines (m2m-communication) as they form an essential part of Internet-of-Things ("IoT"-) applications.

The Notion of "Communication Data"

Electronic communications data means electronic communications content and electronic communications metadata, Art. 4 para. 3 lit. a) ePR.

[54] Koenig et al. (2009), p. 525.

[55] See for the relation between GDPR, ePR and national legislation Sect. 2.1.1.

[56] Art. 2 para. 1, para. 2 lit. c) ePR.

hoeren@uni-muenster.de

Categories of "Communication Data"

Electronic communications data is classified in two categories, electronic communications content and electronic communications metadata. *Electronic communications content* means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound, Art. 4 para. 3 lit. b) ePR. *Electronic communications metadata* means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication, Art. 4 para. 3 lit. c) ePR.

Confidentiality of Communication Data

The confidentiality of communication data is nominated in Art. 5 ePR and derives from the fundamental right to secrecy of communications.[57] Confidentiality of electronic communications data means that any interference with electronic communications data by persons other than the end-users shall be prohibited, except when permitted by the ePR.[58] Permissions are provided in Art. 6 ePR. Para. 1 contains general permissions of the processing of *electronic communications data*. Para. 2 then nominates permissions only regarding the processing of *electronic communications metadata*, whereas para. 3 names permissions to process *electronic communications content*.

Security Measures by the Electronic Communications Providers

There are no specific legal rules about the implementation of security measures by the electronic communications providers in order to protect personal data. Recital 37 ePR refers to Art. 32 GDPR.[59] A direct reference on that provision can be found in Art. 8 para. 2 lit. b) ePR.

In the case of risk of a breach of the security, the provider shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved, Art. 17 ePR.

[57] See Sect. 2.2.1.

[58] Art. 5 ePR.

[59] Directive on security of network and information systems (EU) 2016/1148.

hoeren@uni-muenster.de

Particular Rules on Data Breaches

Besides the duty to information about detected security risks laid down in Art. 17 ePR,[60] the Regulation does not contain any specific legal rules about data breaches, including any obligations to notify the data subject, a supervisory body or any other third party in case a data breach occurs. This situation falls within the subsidiary general rules of the GDPR, which establishes such duties in Art. 33 and 34 GDPR.[61]

2.2.3 The Federal Network Agency as Supervising Body

Under current national legislation, the Federal Network Agency monitors the adherence to the provisions laid down in the TKG. The ePR states that the processing of personal data in the context of electronic communications is monitored by the independent supervisory authorities responsible for monitoring the application of the GDPR, Art. 18 ePR. The provisions laid down in the GDPR shall be applicable mutatis mutandis.[62]

2.2.4 Powers Vested in the Federal Network Agency

If the ePR is adopted, there will probably be no specific supervisory body for the electronic communications context. The main types of powers vested in this supervisory body, including sanctioning powers, are the same as those of the supervisory authorities monitoring the GDPR.[63]

2.3 Data Protection and Inheritance

In July 2018 the BGH had to apply the GDPR for the first time.[64] The judgment brings clarification to the digital inheritance.[65] According to the key statement of the decision, the contract of a user account of social networks is transferred to the heirs by universal succession. In the case at hand, a girl was killed in an unsolved metro accident. The mother of the child claimed access to her Facebook account which was set into the so-called memorial state. In this state it is no longer possible to log in to

[60]Directive on security of network and information systems (EU) 2016/1148.

[61]See for the presuppositions for such duties Sect. 2.1.9.

[62]See for the provisions concerning the supervisory authorities monitoring the GDPR Sect. 1.3.

[63]See for the main powers of the supervisory authorities monitoring the GDPR Sect. 1.4.

[64]BGH, judgment of 12 July 2018, III ZR 183/17 = NZFam 2018, 800.

[65]See discussions of the judgement by Litzenburger (2018); Goratsch (2018), p. 810.

hoeren@uni-muenster.de

the account. The mother claimed access to the account, in particular to the communication in order to find out whether her daughter had suicidal thoughts. Furthermore she aimed to avert the metro drivers' claims for damages.

The BGH decided in favour of the mother when it held that the user account contract is transferred to the heirs by universal succession. The court created clarity in favour of the validity of inheritance law and ensured a balance between analogue and digital inheritance as social networks accounts are transferred to the heirs in the same way as letters or diaries. The Court found that data protection law does not prevent the access by the heirs. Since the regulation only protects persons alive, the interests of the testatrix are not affected. The processing of the data of the communication partners is justified by law. Firstly it is necessary in order to fulfil the contractual obligations towards the contractual partners on the basis of art. 6 para. 1 lit. b) GDPR. Secondly, the processing is justified on the basis of the legitimate overriding interests of the heirs, art. 6 para. 1 lit. f) GDPR.

2.4 Data Protection and Digital Forensics

2.4.1 Investigation, Detection and Prosecution of Crimes Through Electronic Means

Data processing by prosecution authorities is regulated by a new directive concerning the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences.[66]

National law distinguishes between crime prevention and prosecution of crime. Preventive measures are taken by the police and are thus subject to police law, mainly state police law (of the Bundesländer),[67] while the prosecution authorities are competent to take repressive measures according to the Code of Criminal Procedure ("StPO"). For illustration purposes is the following information based on Bavarian state police legislation, the PAG.[68] It addresses data processing by electronic means specifically.[69] So does the StPO.[70] Investigations through electronic and non-electronic means by an employer are subject to sec. 26 para. 1 s. 2 new BDSG.[71]

[66]Directive 2016/680.

[67]A Federal Police does exist but has only very limited competences mainly concentrated on border control, train stations and airports. The police law of the regional states (Bundesländer) set the legal standards.

[68]Gesetz über die Aufgaben und Befugnisse der Bayrischen Staatlichen Polizei (Polizeiaufgabengesetz).

[69]The PAG contains *e.g.* rules for the implementation of technical means in apartments and the secret access to information technology systems, Art. 34a and 34d PAG.

[70]Sec. 100a, 100b, 100g, 100h, 100j StPO.

[71]See Sects. 2.1.5 and 2.1.6.

hoeren@uni-muenster.de

2.4.2 Particular Rules

Preservation and Access to Computer Data Hosted on a Computer System

The preservation and access to computer data hosted on a computer system is limited by the fundamental right to the guarantee of the confidentiality and integrity of information technology systems. It is a special expression of the general right to privacy, Art. 2 para. 1, Art. 1 para. 1 GG. It was derived from that fundamental right by the BVerfG in 2008.[72] It is subsidiary to the right to privacy of telecommunications, Art. 10 GG, the right to informational self-determination, Art. 2 para. 1, Art. 1 para. 1 GG, and the inviolability of the home, Art. 13 GG.

The preservation, handling and/or access to computer data hosted on a computer system for the purpose of the investigation and detection of crimes is issued by Art. 34d PAG for Bavaria and by similar provisions in police Acts of the other federal states.

The preservation, handling and/or access to computer data hosted on a computer system for prosecution purposes are not specifically addressed in the StPO. They fall within the scope of the general rules of seizure, sec. 94 StPO. In this case, the computer is the subject of seizure.[73]

The BVerfG determines the requirements of encroachments on the fundamental right to the guarantee of the confidentiality and integrity of information technology systems. Encroachments, especially online searches of computers, are constitutionally permitted if factual indications exist of a concrete danger to a predominantly important legal interest. Such predominantly important legal interests are the body, life and freedom of a person or the safety of the Federal Republic of Germany. Measures infringing that right must in principle be issued by a judge, except in cases of urgency.

Interception of Communication Data

The interception of communication data infringes the fundamental right to confidentiality of communications, Art. 10 GG. It needs to be legitimized by Act of Parliament. The interception of communication data for investigation purposes is issued in Art. 34a PAG (Bavaria); for prosecution purposes in sec. 100a *et seq*. StPO. Under the relevant conditions inventory data, traffic data, as well as content data may be intercepted.

The requirements for the disclosure of communication data correspond to the severance of the encroachment of the fundamental right to confidentiality of communications. Accordingly, the requirements concerning the disclosure of inventory data are less strict then the ones concerning the disclosure of traffic data while the

[72]BVerfG, judgment of 27 February2008, 1 BvR 370/07, 1 BvR 595/07 = NJW 2008, 822.

[73]Baer in Wabnitz and Janovsky (2014), chapter 27, B. para. 48.

hoeren@uni-muenster.de

disclosure of content data, the most serious encroachment, is subject to the strictest requirements. Before briefly addressing the specific requirements, some general principles shall be pointed out.

Actions interfering the right to confidentiality of communications may only be taken to the extend that it is necessary, concerning duration as well as scope, for the specific purpose and if other means would be much more difficult or offer no prospect of success. Measures infringing the inviolable core area of the private conduct of life are inadmissible. Information concerning that core area shall not be used and be deleted without delay. In case of undercover investigation, the participants in the communication under surveillance shall be notified as soon as the notification can be effected without endangering the purpose of the investigations. Third persons may only be subject to the undertaken actions if this is unavoidable.

Art. 34a para. 1 PAG (as similar provisions in other federal states) allows the interception and recording of telecommunications if it is necessary to avert an imminent danger for body, life and freedom of men, to the extent that there is a common danger, or a danger for the safety of the Federation or of a state. The measure has to be ordered by a court, in exigent circumstances by the head of the police department. In this case, the judge has to confirm the decision immediate, Art. 34c para 1, 34 para. 4 PAG.

For prosecution purposes, content data may only be intercepted if certain facts give rise to the suspicion of serious crime and if the offence is one of particular gravity in the individual case, sec. 100a para. 1 StPO. Measures pursuant to sec. 100a StPO may be ordered by the court only upon application by the public prosecution office and shall be limited to a maximum duration of 3 months. In exigent circumstances, the public prosecution office may also issue an order, sec. 100b para. 1 StPO.

Traffic data may legitimately be obtained to the extent that this is necessary to establish the facts or determine the accused's whereabouts if certain facts give rise to the suspicion that a person has committed a criminal offence of substantial significance in the individual case as well, or certain facts give rise to the suspicion that a person has committed a criminal offence by means of telecommunication, sec. 100g para. 1 StPO.

Inventory data may be requested from any person providing or collaborating in the provision of telecommunications services if it is necessary to establish the facts, or to determine the whereabouts of an accused person, sec. 100j para. 1 StPO.

Data Retention

Data retention for the purpose of the investigation, detection and prosecution of crimes has been subject to different legislation and case law in the recent years. In the following, a short overview of events is given.

hoeren@uni-muenster.de

In 2006, the Data Retention Directive[74] has been adopted on EU level to ensure prosecution of serious crimes. Its provisions have been implemented in Germany by the Telecoms Data Retention Act in 2008. However, this Act was declared unconstitutional by the BVerfG in 2010.[75] Due to a lack of political consent, a new Telecoms Data Retention Act has not been adopted before 2015. In the meantime, the ECJ declared the Data Retention Directive to be invalid in 2014 because it entails a serious interference with the fundamental rights to privacy and data protection without limiting that interference to what is strictly necessary.[76] The BGH then declared that data storage for internal use up to 7 days is valid.[77] Now, the ECJ has again decided in matters of data retention, namely, that groundless data retention is invalid and that member states may not impose a general obligation to retain data on providers of electronic communications services.[78] The verdict can be seen as an end of the data retention in the traditional sense.[79]

2.5 Data Protection and Electronic Surveillance for Security and Defence Purposes

2.5.1 Electronic Processing of Personal Data for Security and National Defence Purposes

The electronic processing of personal data for security and national defence purposes is subject to both, federal level and state level specific legislation.

Security and national defence fall within the remit of different entities, the Federal Intelligence Service, the Federal Office for the Protection of the Constitution and the Military Counterespionage Service. The powers and tasks of these entities are laid down in corresponding legislation, *e.g.* the Act on the Federal Office for the Protection of the Constitution ("BVerfSchG").[80] The BVerfSchG can be seen as starting point, as the other respective Acts partially refer to it in data protection matters. It will therefore exemplary be examined in regard to the following questions. Restrictions on the right to privacy of correspondence, posts and telecommunications are stipulated in the Art. 10 Act.

[74]Directive 2006/24/EC.

[75]BVerfG, judgment of 2 March 2010, 1 BvR256/08 = JuS 2008, 737.

[76]ECJ, judgment of 8 April 2014—Digital Rights Ireland—C-293/12, C-594/12 = MMR 2014, 412.

[77]BGH, judgment of 3 July 2014, III ZR 391/13 = NJW 2014, 2500.

[78]ECJ, judgment of 21 December 2016, C-203/15, C-698/15 = EuZW 2017, 153.

[79]Priebe (2017), p. 136.

[80]The Federal Intelligence Service is subject to the rules of the Act on the Federal Intelligence Service (BNDG); the Military Counterespionage Service to the Act on Military Counterespionage Service (MADG).

hoeren@uni-muenster.de

The processing of personal data for security and national defence purposes on state level is issued by the State Offices for the Protection of the Constitution within their respective laws.

2.5.2 Particular Rules

Scope, Purposes Covered and Activities Permitted

The Art. 10 Act covers measures for the purpose of defence against imminent threat to the free democratic basic order or the existence or the security of the Federation. It furthermore covers measures for purposes within the tasks of the Federal Intelligence Service, *e.g.* the gathering of relevant information about other countries of importance to the foreign or security policy of the Federal Republic of Germany. The Art. 10 Act permits the interception and recording of communications for these purposes, sec. 1 para. 1 Art. 10 Act. Measures infringing the inviolable core area of the private conduct of life are inadmissible, shall not be used and shall be deleted without delay, sec. 3a Art. 10 Act.

The Federal and State Offices for the Protection of the Constitution shall gather and analyze information concerning aspiration against the free democratic basic order or the existence or the security of the Federation or the States, sec. 3 BVerfSchG. For these purposes, sec. 8 para. 2 BVerfSchG allows the usage of methods, items and instruments in order to gather information secretly like undercover investigation, observation, video recording and camouflage papers or signs. Sec. 4 para. 1 MADG and sec. 5 BNDG refer to these provisions concerning the purposes covered and the activities permitted.

Particular Requirements

The Art. 10 Act requires factual indications for the suspicion of a enumerated crime, *e.g.* betrayal peace, sedition, endangering the democratic rule of law, treason or endangering external security, sec. 3 para. 1 BVerfSchG. Furthermore, other measures may have no prospect of success, sec. 3 para. 2 BVerfSchG. The interception of international telecommunications is subject to stricter requirements: threat of *e.g.* an armed aggression or a terrorist attack and approval of the measure by the competent federal ministry and the parliamentary control committee, sec. 5 BVerfSchG.

Measures according to sec. 8 para. 2 may be taken when there are justified indications that knowledge might be gained about activities that fall within the scope of the tasks of the Offices for the Protection of the Constitution, sec. 9 BVerfSchG.

hoeren@uni-muenster.de

2.6 Remedies and Sanctions

2.6.1 Remedies for the Breach of Data Protection Rules

General Rules on Personal Data Protection

Under general data protection rules, the GDPR, each data subject shall have the right to lodge a complaint with a supervisory authority, Art. 77 GDPR, and the right to an effective judicial remedy against both a supervisory authority, Art. 78 GDPR, and a controller or processor, Art. 79 GDPR. Furthermore, each person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered, if the controller cannot prove that it is not in any way responsible for the event giving rise to the damage, Art. 82 GDPR. The civil liability under the GDPR is extended compared to the old BDSG due to the legal anchoring of the right to claim damages in the GDPR. Moreover, the introduction of collective actions, Art. 80 GDPR, facilitates the assertion of these rights.

Administrative fines have increased tremendous in the GDPR. Supervisory bodies can impose fines up to 20 million Euros, or in the case of an undertaking, up to 4% of the worldwide annual turnover of the preceding financial year, whichever is higher, Art. 83 GDPR. Member States shall lay down other penalties applicable to infringements of the Regulation, Art. 84 GDPR. The new BDSG provides for administrative fines up to 50,000 Euro, sec. 43 new BDSG.

The breach of general data protection rules can also lead to criminal prosecution. The new BDSG contains a special penal provision in sec. 42, which foresees financial penalty or imprisonment up to 3 years. The breach of general data protection rules may also violate the German Criminal Code ("StGB"), which contains several sections concerning the violation of privacy in sec. 201 StGB *et seq*. The most severe penalty under those provisions is imprisonment not exceeding 5 years in case of violation of the postal and telecommunications secret, sec. 206 StGB, or violation of the privacy of the spoken word as a public official, sec. 201 para. 3 StGB.

Online Services

The protection of personal data in the context of services provided at a distance, by electronic means, at the individual request of a recipient of services, is subject to general data protection rules, the GDPR.[81] Thus the same remedies apply.

[81] See Sect. 2.1.1.

hoeren@uni-muenster.de

Electronic Communications for Marketing Purposes

The protection of personal data in the context of electronic communications for marketing purposes is subject to the ePR. Every end-user of electronic communications services shall have the same remedies provided for in Art. 77, 78 and 79 GDPR, Art. 21 para. 1 ePR, as well as the right to compensation in case of suffering material or non-material damage as a result of an infringement of the ePR, Art. 22 ePR. Administrative fines shall be up to 10 million Euros, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, Art. 23 para. 2 lit. d) ePR. Moreover, illegal communications for marketing purposes may be answered by cease and desist letters by competitors, consumer organizations and business organizations under § 12 UWG. In practice, this particular German way of private enforcement is of a significant effectiveness and includes lawyers' costs of the sender of the letter.

Personal Data of Employees

The breach of rules regarding the electronic processing of personal data of employees is neither specifically addressed in the GDPR nor in the new BDSG and thus subject to general rules.

Security of Personal Data Processed by Electronic Means

The degree of responsibility of the controller or processor taking into account technical measures to ensure the security of processing shall be regarded when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in the individual case, Art. 83 para. 2 lit. d) GDPR. Beyond that, a breach of rules regarding the security is not specifically addressed in the GDPR and thus subject to general remedies granted by the GDPR. In case of a breach of rules of the BSIG, administrative fines up to 100,000 Euros can be imposed.

Electronic Communications Sector

The end-users of electronic communications services shall have the same remedies provided for in the GDPR, Art. 21, 22 ePR.[82] Administrative fines can also be issued up to 20 million Euros or 4% of the annual turnover, Art. 23 ePR. Member States shall lay down other penalties, Art. 24 ePR.

[82] See Sects. 2.5.1 and 2.5.2.

hoeren@uni-muenster.de

Investigation, Detection and Prosecution of Crimes

Against police measures an action for a specific declaratory judgment on whether the measure was lawful can be brought mutatis mutandis sec. 113 para. 1 s. 4 Administrative Procedure Code ("VwGO").

The person concerned by a seizure of the computer may at any time apply for a court decision, sec. 98 para. 2 s. 2 StPO; on orders according to sec. 100j StPO applies sec. 98 para. 2 s. 2 to stop *mutatis mutandis*. Against measures due to sec. 100a and 100g StPO an immediate appeal can be lodged mutatis mutandis sec. 101 para. 7 s. 2 StPO.

Security and National Defence Purposes

There are no specific rules concerning legal actions in the specific laws. Thus general administrative procedure rules apply. In most of the cases a concerned person will bring an action for a declaratory judgment mutatis mutandis sec. 113 para. 1 s. 4 VwGO.

2.6.2 Maximum Financial Penalty or Sanction

The maximum financial sanction that has been issued on basis of the old BDSG against individual companies has been less than 2 million Euros.[83] As the GDPR does only apply from 25 May 2018, there are no financial penalties yet, issued under the new data protection regime. However, administrative fines are going to increase tremendously under the GDPR. As to Art. 83 GDPR, administrative fines shall in each individual case be effective, proportionate and dissuasive. *Jan Philipp Albrecht*, the rapporteur of the European Parliament expects administrative fines running into the billions.[84] It shall be possible to appeal to courts against legal binding decisions of supervisory authorities, Art. 78 GDPR.

2.7 Private International Law Rules

2.7.1 Territorial Scope of Application of Data Protection Rules

The territorial scope of application of data protection rules, including rules on electronic data processing, is very broad. It does not only comprise the processing of personal data in the context of activities of an establishment of a controller or a

[83] Faust et al. (2016), p. 120.

[84] Albrecht (2015).

hoeren@uni-muenster.de

processor in the Union, regardless of whether the processing takes place in the Union or not, (Art. 3 para. 1 GDPR)[85] but also to processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to either the offering of goods or services to such data subjects in the Union, or the monitoring of their behaviour as far as this behaviour takes place within the Union (Art. 3 para. 2 GDPR). The latter so-called "market place principle" did not form part of the former data protection Framework of the European Union and so significantly extends the territorial scope of application compared to the Directive 95/46.Moreover, the notion of establishment of the controller under Art. 3 para. 1 GDPR has to be understood in a rather broad sense.[86] Following the Google Case of the ECJit would be sufficient for an establishment in a Member State to have an office or subsidiary (as a separate legal person) for the purpose of promoting and selling advertising space, which orientates its activity towards the inhabitants of that Member State.[87]

Art. 3 para. 1 ePR mainly extends the principle enshrined in Art. 3 para. 2 GDPR to the provision of electronic communications services to "end-users in the Union" (Art. 3 para. 1 lit. a)ePR). Art. 3 para. 1 lit. b) and c) ePR clarify that this includes the pure use of such services and the protection of information related to the terminal equipment of end-users located in the Union. Moreover Art. 3 paras. 2–5 ePR oblige the provider to designate a representative in the Union.

Whereas the exact meaning of the rules on the territorial scope under the 1995 Directive had been open to discussion, Art. 3 GDPR brought some clarifications: The article not only has to be understood as a rule for the international application of administrative law but in the sense of private international law, also. In the latter sense the Article also serves as basis for a general *lex protectionis datorum* within the Internal Market,[88] which concurs with other legal instruments on private international law. As did Art. 4 of the Directive 95/46[89] Art. 3 GDPR beyond regulating the pure scope of application of the regulation also establishes general principles for the application of data protection rules within the Internal Market. Therefore, Art. 3 GDPR also provides for rules of private international law organizing the application of the remaining national data protection rules of the Member States.

In its scope of application, Art. 3 GDPR (and the *lex protectionis datorum*) overrules the general regimes of the Rome I and Rome II Regulations as far as applicable, cf. Art. 1 para. 2 lit. g) Rome II Regulation,[90] and the respective national rules on private international law. However, this particular regime does not exclude the application of Art. 9 Rome I Regulation but—as with articles 6 and 8 Rome I

[85]This includes controllers not established in the Union, but in a place where Member State law applies by virtue of public international law, Art. 3 para. 3 GDPR.

[86]Oberverwaltungsgericht Schleswig, NJW 2013, p. 1977, para. 13.

[87]ECJ, judgmentof13 May 2014, C-131/12 = EuZW 2014, 541.

[88]Cf. Schmidt-Kessel in Ferrari (2014), Art. 9 Rome I-Regulation, no. 51–57.

[89]Schmidt-Kessel in Ferrari (2014), Art. 9 Rome I-Regulation, no. 54.

[90]Cf. Voigt (2014), pp. 15 *et seq*.; cf. Bach in Huber (2009), Art. 1 no. 53–59.

hoeren@uni-muenster.de

Regulation—it would be difficult in many cases to establish the quality of a rule being crucial to safeguard the public interest of the forum.

The scope of application of the particular regime established by Art. 3 GDPR in private law cases, *i.e.* with a private person as controller, is determined by the Regulation, which determines the content of the *lex protectionis datorum*. In particular, it covers the general ban on data processing and its exceptions, and the particular subjective rights under the Regulation. In particular, Art. 3 GDPR determines the law applicable to the consent of the data subject. The parties may not deviate from the *lex protectionis datorum* by a choice of law under article 3 Rome I Regulation. On the other hand, the relationship to the contract in which such consent is integrated is determined by the *lex contractus*. This includes the rules on unfair contract terms. Therefore, consent of the data subject declared in standard terms must comply with both sets of rules, the *lex contractus* (and Art. 6 Rome I Regulation in particular) and the *lex protectionis datorum* under Art. 3 GDPR.

2.7.2 Application to Entities Seated Outside the European Union

The electronic data processing by entities seated outside the Union is comprised in the scope of application of local rules. This exactly is the very purpose of Art. 3 para. 2 GDPR and Art. 3 para. 1 ePR.[91]

2.7.3 Transfer of Personal Data to a Foreign Jurisdiction

The transfer of personal data to a foreign jurisdiction is subject to specific conditions. Under the GDPR, any transfer to a third country or international organization may only take place where the Commission has decided that the third country or the organization in question ensures an adequate level of protection, Art. 44, 45 GDPR. When assessing the adequacy of the level of protection, the Commission shall take account of elements like the respect for human rights and fundamental freedoms, data protection rules and security measures, effective and enforceable data subject rights and effective administrative and judicial redress. The effective functioning of independent supervisory authorities is also essential.[92]

Formerly, the Safe Harbor Framework, negotiated in 2009, concerned data transfers from Europe to the United States and provided the basis for the aforementioned decision by the European Commission under the Directive 95/46. However, the Safe Harbor Framework has been declared invalid by the ECJ in 2015.[93] It has been replaced by the EU-U.S. Privacy Shield, which will certainly be under review by the ECJ sooner or later.

[91] See Sect. 2.7.1.

[92] See for a full listing of elements: Art. 45 para. 2 GDPR.

[93] ECJ, judgment of 6 October 2015, C-362/14 = ZD 2015, 549.

hoeren@uni-muenster.de

2.7.4 Applicable Law Liability for Damages for Unlawful Processing

As analyzed before (B VI 1) the *lex protectionis datorum* organized by Art. 3 GDPR replaces—as a kind of *lex specialis*—the more general rules under the European private international law instruments and remaining private international law of the Member States. That covers a *lex contractus* as well as a *lex (loci) delicti*.

However, one has to admit that the beyond material scope of the GDPR and the ePR the general rules of private international still apply. For example, the liability under Art. 82 GDPR (and Art. 22 ePR) should be analyzed as a tortious liability only (also if applied in a contractual context), and does not cover cases of a breach of terms of a contract (as far as valid under the applicable data protection law). Moreover, breaches of other personality rights may still be judged under tort law applicable in parallel to applicable data protection law. Here, the Rome II Regulation applies.

References

Albrecht JP (2015) Starke Verbraucherrechte und mehr Wettbewerb. https://www.janalbrecht.eu/2015/12/2015-12-21-starke-verbraucherrechte-und-mehr-wettbewerb/. Accessed 2 Aug 2018
Auer-Reinsdorff A, Conrad I (eds) (2016) Handbuch IT- und Datenschutzrecht. C.H. Beck, Munich
Bauer J-H, Günther J (2013) Kündigung wegen beleidigender Äußerungen auf Facebook. NZA, 67–73
Faust S, Spittka J, Wybitul T (2016) Milliardenbußgelder nach der DS-GVO? ZD, 120–125
Ferrari F (ed) (2014) Rome I Regulation – pocket commentary. Sellier European Law Publishers, Munich
Goratsch P (2018) Comment on BGH judgement of 12 July 2018. NZFam., 800–811
Huber P (ed) (2009) Rome II Regulation – pocket commentary. Otto Schmid, Munich
Keppeler LM (2015) Was bleibt vom TMG- Datenschutz nach der DS-GVO? Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz. MMR, 779–783
Koenig C, Bartosch A, Braun J-D (eds) (2009) EC Competition and Telecommunications Law. Kluwer, London
Kort M (2012) Kündigungsrechtliche Fragen bei Äußerungen des Arbeitnehmers im Internet. NZA, 1321–1326
Kranig T, Peintinger S (2014) Selbstregulierung im Datenschutzrecht. ZD, 3–9
Kühling J (2017) Comment on BVerfG judgement of 15 December 1983. NJW, 3069–3069
Litzenburger W (2018) Comment on BGH judgement of 12 July 2018. FD-ErbR, 40766
Nebel M, Richter P (2012) Datenschutz bei Internetdiensten nach der DS-GVO – Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf. ZD, 407–413
Pohle J (2017) EU-Datenschutz: Entwurf einer ePrivacy-VO. ZD-Aktuell, 05452-05452
Priebe R (2017) Vorratsdatenspeicherung und kein Ende. EuZW, 136–139
Schmitz P (2017) E-Privacy-VO – unzureichende Regeln für klassische Dienste. ZRP, 172–175
Spindler G (2016) Selbstregulierung und Zertifizierungsverfahren nach der DS-GVO. ZD, 407–414
Voigt P (2014) Internationale Anwendbarkeit des deutschen Datenschutzrechts. ZD, 15–21
Wabnitz H-B, Janovsky T (eds) (2014) Handbuch des Wirtschafts- und Steuerstrafrechts. C.H. Beck, Munich

hoeren@uni-muenster.de

Data Protection in the Internet: Greece

Vassilios Kourtis

1 The General Data Protection Framework

1.1 The Applicable Rules

The Greek Constitution guarantees the right to information (Art. 5A) and the right to protection of personal data (Art. 9A).[1] Specifically, article 5A §1 of the Constitution safeguards the right of each person to be informed, as this right is specified by law. Restrictions to this right may be imposed by law only insofar as they are necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties. Article 5A §2 of the Constitution safeguards a specific facet of the right to information: the right of each person to participate in the information society. The Greek State must facilitate access to information transmitted electronically, as well as to facilitate production, exchange and diffusion of information, in observance of the guarantees of article 9 of the Constitution, which safeguards the right to private and family life, article 19 of the Constitution, which protects the right to confidentiality of communications, and article 9A of the Constitution on personal data protection.

Article 9A is the constitutional basis for personal data protection, as it guarantees the right to informational self-determination. It reads: "All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law". Article 9A provides protection against any type of processing, automated or not, carried out by public or private bodies. The

[1] See Spyropoulos and Fortsakis (2009), *sparsim*; Chryssogonos (2002), pp. 199 ff.; Donos (2000), pp. 109 ff.; Iliadou (2016), pp. 23 ff.; Vidalis (2006), pp. 19 ff.; Sotiropoulos (2006), pp. 69 ff.

V. Kourtis (✉)
Faculty of Law, Aristotle University of Thessaloniki, Thessaloniki, Greece
e-mail: vk@law.auth.gr

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_8

hoeren@uni-muenster.de

right to data protection is not an absolute right, but it is susceptible to restrictions, when its exercise results to violation of other persons' rights and when there are compelling reasons of public interest, taking into account the principle of proportionality.[2]

The protection of personal data is also indirectly grounded on article 2 §1 of the Constitution, which guarantees the fundamental principle of "respect and protection of the value of human being" and article 5 §1 of the Constitution, which guarantees the right of each person to free development of his/her personality on condition that the exercise of the right does not infringe the rights of the others, or violate the Constitution and the good usages. In virtue of article 25 §1c of the Constitution, all the above-mentioned constitutional provisions have also horizontal effect ("Drittwirkung").

Furthermore, the legal framework regarding the protection of personal data in Greece includes the Charter of Fundamental Rights of the EU, which safeguards the right to personal data protection (art. 8) as well as the respect for private and family life (art. 7) and the primary EU legislation guaranteeing the protection of individuals against the processing of personal data (articles 39 TEU and 16 TFEU). This legal framework is expanded by the European Convention for the protection of human rights and fundamental freedoms, which safeguards the protection of private and family life (art. 8) and the relevant case law of the European Court of Human Rights. Greece is also a member of the European Convention 108 for the protection of individuals regarding automatic processing of personal data.[3]

The protection of privacy and personal data traditionally constituted in Greece a facet of the right to personality, which is protected by the Civil Code. Specifically, article 57 provides for the right of a person to demand that any infringement against his/her personality must cease, without excluding the right to appropriate compensation and article 59 provides for the moral redress of the victim. The Greek legal framework enriched by the relevant secondary EU legislation.

The Greek legal framework regarding personal data protection acquired new contents by the recent entry into force of the General Data Protection Regulation (GDPR).[4] A draft bill on the protection of personal data implementing GDPR and transferring the Police Directive (2016/680) was appeared in February 2018 and submitted to public consultation. On 26 August 2019 the Greek Parliament passed the new Law (no. 4624/2019). GDPR as well as the recently enacted Law bring broad amendments to the legislation regarding the protection of personal data in Greece. According to the new Law, the existing Greek legislation as well as the directives and acts issued by the Hellenic Data Protection Authority (DPA) will

[2]See Areios Pagos (plenary session) no. 1/2017.

[3]See Law 2068/1992 Government Gazette A 118, valid from 01.12.2005; see also Tsevas (2010), pp. 92 ff.

[4]For the new Regulation in Greek legal literature see Christou (2017), pp. 223 ff.; Iglezakis (2018); Kotsalis and Menoudakos (2018); Mitrou (2017); Panagopoulou-Koutnatzi (2017).

hoeren@uni-muenster.de

continue to be in force insofar as they will not conflict to the GDPR and the new Law.

Law 2472/1997 on the p*rotection of individuals with regard to the processing of personal data*,[5] which transposed Directive 95/46 into the Greek law, constituted for a long period the general legal framework on the protection of personal data in the country.[6] In so far as GDPR replaced Law 2472/1997, the latter is no longer enforced; it has been typically abolished by the new Law 4624/2019 except for some provisions such as those containing the basic definitions. Any reference to the Law 2472/1997 shall be understood as reference to the GDPR and the new Law.

Furthermore, the Greek legal framework regarding personal data protection consists of the following Laws, which, as far as they do not conflict to the GDPR and the Law under preparation, will continue to be in force: (a) Law 3471/2006 on the p*rotection of personal data and privacy in the electronic communications sector and amendment of Law 2472/1997*, as in effect,[7] by which, *inter alia*, the e-Privacy Directive (2002/58) was transposed into national legislation.[8] Law 3471/2006 was later amended by Law 4070/2012 on *electronic communications, transports, public works and other provisions*,[9] which transposed the Directive 2009/136. Law 3471/2006 aims at the protection of fundamental human rights, especially privacy, and the establishment of the conditions for the processing of personal data and the reservation of communication confidentiality in the electronic communications sector. Law 3471/2006 constituted a *lex specialis* in relation to the general Law 2472/1992.[10] Both Laws formed a system consisting of substantial requirements, sanctions and monitoring regarding the personal data processing as well as of specific rules regarding confidentiality[11]; (b) Law 3783/2009 on the *identification of owners and users of equipment and services for mobile telephony and other provisions* for national security reasons and for the detection of particularly criminal offences[12]; (c) Law 3917/2011 on the *retention of data generated or processed in connection with the provision of publicly available electronic communications services or of*

[5]Government Gazette A 50.

[6]For an overview of Law 2472/1997, see Iglezakis (2011), pp. 240 ff.; Alexandropoulou-Aigyptiadou (2016), pp. 38 ff.; Armamentos and Sotiropoulos (2005, 2008); Christodoulou (2013); Yerontas (2002), pp. 178 ff.

[7]Government Gazette A 133. For an overview of Law 3471/2006, see Iglezakis (2011), pp. 261 ff.; Alexandropoulou-Aigyptiadou (2016), pp. 171 ff.; Arkouli (2010), pp. 43 ff.; Tountopoulos (2000), pp. 475 ff.

[8]Law 3471/2006 replaced Law 2774/1999, which previously had transposed Directive 97/66/EC. The provisions of the second part of Law 3471/2006 (articles 18–31) amended Law 2472/1996.

[9]Government Gazette A 82.

[10]Article 3 § 2 L. 3471/2006. However, according to a different—not predominant—interpretation of Art. 3 § 2, based on the argument of consistency to article 9A of the Constitution, the provisions of Law 3471/2006 were only applicable when they were more favorable to the data subject, see Christodoulou (2013), pp. 152 ff.

[11]See Iglezakis (2009), p. 197.

[12]Government Gazette A 136.

hoeren@uni-muenster.de

public communications networks, use of surveillance systems with the obtaining or recording of sound or image at public areas and relative provisions,[13] transposing Directive 2006/24.

1.2 The Notion of Personal Data

In Greek legislation, personal data means any information relating to the data subject, that is, to any identified or identifiable individual to whom such personal data refer. An identifiable natural person is one who can be identified, directly or indirectly, especially by reference to a name, an identity card number, location data or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, political or social identity.[14] The data kept for statistical purposes, which can no longer be attributed to a data subject, are not considered as personal data in the meaning of the law on personal data protection. Personal data are relating to living persons.[15] Although only individuals are afforded protection of their personal data, Greek academics expressed the opinion that the constitutional data protection is not limited to individuals.[16] Moreover, certain matters relating to legal persons might be subject to data protection legislation, *e.g.* when the name of the principal partner of a commercial company is referred to the company name.[17]

Areios Pagos, the Greek Supreme Civil and Criminal Court, held that an information falls within the definition of personal data, when it is directly linked to the data subject and to his/her personal qualities or activities that are not to become known to the public, unless the data subject consented.[18] Moreover, the Greek courts held that the picture of a person posted on the Facebook constitutes processing of personal data[19] and that the picture of an individual without a name associated to it constitutes indirect identification of that person.[20] In another case, the judge accepted that a photo accompanied by an article containing relevant content identified an individual to constitute personal data, even if the facial image was unrecognizable.[21] Moreover, according to the Data Protection Authority, factors of indirect identification, such as an email address, can sufficiently identify an individual from other members of a group, even without a name associated to it.[22] The Authority

[13]Government Gazette A 22.

[14]See art. 4 GDPR and art. 2 L. 2472/1997.

[15]See DPA decision no. 38/2010.

[16]See Sotiropoulos (2006), pp. 84 and 89.

[17]See Mittleton (2016), p. 10.

[18]Areios Pagos no. 637/2013.

[19]First Instance Court of Thiva no. 54/2014.

[20]Court of Peace of Athens no. 4048/3014.

[21]Court of Appeal of Athens no. 3808/2014.

[22]See DPA decision no. 25/2013.

hoeren@uni-muenster.de

repeatedly held that the subjective judgments and evaluations only exceptionally may be accepted as personal data.[23] Such are the cases of a criminal charge or conviction as well as the employee evaluation or the grades of a student.[24] Moreover, an evaluation made for ascertainment of a person's credibility[25] as well as any use of the credit profile databank TEIRESIAS constitutes processing of personal data.[26]

Law 2472/1997 specified the category of "sensitive data",[27] which included the data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sexual life and health, *i.e.* "medical data" including, at least, certain types of "genetic data" related to health.[28] In addition, as sensitive were also characterized the data referring to social welfare, criminal charges or convictions as well as membership to associations of persons dealing with the categories mentioned above.[29] The GDPR and the Law which has recently been enacted to implement it keep the basic distinction between "simple" and special categories of personal data. They refer to special categories of data including definitions of certain categories of data such as the genetic and biometric data and the data related to health.

1.3 The Supervisory Authorities

The establishment and operation of an independent Authority with a task to ensure the protection of personal data are provided for by article 9A of the Constitution. To implement that constitutional provision, Law 2472/1997 established the Hellenic Personal Data Authority (DPA), which has been operational since 1997.[30] This Authority is the supervisory authority for monitoring and enforcing the application of the GDPR in Greece. Its legal status as well as its powers and tasks are provided for by the new Law 4624/2019. Moreover, the new Law regulates special matters concerning the establishment and function of the Authority such as the conditions required for the appointment of its members, the tasks and powers of its members as well as the necessary financial resources.

[23]See, *e.g.*, DPA decision no. Γ/ΕΞ/691/3.2.2014. On this matter, see Christodoulou (2013), pp. 15 ff.; Mittleton (2016), pp. 19–20.

[24]See DPA directive no. 115/2001; see also Court of Appeal of Athens no. 5433/2011 and Administrative First Instance Court of Thessaloniki no. 4796/2013.

[25]See DPA decision no. 59/2000.

[26]See DPA decisions nos. 86/2002, 24/2004, 25/2004 and 186/2014. See also Iglezakis (2006).

[27]Art. 2b L. 2472/1997; on sensitive data see Iglezakis (2003).

[28]In its Opinion no. 15/2001, DPA adopted the definition of genetic data given by the Council of Europe Recommendation R (97) 5 on the protection of medical data. Greek academics argued that certain types of genetic data are not covered by the definition of health data containing in Law 2472/1997, see, *e.g.*, Papachristou and Papadopoulou-Klamaris (2006), pp. 41 ff.

[29]On this see also the decision of the Misdemeanor Court of Thessaloniki no. 1247/2011.

[30]See Spyropoulos and Fortsakis (2009), pp. 150–151; Mitrou (1999); Donos et al. (2002).

hoeren@uni-muenster.de

The Data Protection Authority constitutes an independent public authority, not subjecting to administrative control, reports to the Minister of Justice and its seat is in Athens.[31] Its members enjoy personal and functional independence. The Authority is entrusted with the task of supervising the implementation of any regulation pertaining the protection of individuals from the processing of personal data. In addition, it exercises the duties assigned to it, such as to issue guidelines and recommendations for any matter regarding the processing of personal data, to give opinions regarding any rules concerning the processing and protection of personal data that will be included to a Law or regulation, to give its opinion to the data controllers according to the procedure of prior consultation (art. 36 GDPR), to issue forms for the notification of personal data breach (art. 33 GDPR) and the communication of breach to the data subject (art. 34 GDPR) and to issue certifications (art. 42 GDPR). Moreover, the Authority has the task to examine the lawfulness of personal data processing and to inform the data subject concerned, to handle the complaints lodged by data subjects, to announce to the Parliament any breach of the rules regarding the protection of individuals from the processing of personal data and to draw up annual reports on the performance of its duties.

The Authority is empowered to carry out *ex officio* or following a complaint reviews regarding the implementation of the GDPR and other legislation on processing of personal data. During the investigation, the Authority may obtain access to the data protection equipment and means, as well as to data and information necessary for the performance of its tasks. Moreover, the Authority may denounce any breach of data protection law to the competent judicial authorities. It may impose administrative sanctions.

1.4 The Self-Regulation Instruments

According to Law 2472/1997, the Data Protection Authority encouraged and assisted the trade associations as well as the associations of natural and legal persons keeping personal data files to draw up codes of conduct intended to secure wider and more effective protection of the right to privacy and other rights and fundamental liberties of individuals in their field.[32] Thus, already under the previous legislative regime, Greek data protection law recognized the possibility of trade associations and other bodies to prepare codes of conduct for their members, without providing for approval procedures.[33]

[31] See the website of this Authority, at: www.dpa.gr/en.

[32] Art. 19 § 1b L. 2472/1997.

[33] See Papakonstantinou (2010), § 15.2.2.

hoeren@uni-muenster.de

2 Specific Problems Concerning Data Protection in the Internet

2.1 Personal Data Processed by Electronic Means

The guiding and interpretive principles laid down by the general Law 2472/1997 to govern the protection of personal data and privacy were also applicable to the electronic data processing with the necessary adjustments. The basic requirements for carrying out lawful personal data processing provided for by the previous law are also laid down by the GDPR.[34] Moreover, Law 3471/2006 governing personal data processing in the framework of publicly available electronic telecommunications services including internet stipulates that the data processing must be limited to the extent as is strictly necessary for the purposes it is carried out.[35] The electronic data processing is only allowed, if the subscriber or user has given his/her consent upon notification as to the type of data, the purpose and extent of the processing and the recipients.[36] The consent must be given in an explicit manner and it must concern the processing that is carried out for a specific purpose, whereas the consent that is given in an abstract and general manner for any future processing relating to him/her is not valid.[37] The rule regarding the consent is subject to limitations so that a fair balance to be achieved between the protection of personal data and the satisfaction of other constitutionally guaranteed rights.[38] Thus, processing may be carried out without the subject's consent in certain circumstances, such as when processing is necessary for the performance of a contract concluded online or for the controller to comply with a legal obligation to which s/he is subject.[39] Moreover, when data processing is necessary for the protection of a vital interest of the data subject,[40] if the subject is physically or legally incapable of giving the consent, or for the purposes of a legitimate interest pursued by the data controller or by the third party to whom the data are disclosed and on condition that such an interest manifestly prevails over the rights and interests of the persons to whom the data refer and their fundamental rights are not affected.

[34] See art. 5 GDPR.

[35] Art. 5 § 1 L. 3471/2006.

[36] Art. 5 § 2 L. 3471/2006.

[37] See Alexandropoulou-Aigyptiadou (2016), p. 60; Christodoulou (2013), p. 361; Iglezakis (2009), pp. 218 ff. See also Consumer Ombudsman's decision no. 1204/2007.

[38] See Areios Pagos no. 1/2017 and Council of State nos. 1616/2012 & 2254/2005.

[39] Art. 5 § 2 L. 2472/1997.

[40] See also recital 46 of the GDPR.

hoeren@uni-muenster.de

2.1.1 Processing of Personal Data in the Context of Services Provided at a Distance by Electronic Means

The protection of personal data in the context of services provided at a distance, by electronic means, at the individual request of a recipient of services is governed, in addition to the rules on personal data processing provided for by the Laws 2472/1997 and 3471/2006,[41] by the Presidential Decree 131/2003 on electronic commerce, which has been transposed the Directive 2000/31/EC into Greek law.[42] The Presidential Decree aiming at the protection of personal data of the recipient of an information society service, obliges the service provider—except when otherwise agreed by parties who are not consumers—to inform in a clear, comprehensible and unambiguous manner the recipient of the service, before s/he places the order, whether the contract concluded will be filed and whether it will be accessible.[43] Worth to mention is also the recently adopted code of conduct for consumer protection in electronic commerce,[44] constituting a specific form of the code of conduct for consumer protection,[45] which contains guidelines for the data protection of e-consumers.

The automatic calling machines, faxes, or emails can be used for the purposes of direct marketing of goods or services or any advertising purposes, only upon the prior consent of the recipient ("opt-in system").[46] However, the email contact details lawfully obtained in the course of the sale of goods or the provision of services can be used for direct marketing of similar products or services by the supplier, even without the consent of the recipient, provided that the recipient is clearly given the opportunity to object to such collection and use of his/her electronic contact details ("opt-out system").[47] Any unsolicited commercial communication by e-mail shall be identifiable clearly and unambiguously as such as soon it is received by the recipient.[48] Such an e-mail must contain the identity of the sender, as well as a valid address to which the recipient can request the termination of such communications.[49] The providers of services undertaking unsolicited commercial communication must keep and consult regularly the opt-out registers, in which individuals not wishing to receive such commercial communications can register themselves.[50] The provider

[41] See Arkouli (2010), p. 44.

[42] See Alexandridou (2018), pp. 259 ff.

[43] Art. 9 §1b P.D. 131/2003.

[44] See Decision of the Minister of Economy and Development 316/2017, Government Gazette B 969.

[45] See P.D. 10/2017, Government Gazette A 23.

[46] Art. 11 § 1 L. 3471/2006. Recipient of the messages is the subscriber or user of electronic communications, as defined in art. 2 §§1–2 L. 3471/2006.

[47] Art. 11 § 3 L. 3471/2006.

[48] Art. 6 § 1 P.D. 131/2003.

[49] Art. 5 P.D. 131/2003.

[50] Art. 6 § 2 P.D. 131/2003.

hoeren@uni-muenster.de

must enter these statements in a special directory, which must be at the subscriber's disposal, free of charge. The unsolicited communication with human intervention (phone calls) for marketing purposes is permitted without the prior consent of the subscriber, unless s/he has stated to the provider the wish not to accept such communications in general ("opt-out system").[51]

Furthermore, the subscriber or user is protected as consumer against the unsolicited communication practices made for marketing purposes on the basis of Law 2251/1994 on consumer protection, as in effect. Under the initial version of Law 2251/1994, an opt-in system without exceptions had been established protecting the consumer against direct marketing of goods or services.[52] According to its current version, the transmission of advertising messages directly to the consumer through electronic means is only allowed on condition that the terms and requirements concerning unsolicited commercial communication by electronic means provided for by Law 3471/2006—as described above—are met.[53] Furthermore, Law 2251/1994 provides for the mandatory storage of information concerning the conclusion of a contract by electronic means in a durable medium in a way accessible for future reference.

The Data Protection Authority has issued special guidelines for the electronic consent given by the persons contacted for marketing purposes by means of electronic communication.[54] Furthermore, according to the code of conduct in e-commerce mentioned above, the business must have and apply clear, true, lawful, easily accessible and updated personal data policy as well as they shall provide relevant information to the consumers according to the law and directions given by the Data Protection Authority. The business is not allowed to collect, restore and process the consumer's sensible personal data. Collecting, processing or using personal data, which have not qualified as sensible, may be carried out when it is permitted by law. The "cookies" can be stored if the consumer consented to it after being adequately informed. If the consent has not been given, the business shall allow the use of its website without sending cookies, as long as it is technically feasible. The business shall guarantee that the collected data are not disclosed or transmitted to third parties without prior getting the consent of the informed subject data or, in the circumstances where disclosing of data is provided for by law, it must be done according to the data protection legislation. The business shall respect the wish of the consumer not to be included in files having as purpose the performance of unsolicited commercial communications with human intervention (phone calls) for the purposes of marketing goods or services, provided that the data subject has stated her/his wish to the provider of communications available to the public. The businesses must provide the consumers with the option of choosing if they wish to receive marketing messages or newsletters and, if they accept it, to be able to revoke

[51] Art. 11 § 2 L. 3471/2006.

[52] See Delouka-Igglesis (2018), p. 599.

[53] Art. 9 § 5 L. 2251/1994.

[54] See DPA Directive no. 2/2011, published in the Government Gazette, B 889.

hoeren@uni-muenster.de

their consent. The consumer must have direct access to his/her personal data and to be able to object to their future use for marketing purposes, to request from the business to partially or totally erase or complete or rectify them and to be informed about the time and the way of obtaining the data as well as for the methods for the protection of the data applying by the business.

The recipient of unsolicited communication has the right to demand compensation for any material or non-material damage caused by the provider of publicly available electronic communications services, who by negligence violated the obligation to take suitable measures to prevent the unsolicited communications. The same right of compensation has the recipient against the provider who violated the obligation to enter the statements of the recipient in a special subscriber directory.[55]

2.1.2 Protection of Minors' Personal Data Processed by Electronic Means

The protection of minors' personal data in the framework of the offer of information society services has not been regulated by specific provisions in Greece. In respect to the consent required for the processing of personal data relating to a data subject, who is underage, the Data Protection Authority held that the consent shall be given by the holder of the parental responsibility.[56]

The Greek legislator uses the possibility given by article 8 § 1of GDPR to set an age limit for these purposes lower than 16 years. Thus, the new Law 4624/2019 sets the age limit for valid consent at 15 years. Where the child is below the age of 15 years, the processing of its personal data shall be lawful only if that consent is given or authorized by the holder of parental responsibility over the child.[57]

In relation to the protection of the children's personal data, worth to mention are the guidelines issued by the Data Protection Authority for the use of CCTV systems in schools and other places where minors are active.[58]

2.1.3 The Right to the Erasure of Personal Data Processed by Electronic Means

Greek academics consider that the so-called "right to be forgotten" can rely on the articles 2 and 5 §1 of the Constitution, which established the principle of human

[55]Art. 11 § 5 L. 3471/2006.

[56]See DPA Decision no. 112/2012 addressing the issue of the use of geolocation technology for the location tracking of individuals, *e.g.*, minors or patients.

[57]On this matter see also Christodoulou (2018), pp. 61 ff.

[58]See art. 18 of DPA Directive no. 1/2011 on the use of CCTV systems and the protection of individuals and property.

hoeren@uni-muenster.de

dignity and the right to the free development of personality, respectively, and on the articles 9 and 9A of the Constitution, which guarantees the right to privacy and the protection of personal data, respectively.[59] The "right to be forgotten" was not enshrined in any Greek specific provision regarding data protection in the way it is provided for by the GDPR (article 17) and was recognized in the CJUE's decision on the *Google Spain* case.[60] However, one can trace the right to the erasure of personal data processed in certain provisions of the older legal framework, which established a right of the data subject to delete his/her own personal data. *E.g.*, pursuant to Art. 4 §1d of Law 2472/1997, the personal data might be kept in a form permitting identification of the data subject for no longer than the period required for the purposes for which such data were collected or processed. Exceptionally, the maintenance of personal data might be allowed under conditions for historical, scientific or statistical purposes. In relation to the lawful duration of data processing, the Data Protection Authority held that after the termination of a mobile contract or the cancellation of a smart card, the personal data collected during the transaction must be deleted.[61] Moreover, Article 12 §2e of Law 2472/1997 provided for the right of the data subject to ask the controller to erase or lock of his/her data, when the processing is not in accordance with the law, especially due to the incomplete or inaccurate nature of data. Furthermore, Article 6 §1 of Law 3471/2006 recognized the obligation of the providers of electronic communication services to erase or make anonymous the traffic data relating to subscribers and users after the end of the transmission of a communication.[62] Finally, worth to say is that the Data Protection Authority examined during the last years certain requests concerning the deletion of links from the Google search results, taking into account the Google Spain decision and the relevant guidelines issued by the article 29 data protection working party.[63]

2.1.4 Protection of Employees' Personal Data Processed by Electronic Means

Electronic personal data processing in the field of employment relationships is a subject to the general personal data legal framework.[64] An exemption in respect to the processing of employees' personal data was introduced by Article 7A of Law 2472/1997 that has been added by an amendment in 2001. According to that provision, the controller—who is usually identified with the employer or

[59]See Iglezakis (2014), pp. 37 ff.; Panagopoulou-Koutnatzi (2016), p. 714.

[60]CJEU, 13.05.2014, C-131/12, Google Spain v. Agencia Española, ECLI:EU:C:2014:317.

[61]See DPA Decision no. 38/2002.

[62]However, this obligation was subject to Law 3917/2011, which provided for the traffic data's retention for a period of 12 months.

[63]WP 225/26.11.2014. See DPA decisions nos. 82/2016, 83/2016 and 84/2016.

[64]For the protection of employees against the unlawful processing of their personal data, see Douka (2005); Malagardi (2010); Mitrou (2016), pp. 191 ff.

hoeren@uni-muenster.de

director—is exempted from (a) his/her obligation to notify the Authority about the establishment and operation of a file or the commencement of data processing, and (b) his/her obligation to receive a permit for the processing of sensitive data, when the processing of the employees' data is carried out exclusively for purposes relating *directly* to (1) an employment relationship or to provision of services to the public sector, and (2) is *necessary* for the fulfilment of an obligation imposed by law or for the performance of obligations arising from the employment relationship, and upon the prior relevant information of the employee.

The Data Protection Authority dealing with specific issues that arose during the period where Law 2472/1997 applied to employees repeatedly stressed that the horizontal nature of the general rules regarding data protection has the effect that the specific purposes as well as the conditions of the employment relationships are often overlooked, and the protection of employees' personal data becomes ineffective.[65] Besides that, the article 7A of Law 2472/1997, mentioned above, gave birth to issues of interpretation and legal certainty, because of the absence of specific regulations and guarantees regarding its implementation. Due to that situation and the fact that the methods of monitoring the employees at the workplace became more advanced, the Authority proceeded to issuance of guidelines,[66] whereby general rules on personal data protection are interpreted to be uniformly applied and adapted to employment relationships.

According to the interpretation given by the Authority in relation to Law 2472/1997, the collection and processing of employees' personal data shall be carried out through legitimate means and in such a way that ensures respect of privacy, personality and human dignity at the workplace and the framework of employment relationship in general.[67] As it follows from the basic principle of purpose limitation, the collection and processing of employees' personal data are permitted exclusively for purposes *directly* related to the employment relationship and provided that they are *necessary* for fulfilling obligations of both parties arisen out of this relationship, either legal or contractual. The purposes for collecting and processing employees' personal data must be precisely determined, and the employees must be aware of the purposes of processing in advance and understand them.[68]

The Data Protection Authority, in its Directive 1/2011 concerning "the use of CCTV systems for the protection of persons and property", stressed the high importance of the application of the principle of proportionality.[69] Furthermore, according to the Authority,[70] the surveillance cameras may be exceptionally

[65]See, *e.g.* DPA Decision no. 245/2000 on processing of personal data of workers for the purposes of entrance and exit at the workplace by means of taking fingerprints and Decision no. 637/2000 on monitoring of the calls of workers at the workplace.

[66]See DPA Directive no. 115/2001.

[67]See also Areios Pagos no. 1/2017.

[68]See, *e.g.* DPA Decision no. 34/2018.

[69]Art. 5 DPA Directive no. 1/2011.

[70]Art. 18 DPA Directive no. 1/2011.

hoeren@uni-muenster.de

permitted, where their use is justified by the nature or the conditions of work and is necessary for the protection of health and security of employees or the protection of high-risk workplaces, *e.g.* banks and military plants. The systems used for monitoring of places, such as the entrance and exit at the premises of an enterprise or places where safe deposit boxes or electromechanical equipment are located, are compliant with the law, if the cameras focus on the property or goods to be protected and are not used to control employees at the workplace.

The new Law 4624/2019 adopts the principles in respect to the surveillance at the workplace mentioned above (art. 27). It states that the surveillance systems at the workplace shall be used in a way that does not offend the dignity of the employees. The collection of employees' personal data shall be limited to those data that are directly connected to employment and not extend, as far as possible, to the personal behaviour and personal contacts of the employees. The personal data of employees that are collected by means of a surveillance camera is prohibited to be used as criteria for their evaluation.[71]

As concern the thorny issue of the consent that is necessary for processing employees' personal data, the Data Protection Authority held that the imbalance of powers between the parties in an employment relationship casts doubts on the possibility of the employees to refuse giving their consent or withdraw it without any detriment being suffered. Such an opinion appears to be aligned with the approach adopted by the General Data Protection Regulation.[72]

A specific regulation is provided for by the Greek legislation in respect to the medical data of employees. Pursuant to Law 3144/2003 on "social dialogue for the promotion of employment and social protection",[73] the processing of medical data shall be only permitted if it were necessary for the evaluation of an employee's suitability for work or for implementing the employer's duty to protect the health and safety of employees, or to establish employee's rights to social benefits. Moreover, the personal data of employees is prohibited to be included in his/her individual book of professional risks, with the exception of the results of medical tests. In relation to data resulting from genetic examinations related to employees, the Authority held that such examinations were prohibited under the existed legislative framework as contravened to the principle of proportionality, taking also into consideration the constitutionally guaranteed human values.[74]

Finally, worth to mention is a judgment recently rendered by Areios Pagos on a case concerning claims of an employer against his employees who had provided corporate information to a competitor company via electronic mail.[75] The critical e-mails have been sent using corporate computers and corporate electronic addresses

[71]See also DPA Directive no. 115/2001 on the processing of employees' personal data, part e, §§ 6–8.

[72]See the recital 155 of the GDPR.

[73]Article 8 L. 3144/2003, Government Gazette A 111.

[74]See DPA Directive no. 115/2001 on the processing of employees' personal data, part d, §7.

[75]Areios Pagos no. 1/2017.

hoeren@uni-muenster.de

and stored in the hard disk of the computers used by the defendants.[76] The contents of the e-mails infringed the employers' rights protected by legislation on unfair competition. The Court estimated that, in the circumstances of the case, the exercise of the right to judicial protection by the employer[77] to secure his right to carry on business activity[78] prevailed over the constitutional right of the employees to protect their personal data[79]; thus, the contents of the harmful emails might be admitted as evidence in court against the defendants.

The employees may exercise all remedies provided for by the Civil Code in regard to the right to personality as well as those remedies provided for by the legislation on personal data protection.[80] The waiving of the rights conferred to the employee by Law 2472/1997 is void.[81] The exercise of the rights by the employee cannot lead to unfavourable results for him/her. If an employee considers that the infringement makes the performance of work intolerable, s/he may abstain from the work for as long as the insult occurs; in that case the employer is in default and the employee continues to have claims to wages.

2.1.5 Security Obligations and Data Breach Notifications Concerning Data Processed by Electronic Means

Under Law 2472/1997, the data controller had the duty to take the appropriate organisational and technical measures to ensure security and protection of personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to as well as any form of unlawful processing,[82] during the whole data processing period, which was completed with the destruction of the data.[83] However, a controller was not obliged to give notice of data breach or an incident concerning the security of personal data to the Data Protection Authority or the data subject concerned, as a controller is obliged to do according to the General Data Protection Regulation.

[76] According to Areios Pagos, when an electronic correspondence has been terminated, it is no longer protected by art. 19 of the Constitution, which guarantees the correspondence secrecy, but by art. 9A of the Constitution on personal data protection. See also the Opinion no. 6/2008 of the Attorney of Areios Pagos, according to which a hard disk is not a means of communication; hence, the data stored in a hard disk do not fall within the protective scope of the communication secrecy.

[77] Art. 20 § 1 of the Constitution.

[78] Articles 5 and 106 § 2 of the Constitution.

[79] Article 9A of the Constitution.

[80] See Malagardi (2010), pp. 297 ff.

[81] See DPA Directive no. 115/2001.

[82] Art. 10 § 3 L. 2472/1997.

[83] Art. 4 § 1 d L. 2472/1997. See also DPA Directive no. 1/2005 concerning the secure destruction of personal data after the end of the period that is required for the accomplishment of the processing purpose.

hoeren@uni-muenster.de

Unlike general Law 2472/1997, an obligation of the providers of publicly available electronic telecommunications services to notify the Data Protection Authority as well as the Authority for Communication Security and Privacy (ADAE), when data breach occurs, is imposed by Law 3471/2006.[84] Such a notification shall include at least a description of the nature of the breach, the contact points from which further information can be obtained, a description of the consequences of the breach as well as the measures that were suggested or taken by the provider. If the personal data breach is likely to affect the personal data or the private life of the subscriber, the provider is also obliged to notify the subscriber, except if s/he has proved that implemented appropriate technological security measures, which must at least include secure data encryption. The Authorities, mentioned above, can jointly issue guidelines concerning the circumstances in which providers are required to notify personal data breaches.

2.1.6 Specific Legislation on Certain Sectorial Areas Regarding the Processing of Personal Data by Electronic Means

Under the Code of Medical Ethics,[85] the doctors are obliged to maintain medical records, in electronic form or other, containing data that are linked to the disease or the health of their patients. The processing of medical records is subject to stricter requirements provided for sensitive data.[86] A patient is entitled to access his/her health data[87] and the national or international records where his/her personal data have been added.[88]

In virtue of Article 41 of Regulation 1987/2006 on Schengen Information System ("SIS II"), the rights of the third-country nationals who are registered to Schengen Information System II or/and to national catalogue of undesirable aliens (EKANA)[89] as concern their personal data are governed by the Greek legislation on personal data protection. It follows that the Data Protection Authority applies national legislation on personal data protection to relevant objections raised by third country nationals.

Finally, the processing of personal data collected by unmanned aerial vehicles ("drones") is governed by the general legislation on data protection in conjunction with article 14 of Law 3917/2011 concerning the use of surveillance systems in public areas. In addition, article 370A of Criminal Code is applicable, pursuant to which intercepting "by monitoring using special technical means or taping non-public conversations or video recording non-public acts of third parties" is punishable. Furthermore, the directives and opinions issued by the Data Protection

[84] Art. 12 §§ 5–10 L. 3471/2006.

[85] Law 3418/2015, Government Gazette A 287.

[86] See Latsiou (2016), p. 155.

[87] Art. 12 L. 2472/1997 and art. 14 § 8 L. 3418/2005.

[88] Art. 14 § 10 L. 3418/2005.

[89] Papassiopi-Passia and Kourtis (2015), pp. 83 ff.

hoeren@uni-muenster.de

Authority in relation to the CCTV systems and the use of systems of surveillance must also be respected on the matter.[90] This legal framework, however, is considered by the Greek theory as inadequate to protect an individual.[91]

2.2 *Data Protection in the Electronic Communications Sector*

2.2.1 Legal Framework

The Greek Constitution guarantees the right of confidentiality of letters and all other forms of free correspondence or communication (article 19 §1a), included all the means of telecommunication and the internet.[92] Restrictions on the freedom of communication and the protection of confidentiality are only allowed under the conditions set up by article 19 §1b of the Constitution, which provides that the judicial authority is not bound by the provisions above for reasons of national security or for investigating especially serious crimes under guaranties which are specified by law. Such guaranties are provided for by Law 2225/1994 on the protection of personal data processing and private life in the sector of telecommunications, as in effect.[93] In the past, the Greek theory as well as the courts admitted that the traffic and location data of communication did not fall within the definition of communication protected by the Greek Constitution and, as a result, only the content of communication was protected.[94] According to the opinion that is now predominant, the traffic and location data fall within the protective scope of article 19 of the Constitution interpreted in the light of article 8 ECHR.[95]

The processing of personal data as well as the safeguarding of confidentiality in communications in the field of publicly available electronic communications services are governed by Law 3471/2006, while the processing of personal data within the framework of not publicly available networks and electronic communications services is governed by the general legislation on data protection.[96] Law 3471/2006

[90] See DPA Directive no. 1/2011 and Opinions nos. 1/2009 and 2/1010.

[91] See Tsolias (2016), pp. 363 ff.

[92] See Spyropoulos and Fortsakis (2009), p. 228; Papadopoulos (2009), pp. 169 ff.; Karakostas (2009), p. 153.

[93] Government Gazette A 121.

[94] See Manessis (1982), p. 238 and the decision of Areios Pagos no. 570/2006. The same steps were followed by the opinions of the Attorney of Areios Pagos nos. 9/2009, 12/2009 and 9/2011.

[95] Areios Pagos no. 924/2009, relied, *inter alia*, on the decision Copland v. UK. See also the ADAE Opinion no. 1/2005, by which the Authority changed its previous view and admitted the confidentiality of communication data.

[96] Art. 3 § 1 L. 3471/2006.

hoeren@uni-muenster.de

applies to individuals as well as to legal persons, as it is implied by the definition of the "subscriber"[97] and by the provisions regarding unsolicited communication.[98]

2.2.2 The Notion of Communication Data

"Traffic data" are, according to the Greek legislation, the data processed for the purposes of the conveyance of a communication on an electronic communications network or for the billing thereof.[99] "Location data" are the data indicating the geographic location of the terminal equipment of a user of a telecommunication service available to the public. The court decisions refer the term "communication data", by which is meant the information generated during a communication, which determines the conditions of the communication and identify it, such as location, time, duration, format and type of communication, as well as means by which the communication was conducted and details of the communication partners.[100] Greek academics often refer to the communication data by the terms "external data" or "context data" as opposed to "internal data" or "content data", which consist of the actual content of the electronic communication.[101]

2.2.3 Confidentiality of Electronic Communications

Law 3471/2006 specifies that any use of electronic communications services offered through a publicly available electronic communications network, as well as the related traffic and location data are protected on the basis of the principle of confidentiality of communications. The lifting of confidentiality is only permitted under the conditions and procedures provided for by Article 19 of the Constitution.[102] The listening, tapping, storage or other kinds of interception or surveillance of the content, as well as of the traffic and location data are prohibited, except when the law provides for otherwise.[103] Certain circumstances where the confidentiality lowers are the following: (a) The recording of a communication, *e.g.* in the case of phone banking, is permitted when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of

[97] Art 2a L. 3471/2006.

[98] Art. 11 § 7 L. 3471/2006.

[99] They may, *inter alia*, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or the recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network, see Art. 2 § 3 L. 3471/2006.

[100] See Council of State no. 1593/2016.

[101] See Arkouli (2010), pp. 4–5; Christodoulou (2013), p. 130; Tountopoulos (2000), p. 476.

[102] Art. 4 § 1 L. 3471/2006.

[103] Art. 4 § 2 L. 3471/2006.

hoeren@uni-muenster.de

any other business communication, under the condition that both parties have provided their consent, upon previous notification of the aim of the recording.[104] The parties do not waive of their right for confidentiality when they give their consent for such recording[105]; (b) The technical storage is permitted, where necessary for the conveyance of the communication[106]; (c) The storage of data or the acquisition of access to information already stored in the equipment of a subscriber or user is only allowed, if their purpose is the conveyance of information through an electronic communications network or is necessary for the provision of information society services explicitly requested by the user or subscriber, and upon the prior consent of the latter[107]; (d) The provider of a public network or publicly available electronic communications services is permitted to process traffic data aiming at the subscriber's billing and interconnection payment,[108] without the consent of the user.

2.2.4 Security Measures Implemented by the Electronic Communications Providers for the Protection of Personal Data

The providers of public communications networks or publicly available electronic communications services are obliged to erase or make anonymous the traffic data processed or stored, which are relating to subscribers or users at the end of the transmission of communication.[109] Furthermore, they must inform their subscribers about the purposes of a directory of subscribers available to the public. The subscribers have the option not to be included in such a directory. The personal data included in such directories must be limited to those data that are necessary for the identification of a subscriber, unless the subscriber wishes otherwise. Where the subscriber is a legal entity, the data published in a directory are limited to those necessary to ascertain the identity of the legal entity, unless its legal representative has given written consent on the publication of complementary data.[110]

[104] Art. 4 § 3 L. 3471/2006. The way in which parties are notified and give their consent as well as the manner and duration of storage for the recorded conversations and relevant traffic data are determined by act issued by the DPA.

[105] See Papadopoulos (2009), p. 216.

[106] Art. 4 § 4 L. 3471/2006.

[107] Art. 4 § 5 L. 3471/2006.

[108] Art. 6 § 2 L. 3471/2006.

[109] See L. 3917/2011 and §§ 2–6 L. 3471/2006.

[110] Art. 10 L. 3471/2006.

hoeren@uni-muenster.de

2.2.5 Supervisory Authorities for Communication Security and Privacy

The Authority for Communication Security and Privacy (ADAE) has been established by Law 3115/2006,[111] in virtue of Article 19 § 2 of the Constitution. Its purpose is the protection of correspondence confidentiality, free communication in any possible way, as well as the networks' and information security. It reports to the Minister of Justice and its seat is in Athens.[112] By virtue of the powers vested in it, ADAE is competent for a number of matters regarding the application of Law 3471/2006 on the protection of personal data and privacy in the electronic communications.[113]

In particular, ADAE carries out *ex officio* or upon complaint, inspections at installations and databases, as well as inspections of documents of the public services, including the Greek National Intelligence Service, and documents of private companies that are involved in postal, telecommunications or other services concerning networking and communication. It examines complaints concerning the protection of persons whom rights are prejudiced by the way and procedure of lifting communication confidentiality. It is empowered to proceed to the seizure of the means of breach of secrecy, the destruction of information, evidence or data, which were obtained illegally. It issues opinions and recommendations regarding the measures to be taken to secure the communications confidentiality. And, it submits to the Parliament an annual activity report containing observations and suggestions for appropriate legislative changes.[114] Furthermore, ADAE is entrusted the task to set up the specific procedures that are necessary for certain circumstances to be dealt, such as the processing of the location data that is exceptionally permitted without the prior consent of the subscriber or user for purposes of emergency,[115] the tracing of the nuisance calls, following a subscriber's request[116] and the compatibility issues arisen between the voice messages encryption methods used by the providers.[117] Moreover, ADAE carries out inspections in the infrastructure, hardware and software which are under the supervision of the providers to verify its compliance with the legislation regarding the confidentiality of communications.[118]

Since competent for the application of the Law 3471/2006 is also the Hellenic Data Protection Authority, as, *e.g.*, for imposing administrative sanctions, often it is not easily identifiable which authority is competent to decide cases concerning data

[111] Government Gazette A 47.

[112] See the website of this Authority, at: www.adae.gr/en.

[113] Art. 13 § 2 L. 3471/2006.

[114] Art. 6 L. 3115/2003.

[115] Art. 6 § 5 L. 3471/2006.

[116] Art. 8 § 7 L. 3471/2006.

[117] Art. 4 L. 3674/2008.

[118] Art. 6 L. 3674/2008.

hoeren@uni-muenster.de

processing in the sector of telecommunications. The distinction of their competences is often not based on legal criteria.[119]

2.3 Data Protection and Digital Forensics

The personal data protection provided for by the Greek law is restricted where personal data processing is carried out by judicial or public prosecution authorities in the framework of attributing justice or for verifying serious crimes, especially crimes against life, sexual freedom, personal freedom, property rights, minors, public order and violations of legislation regarding drugs.[120] The recording of sound or image by means of special technical devices made by the authorities with purpose to verify the perpetration of the crimes is only permitted upon an order issued by a Public Prosecutor and provided that a serious danger to the public order or security is imminent. Furthermore, by way of exception to the general prohibition of processing *sensitive* personal data, the Public Prosecutor can order the public disclosure of information relating to cases of criminal prosecution or conviction. That disclosure aims at the protection of the general public, of minors and of vulnerable or disadvantaged groups, as well as at the facilitation of the punishment of those offences by the State.[121] In theory, it was argued that the restrictions mentioned above are contrary to the Constitution.[122]

By virtue of the principle of necessity, which governs the restriction of the fundamental right to the protection of personal data, the recognition, exercise or defence of rights before a court or a disciplinary body constitutes a basis for exceptionally justifying the processing of *sensitive* data.[123] Areios Pagos held that the processing of *simple* data is also subject to the same exception.[124] The Data Protection Authority held that a provider of mobile telecommunication services was allowed, upon previous notification of the data subject, to provide telephone call data to a third party to use them for defending himself in criminal proceedings.[125]

Regarding the interception of communication data, Law 2225/1994 on "the protection of personal data processing and private life in the sector of telecommunications"[126] sets the requirements and the procedures for the lawful interception of the content of communications as well as the access to communication data. This

[119] See Papakonstantinou (2010), § 15.3.01.

[120] Art. 3 § 2 b L. 2472/1997.

[121] Art. 2 b L. 2472/1997/.

[122] See Iglezakis (2011), p. 2.

[123] Art. 7 §2c L. 2472/1997.

[124] Areios Pagos 252/2018 (A 2). The same opinion has been expressed by the Authority, see, *e.g.*, the decisions nos. 27/2001, 75/2001, 92/1011, 111/2011 and 4/2013.

[125] DPA Decision no. 12/2004.

[126] Government Gazette A 121.

hoeren@uni-muenster.de

Law contains a list of serious crimes, the investigation, detection and prosecution of which allows the access to communication data or real time lawful interception of communication by the competent authorities. The list contains: (a) Offences of the Penal Code: In particular, offences against the constitutional status and against the life of political persons, treason against the Greek State, offences against the Parliament, political parties or the Government, violence against the person or the honour of the President of the Republic and torture or other violations of human dignity perpetrating by public officials or members of the armed forces; Offences relating to organized crime or terrorism, forgery and circulation of counterfeit currency, and passive or active bribery of a public official, including a judge; Common dangerous offences, offences against security in transportation and telecommunications, offences against human life and personal freedom, offences relating to violation of secrecy (unlawful interception of telecommunication, unlawful monitoring or recording of private transmission of data or electromagnetic emissions by any technical means or interfering with them in order to know their content as well as use of such recordings) and offences against property. (b) Offences of the Military Penal Code; and (c) other offences provided for by specific penal legislation, such as offences relating to arms trafficking, drugs trafficking, smuggling, bribery of foreign public officials, money laundering, environmental protection, protection of capital market from actions of persons that possess inside information and actions for market, protection of antiquities and protection of the cultural heritage.

According to the procedure set out by Law 2225/1994, the competent Public Prosecutor files the application to the judicial council that is competent to issue the necessary order.[127] This order shall contain the details of the person against whom the measure of interception is taken and the reasoning for the lift of secrecy.[128] The order is sent to the electronic communication network/service provider, which executes it by sending the communication data to the competent authorities within 7 days. If the order concerns real-time lawful interception the provider grants access to the communications under interception within 3 days. The Presidential Decree 47/2005 on "the procedure, technical and organisational guarantees for ensuring lawful interception"[129] stipulates the details for the technical and organisational measures that shall be taken for lawful interception and access to data. Between others, it contains the list of data that must be provided for each type of electronic communication. This list contains the content data as well as the traffic and location data of communications.

Law 3917/2011 regulates the *retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, use of surveillance systems with the*

[127] A panel of judges deciding in camera; their decisions must be reasoned like the decisions in public trials.

[128] Art. 5 §§2, 3 L. 2225/1994.

[129] Government Gazette A 64.

hoeren@uni-muenster.de

obtaining or recording of sound or image at public areas and relative provisions, implemented Directive 2006/24.[130] This Law also provides for further measures on the effective protection of the retained data of communication of subscribers and registered users, with respect to the principle of proportionality and it specifies the requirements for the installation and operation of surveillance systems at public areas. A special committee was set up by the Ministry of Justice to study the abolition or modification of Law 3917/2011, so that the Greek law to be complying with the CJEU's decision on the cases C-293/12 and C-594/12; in the meanwhile, this Law is still in force.

Law 3917/2011 applies to traffic and location data on legal entities as well as natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network. The categories of data that can be retained follow verbatim the categories referred to in Directive 2006/24. Pursuant to Article 1 §1, the providers are obliged to retain the traffic and location data in order to be available to the competent authorities for investigating, detecting and prosecuting very serious crimes.[131]

2.4 Data Protection and Electronic Surveillance for Security and Defence Purposes

National security is a constitutionally established reason for allowing restrictions on the freedom of communication and protection of confidentiality under guarantees, which shall be specified by law.[132] Due to its vagueness, the concept of national security must be specified in each one case regarding personal data protection.[133] In respect to processing of personal data on grounds of national security, certain restrictions to the basic rules regarding data protection are provided for.

In particular, the processing of *sensitive* personal data is exceptionally allowed when is carried out by a public authority and is necessary for the purposes of national security or public health.[134] Even in such a case, the basic requirements for lawful processing must be met.[135] The processing of other (simple) personal data is allowed without the data subject's consent when processing is necessary for the performance of a task carried out in the public interest or carried out in the exercise of public function by a public authority.[136] When the processing is carried out on national

[130] Government Gazette A 22.

[131] As defined by art. 4 L. 2225/1995.

[132] Art. 19 § 1b of the Constitution.

[133] See Alexandropoulou-Aigyptiadou (2016), p. 102.

[134] Art. 7 § 2e L. 2472/1997.

[135] As laid down by articles 4 and 5 L. 2472/1997. See also Iglezakis (2003), p. 238.

[136] Art. 5 § 2d L. 2472/1997.

hoeren@uni-muenster.de

security grounds or for the detection of particularly serious crimes, the controller may be released from the obligation to inform the data subject about the contents of personal data collected and the purpose of processing upon decision by the Data Protection Authority.[137] In a case regarding a Greek Coastal Guard's request addressed to providers of telecommunication services to disclose personal data of their subscribers, which were necessary for the Coastal Guard to exercise its law enforcement task, the Data Protection Authority based on the fact that the enforcement tasks of the Coastal Guard concern the national security and the detection of serious crimes, considered the subscribers' consent not necessary for processing and released the providers of his/her obligation to inform their subscribers for the disclosure of the data requested.[138]

2.5 Remedies and Sanctions

Remedies and sanctions are provided for by the common Greek legislation as well as by the special legislation on personal data protection. The civil and criminal sanctions are imposed by courts and the administrative sanctions by the Data Protection Authority.

2.5.1 Civil Sanctions

The person affected by unlawful processing of his/her personal data is protected, firstly, on the basis of the provisions of the Greek Civil Code regarding the right to personality.[139] Regarding the violation of personality, the person has the right to claim the cessation of the violation and the refrain thereof in the future. In addition, one has the right to damages and compensation for moral damage.[140]

Furthermore, on the basis of the Greek data protection legislation, the data subject has a right to provisional judicial protection.[141] Moreover, civil law sanctions are provided for breach of data protection legislation.[142] Any individual or legal entity of private law that causes material damage or non-material damage shall be liable for damages in full or compensation, respectively. The liability is considered objective, so that the party who suffered damage is not required to prove the fault of the

[137] Art. 11 § 4 L. 2472/1997.
[138] DPA Decision no. 19/2008.
[139] Articles 57 and 59 CC.
[140] Articles 914 and 932 CC.
[141] Art. 14 L. 2472/1997.
[142] Art. 23 L. 2472/1997 and Art. 14 L. 3471/2006.

hoeren@uni-muenster.de

controller,[143] except if s(he) gave the relevant consent.[144] Under Law 2472/1997, the compensation payable for non-material damage was set at the amount of *at least* two million drachmas (about 6000 euros), unless the plaintiff claimed a lesser amount for compensation, or the breach was due to negligence.[145] Areios Pagos held that the minimum threshold provided for compensation is contrary to the Constitution.[146] Under Law 3471/2006, the compensation is set at the amount of at least 10,000 euros, unless the plaintiff claims a lesser amount. The claims shall be litigated according to the Code of Civil Procedure, notwithstanding whether the Authority has issued a relevant decision or whether criminal charges have been filed.

The new Law 4624/2019 recognizes the right of the data subject who considers that his/her rights under the GDPR or Directive 2016/680 or other data protection legislation have been infringed as a result of the processing to bring an action before the Greek courts against the controller or processor claiming compensation (art. 40). The data subject has the right to mandate a not-profit body or organisation or association, which has statutory objective the protection of data subjects' rights and freedoms with regard to the protection of their personal data to exercise his/her rights to seek judicial redress for compensation (art. 41).

2.5.2 Criminal Sanctions

The earlier Greek data protection legislation[147] as well as the new Law 4624/2019 provides for criminal sanctions: In particular, anyone who unlawfully interferes in any way with a personal data file or takes notice of such data or extracts, alters, hurts, destroys, processes, transfers, discloses, makes accessible to unauthorized persons or permits such persons to take notice of such data or anyone who exploits such data in any way, will be punished by imprisonment. If the offences mentioned above concern special categories of data or data relating to convictions or security measures, the perpetrator will be punished by a term of imprisonment of between 1 and 5 years and by a fine ranging from 10,000 to 100,000 euros. If the perpetrator purported to jeopardize the free functioning of democratic government or national security, the sanctions imposed shall be imprisonment for a period at least of 5 years and by a fine ranging from 100,000 to 300,000 euros. If the perpetrator of any of the acts mentioned above purported to gain unlawful benefit on his/her behalf or on behalf of another person or to cause harm to a third person, s/he shall be punished by a term of imprisonment of at least 3 years and by a fine ranging from 100,000 to

[143] See Augoustianakis (2011), pp. 673 ff.

[144] See Areios Pagos no. 1284/2017.

[145] See Areios Pagos no. 476/2009.

[146] Areios Pagos no. 252/2018 (A 2). The same opinion was expressed in the past by academics, see Kornilakis (2002), p. 435.

[147] See articles 22 L. 2472/1997 and 15 L. 3471/2006. On the criminal sanctions see also Anastassopoulos (2016), pp. 421 ff.; Nouskalis (2005).

hoeren@uni-muenster.de

300,000 euros.[148] A data protection officer who violates his/her duty of confidentiality shall be punished by a term of imprisonment between 1 and 5 years and by a fine ranging from 10,000 to 100,000 euros.

2.5.3 Administrative Sanctions

Under the outgoing Law 2472/1997, the Personal Data Authority was empowered to impose on the controllers the following administrative sanctions for breach of duties arising out of the personal data protection legislation[149]: (a) A notice of violation with an order to cease within a specified time limit[150]; (b) a fine amounting between c. 900 and c. 147,000 euros[151]; (c) a temporary or definitive revocation of the permits that have been granted by the Authority to the perpetrator in order to collect and process sensitive personal data or to establish and operate the file or to interconnect files containing sensitive data, or for the purpose of transborder transmission of data; and (d) the destruction of the file or disruption of processing and destruction, return or locking of the relevant data.[152] The sanctions under (c) and (d) shall only be imposed in case of a particularly serious or repeated violation. A fine may be imposed in conjunction with the sanctions under (c) and (d).The decisions issued by the Authority imposing a fine constitute an enforceable instrument. They may be challenged before the Council of State. The maximum fine imposed by the DPA to

[148]The earlier legislation (L. 2472/1997) also imposed criminal sanctions for acts or omissions for which the Authority has not yet issued a decision, such as the non-notification of the establishment of a file or the operation of a file containing sensitive data without permit or in breach of the terms and conditions referred to the Authority's relevant permit. Moreover, for not complying with the courts' decisions ordering provisional measures as well as for not implementing decisions issued by the Authority. Furthermore, for unlawful transfer of personal data as well as interconnection of files without the Authority's permit.

[149]Art. 21 L. 2472/1997.

[150]See, *e.g.*, the DPA Decisions no. 61/2004 [notice addressed to employer to cease recording the webpages visited by employees], no. 11/2005 [notice addressed to banks and to an insurance company to apply the necessary procedures for the secure deletion of personal data after the termination of the period required for the purposes for which such data were processed], no. 17/2016 [notice to Mayor to delete postings in his Facebook containing references to third party's sensitive personal data].

[151]See, *e.g.*, the DPA decision no. 71/2017 [imposition of a fine of 10,000 euros on a telephone company for failing to implement the right to access according to Art. 12 L. 2472/1997].

[152]See, *e.g.*, the decisions of the DPA: no. 38/2005 [prohibition to a TV station to re-broadcast and use a transcribed text containing unlawful processing of personal data], no. 8/2016 [order against a rehabilitation care center for disabled persons to uninstall video monitoring system that operated unlawfully and to destruct of any relevant file containing personal data collected], no. 245/2000 [order against a Municipality to disrupt data processing that intended to monitor the entrance and exit of employees at the workplace].

hoeren@uni-muenster.de

date on a public authority for failing to take appropriate security measures during the processing of taxpayers' personal data.[153]

The new Law 4624/2019 provides that, without prejudice to its corrective powers according to art. 58 § 2 of the GDPR, the Data Protection Authority is empowered to impose the administrative fines provided for by article 83 §§ 4, 5 and 6 of the GDPR.

3 The International Dimension of Data Protection

3.1 The Territorial Scope of the Rules on Data Protection

The outgoing Law 2472/1997, implementing Directive 95/46, based its territorial scope on the criterion of the place of establishment of the controller/processor or the place in which the equipment used for the purposes of the personal data processing was situated. Specifically, Greek Law was applicable to any personal data processing, which was carried out by a controller or a processor established on the Greek territory, or in a place where the Greek law was applicable by virtue of international law, *e.g.* a Greek embassy.[154] A conflict of laws rule was established for intra-community cases, according to which the data protection law of the member state in which the controller was established applied, regardless of the place where the equipment was situated.

A controller is considered to be established in Greece when s/he exercises effective and real activity through stable arrangements in the country. The "form of the arrangements, for example, whether they are carried out through a branch or a subsidiary, is not relevant".[155] The term "establishment" was given a broad interpretation by CJEU in the well-known decisions rendered on the cases Spain Google and Weltimmo.[156] According to that case-law, the concept of establishment in Greece within the meaning of Directive 95/46 and Law 2472/1997 extends to any real and effective activity, even a minimal one, exercised through stable arrangements in Greece and the presence of only a representative in Greece can be sufficient to constitute a stable arrangement. This reasoning of the Court was replicated by the language of the GDPR. Under Regulation, of high importance is the concept of "main establishment".[157]

[153] DPA decision no. 98/2013.

[154] Art. 3 § 3 L. 2472/1997.

[155] See recital 19 of Directive 95/46; see also recital 22 GDPR.

[156] CJEU, 13.05.2014, C-131/12, Google Spain *v* Agencia Española, ECLI:EU:C:2014:317; 01.10.2015, C-230/14, Weltimmo *v* NAIH., ECLI:EU:C:2015:639.

[157] See art. 4 (16) GDPR.

hoeren@uni-muenster.de

3.2 The Applicability of Data Protection Rules to Foreign Entities

The rules of Law 2472/1997 were also applicable to personal data processing carried out by a controller established in a third country, *i.e.* outside the EU/EEA territory, who, for the purposes of processing, used of the equipment situated on the Greek territory, except if the equipment was used only for data transfer through the Greek territory. In the latter case, the controller should appoint, by a statement addressed to the Data Protection Authority, a representative established in Greece, who substituted the controller to all his/her rights and duties, without prejudice to legal actions which might be initiated against the controller. The same applied when the controller or processor was subject to immunities or other reason prohibiting criminal prosecution.

The Greek Law, like the Directive 95/46, did not explicitly enshrined as criterion for its territorial scope the "market-place principle",[158] so individuals domiciled in Greece often deprived of the high protection in respect to their personal data provided for by the harmonized EU legislation, when the controller was established outside the EU and the data processing was related to offering of goods or services in Greece by non-EU businesses (e-shops). The extended extraterritorial applicability of the General Data Protection Regulation opens a promising perspective on this matter.

According to the new Law, which has been enacted to implement the GDPR in Greece, the Regulation as well as the new Law apply to the processing of personal data carried out in Greece, as well as the processing carried out in the context of the activities of an establishment in Greece, regardless of whether the processing takes place in Greece or not.

3.3 The Specific Conditions Applicable to the Transfer of Personal Data to a Foreign Jurisdiction

Until the entry into force of the GDPR, the article 9 of Law 2472/1997, following article 25 of Directive 95/46, regulated the transborder flow of personal data. The term transfer of personal data was not defined by the Greek legislation, as was not defined by the Directive 95/46. With respect to the meaning of this term, important is the decision rendered by the CJUE on the case Lindquist.[159]

According to the outgoing Law 2472/1997, the transfer of personal data from Greece to another EU Member State was freely allowed, while the transfer of

[158] See the General Report, no. 4.2.

[159] CJEU, 06.11.2013, C-101/2001, Lindquist, ECLI:EU:C:2003:596. On this matter, see Yannopoulos (2001), pp. 733 ff.

hoeren@uni-muenster.de

personal data to third countries was subject to preventive control by the European Commission or the Greek Data Protection Authority in respect to the adequate level of data protection ensured by the third country in question.

Specifically, the transfer of personal data to a third country was allowed if the European Commission confirmed on the basis of an adequacy decision that the country in question guaranteed "an adequate level of protection".[160] In the absence of a Commission's adequacy decision for a third country, the transmission of personal data to that country might be done upon a permit granted by the Data Protection Authority. For examining if the third country offered an adequate level of protection, the Authority assessed the nature of the personal data, the purpose and duration of the data processing, the relevant general and specific rules of law, the codes of conduct, the security measures provided for the protection of personal data, as well as the protection level in the countries of origin, transfer and destination of the data.

Furthermore, the personal data might be exceptionally transmitted to a third country not ensuring an adequate level of protection upon a permit issued by the Authority on the basis of the data subject's consent, unless the consent has been deduced in a manner contrary to the law or the *bonos mores*, *e.g.*, hiding the country where the personal data would be really kept.[161] Other grounds which could make the personal data transfer permissible was the protection of the vital interests of the data subject, the conclusion or performance of a contract, important reasons of public interest, the establishment or defence of a right in court, or that the transfer was carried out by a public register intended to provide information to the public. Moreover, if the data controller might ensure that the personal data would be sufficiently protected by the recipient; this could be assured using contractual clauses.[162]

Among the changes which the GDPR brings to the system of international data transfers established by the Directive 95/46 and the Law 2472/1997, as described above, the most important are the adoption of new legal bases for the transborder transfer of personal data and the abolition of the supervisory Authority's power to certify the adequate level of data protection of a third country or to decide if an entity has adapted a satisfactory personal data protection control system. Under the GDPR, this decision-making burden is largely transferred from the Authorities to the controllers. However, this change raises doubts as to whether all the private and public entities processing personal data provide sufficient guarantees for the purposes of reaching a proper decision.[163]

[160]Compare this to art. 45 GDPR; for more details regarding the procedure provided for by the GDPR for the issuance of the Commission's decision, see the General Report, no. 4.3.

[161]DPA Decision no. 12/2003.

[162]A permit was not required if the Commission had decided, based on art. 26 § 4 of Directive 95/46 that certain conventional clauses offered adequate safeguards for the protection of data.

[163]See Vlachopoulos (2018).

hoeren@uni-muenster.de

3.4 The Law Applicable to Liability for Damages Caused by the Unlawful Processing of Personal Data

The protection of personal data is deemed as a matter that falls within the scope of the protection of privacy and rights related to personality, so the infringement of personal data legislation is excluded from the material scope of the Regulation 864/2007 on applicable law to non-contractual obligations ("Rome II Regulation"). Greek academics support the exclusion of civil liability for damages caused by unlawful processing of personal data from the scope of Rome II Regulation.[164] Consequently, the liability for damages caused by the unlawful data processing is governed by article 26 of the Civil Code, according to which *lex loci delicti* applies. The academic discussion in Greece regarding the place where the wrongful act was committed in case of the so called "offences at a distance" and the disseminated or multiple-location offences never reached a conclusion, with some tendency to favour conduct over effects or to give plaintiff the choice.[165] The Greek courts favour the possibility of the injured party to choose the applicable law.[166] In absence of such a choice, the courts usually apply the law of the state where the most significant element or elements of the damage occurred.

The cases of infringement of rights of personality brought before the Greek courts are usually defamation cases. The case law admitted that the location of the wrongful act of defamation is the place where the defamatory material is received and read. Based on this opinion, in a published judgment concerning defamation committed by means of content posted on an internet website, the court considered that the plaintiff's reputation was harmed in Greece, where he had his habitual residence, as well as in those countries where the defamatory content was accessible. It applied Greek law based on the criterion that the damage has been suffered mostly in Greece.[167]

As regards the applicable law to delictual claims arisen out of the legal relationship between the provider of services provided at a distance and the recipient of the service, in Greek theory it has been argued that the law designated by article 2 of the Presidential Decree 131/2003, which transposed the article 3 of Directive 2000/31, is applicable not only to contractual claims arisen out of an agreement for provision of information society services but also to delictual claims arisen from the same legal relationship.[168]

[164] See Grammatikaki-Alexiou (2016), p. 532; Christodoulou (2013), p. 142.

[165] For the different theories that have been formulated on the issue see Vrellis (2008), pp. 249 ff.

[166] See Areios Pagos no. 903/2010.

[167] See Court of Appeals of Rhodes no. 220/2013.

[168] See Christodoulou (2010).

hoeren@uni-muenster.de

References

Alexandridou E (2018) Electronic commerce. In: Alexandridou E (ed) Law of consumer protection, 3rd edn. Nomiki Vivliothiki, Athens (in Greek)
Alexandropoulou-Aigyptiadou E (2016) Personal data. Nomiki Vivliothiki, Athens. (in Greek)
Anastassopoulos D (2016) Criminal protection of personal data. In: Kotsalis L (ed) Personal data. Nomiki Vivliothiki, Athens, pp 421 ff (in Greek)
Arkouli K (2010) Personal data protection in electronic communications. Nomiki Vivliothiki, Athens. (in Greek)
Armamentos P, Sotiropoulos V (2005) Personal data: interpretation of law 2472/1997. Sakkoulas Publications, Athens. (in Greek)
Armamentos P, Sotiropoulos V (2008) The amendments of law 2472/1997 by laws 3471/2006 and 3625/2007. Sakkoulas Publications, Athens. (in Greek)
Augoustianakis M (2011) Protection of individual from personal data processing. Hum Rights J 673. (in Greek)
Christodoulou K (2010) Internet provider's liability for infringements of the private sphere. Media Commun Law J 328. (in Greek)
Christodoulou K (2013) Law of personal data. Nomiki Vivliothiki, Athens. (in Greek)
Christodoulou K (2018) Minor's consent to personal data processing. In: Kotsalis L, Menoudakos K (eds) General Data Protection Regulation. Nomiki Vivliothiki, Athens (in Greek)
Christou V (2017) The right to protection against data processing. Sakkoulas Publications, Athens. (in Greek)
Chryssogonos K (2002) Individual and social rights. Nomiki Vivliothiki, Athens. (in Greek)
Delouka-Igglesis C (2018) Articles 9 and 9a-9i of law 2251/1994. In: Alexandridou E (ed) Law of consumer protection, 3rd edn. Nomiki Vivliothiki, Athens (in Greek)
Donos P (2000) The constitutional consolidation of the right to protection of the citizen against the processing of personal data and the corresponding independent authority. In: Papademetriou G (ed) Revision of the constitution and modernization of the institutions, pp 109 ff. (in Greek)
Donos P, Mitrou L, Mittleton P, Papakonstantinou V (2002) Personal data protection authority and the enhancement of the protection of rights. Sakkoulas Publications, Athens. (in Greek)
Douka V (2005) The protection of personal data in the employment relationship. Sakkoulas Publications, Athens. (in Greek)
Grammatikaki-Alexiou A (2016) Article 26 of the Greek Civil Code. In: Georgiadis A, Stathopoulos M (eds) Civil Code, 2nd edn, vol Ia. P.N. Sakkoulas, Athens (in Greek)
Iglezakis I (2003) Sensitive personal data. Sakkoulas Publications, Athens. (in Greek)
Iglezakis I (2006) Teiresias. Personal data protection in credit information systems. Sakkoulas Publications, Athens (in Greek)
Iglezakis I (2009) The law of electronic commerce. Sakkoulas Publications, Athens. (in Greek)
Iglezakis I (2011) Privacy protection. In: Manitotis D, Marinos M-T, Anthimos A, Iglezakis I, Nouskalis D (eds) Cyber law in Greece. Kluwer Law International
Iglezakis I (2014) The right to be forgotten and its limitations. Sakkoulas Publications, Athens. (in Greek)
Iglezakis I (2018) The General Data Protection Regulation. Interactive Books, Thessaloniki. (in Greek)
Iliadou E (2016) The constitutional safeguarding of personal data. In: Kotsalis L (ed) Personal data. Nomiki Vivliothiki, Athens (in Greek)
Karakostas I (2009) Law and internet. P.N. Sakkoulas, Athens (in Greek)
Kornilakis P (2002) Special law of obligations. Sakkoulas Publications, Athens. (in Greek)
Kotsalis L, Menoudakos K (2018) General Data Protection Regulation. Nomiki Vivliothiki, Athens. (in Greek)
Latsiou C (2016) Medical data. In: Kotsalis L (ed) Personal data. Nomiki Vivliothiki, Athens (in Greek)

hoeren@uni-muenster.de

Malagardi A (2010) New technologies – personal data and employment law. Ant. N. Sakkoulas, Athens (in Greek)
Manessis A (1982) Constitutional rights. Individual freedoms. Sakkoulas, Athens (in Greek)
Mitrou L (1999) The Personal Data Protection Authority. Ant. N. Sakkoulas, Athens (in Greek)
Mitrou L (2016) The protection of employees' data. In: Kotsalis L (ed) Personal data. Nomiki Vivliothiki, Athens, pp 191 ff. (in Greek)
Mitrou L (2017) The General Data Protection Regulation. Sakkoulas Publications, Athens. (in Greek)
Mittleton P (2016) The concept of personal data. In: Kotsalis L (ed) Personal data. Nomiki Vivliothiki, Athens, pp 5 ff. (in Greek)
Nouskalis G (2005) Criminal protection of personal data (in Greek)
Panagopoulou-Koutnatzi F (2016) The evolution of the right to be forgotten. J Administ Law 714. (in Greek)
Panagopoulou-Koutnatzi F (2017) The General Data Protection Regulation 679/2016/EU. Sakkoulas Publications, Athens. (in Greek)
Papachristou T, Papadopoulou-Klamaris D (2006) Medical confidentiality. In: Kounougeri-Manoledaki E et al (eds) The new code of medical deontology (law 3418/2005). Sakkoulas Publications, Athens (in Greek)
Papadopoulos N (2009) Protection of the confidentiality of communication. Interpretive approach to Article 19 of the Constitution of Greece. P.N. Sakkoulas, Athens (in Greek)
Papakonstantinou E (2010) Computer law. Sakkoulas Publications, Athens. (in Greek)
Papassiopi-Passia Z, Kourtis V (2015) Law of Aliens. Sakkoulas Publications, Athens (in Greek)
Sotiropoulos V (2006) The constitutional protection of personal data. Sakkoulas Publications, Athens. (in Greek)
Spyropoulos P, Fortsakis T (2009) Constitutional law in Greece. Kluwer Law International
Tountopoulos V (2000) The protection of personal data in the field of telecommunications. Bus Company Law 475
Tsevas A (2010) Personal data and mass media. Ant. N. Sakkoulas, Athens (in Greek)
Tsolias G (2016) Risks to individual's personal data due to the use of unmanned aerial vehicles (U.A.V., "drones"). In: Kotsalis L (ed) Personal data. Nomiki Vivliothiki, Athens (in Greek)
Vidalis T (2006) A suggestion for a constitutional right to participate in the information society. In: Papachristou T, Vidalis T, Mitrou L, Takis A (eds) The right to participate in the information society. Sakkoulas, Athens (in Greek)
Vlachopoulos S (2018) Cross-border transfer of personal data from E.U. to third countries. In: Centre of International and European Economic Law, Personal data protection, Sakkoulas Publications, Thessaloniki, pp 27 ff (in Greek)
Vrellis S (2008) Private international law, 3rd edn. Nomiki Vivliothiki, Athens. (in Greek)
Yannopoulos G (2001) Protection of personal data and cross-border flow of information. Revue hellénique des droit de l'homme 11 (in Greek)
Yerontas A (2002) Citizens' protection against the electronic processing of personal data (in Greek)

hoeren@uni-muenster.de

Italian National Report: Data Protection in the Internet

Vincenzo Zeno-Zencovich

1 Premise

Data protection in EU countries has been to a great extent harmonized over the last 20 years (Directive 1995/46 and subsequent amendments).

Data protection on telecom networks has been to a great extent harmonized for over 15 years (Directive 2002/22 and subsequent amendments).

Data protection has become a central aspect of EU external policy though a great number of decisions of the Court of Justice of the European Union

V. Zeno-Zencovich (✉)
Università degli Studi Roma Tre, Rome, Italy
e-mail: vincenzo.zenozencovich@uniroma3.it

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_9

hoeren@uni-muenster.de

(Transfer of PNR to the US[1]; Google Spain[2]; Schrems[3]; PNR agreement with Canada[4]).

This is also the result of the "constitutionalisation" of data protection which is expressly affirmed by Articles 7 and 8 of the European Charter of Fundamental Rights which has the same value as the two Lisbon Treaties (Treaty on the European Union and Treaty on the Functioning of the European Union).

In May 2018 the General Data Protection Regulation (2016/679)[5] has entered fully into force, together with Directives 680[6] and 681[7] concerning processing of personal data for contrast of terrorist and serious criminal activities.

[1]CJEU 30 May 2006 in joint Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union* which annuls Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, and Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection.

[2]CJEU 13 May 2014 in Case C-131/12, *Google Spain v. Costeja* holding that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

[3]CJEU 6 October 2015 in Case C-362/14, *Schrems v. Data Protection Commissioner (Ireland)* holding that the Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

[4]CJEU 26 July 2017, Opinion in Case 1/15 setting stringent conditions for the compatibility of the Draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data from the European Union to Canada with Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union.

[5]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). For some of the many Italian Commentaries on the GDPR, see: Bravo (2018); Califano and Colapietro (2018); De Franceschi (2017); Di Resta (2018); Finocchiaro (2017); Pizzetti (2016); Riccio et al. (2018).

[6]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[7]Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

hoeren@uni-muenster.de

In the pipeline is the Draft regulation on data protection on the internet.[8]

As for Italy, after the first data protection law (n. 675 of 1996) since 2003 it has enacted a lengthy 186 article long "Privacy Code" (Legislative Decree 2003/196) to which are attached over fifteen equally long schedules which discipline data protection in various areas (workplace, genetic data, historical and research purposes, associations, news gathering *et cetera*).

Since 1997, when the Italian Data Protection Commissioner (*Garante per la Protezione dei Dati Personali*) was created, thousands of decisions have been taken on the basis of individual requests or *ex officio* procedures.

A certain number of these decisions have been appealed in front of the courts. One can therefore rely also on a significant body of case law even from the Italian Court of Cassation.

The role of Italian practices in the formation of EU data protection cannot be underestimated. Professor Stefano Rodotà, the first Italian data protection Commissioner was the drafter of Article 7 the ECFR. Giovanni Buttarelli, for 10 years the Secretary general of the Italian *Garante*, was until 2019 the European Data Protection Supervisor. Many of the issues tacked with by the Article 29 [of Directive 1995/46] Working Group were set by the Italian *Garante* which has been regularly liaising with other European Commissioners.

2 Specific Features and Differences of the Italian Data Protection

The normative system of data protection is—on its black-letter—mostly harmonized, and it is uselessly pointillistic to detect minor changes in the words used.

What changed is the general legal, ideological, social and economic context in which such norms are immersed and with which they interact. One therefore has to look more outside data protection laws to compare systems and understand the differences between them.

Only "data protection radicals" see data protection as the sun around which all the other legal institutions revolve. A more realistic approach brings us to consider how, owing to external factors, same-worded rules may be applied differently in nearby jurisdictions within the European Union.

One further premise is necessary: practically all activities that fall under data protection regulations not only are digitalized, but also are put into place on telecommunication networks, the most important being the internet. One can therefore say that data protection is and must be, necessarily, on the internet. One

[8]Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final—2017/03 (COD).

hoeren@uni-muenster.de

therefore notices that rules and decisions issued in the pre-internet age are now adapted to the new environment.

2.1 Data Protection As a Personality Right

Even before data protection laws were enacted, the right to data protection has been qualified as a personality right (such as reputation, image, or name). In particular both the first data protection law (n. 695/96) and the Privacy code have connected data protection to the right to privacy and to personal identity.

This approach is generally followed by the courts (see for one of the first decisions *Cassazione* 30 June 2001, n. 8889[9]) and by legal doctrine. This implies that data protection is generally qualified as a fundamental right protected under Article 2 of the Italian Constitution (see *Cassazione* 19 July 2016, n. 14694[10]) and is of a non-patrimonial nature.

This qualification is relevant for what will be said further on under Sect. 2.6.

2.2 Countervailing Interests: Data Retention for Police and Judicial Investigations

There has always been an open conflict between the Italian *Garante* and Parliament and Government as to the maximum time for data retention for police and judicial investigations. The reasons are related to the strong need to contrast criminal organizations which are deeply rooted in certain regions (the Mafia and similar organized crime).

The Privacy Code (article 132) sets a rather short period for data retention of data concerning telephone traffic (2 years) and of computer traffic (1 year). However, these deadlines have constantly been prolonged up to 6 years for the needs of police and criminal investigations. At any rate the discussion on the actual length of data retention in Italy appears to be belittled by the sweeping powers given to police and judicial authorities to analyse and match all sort of data in order to contrast terrorist and serious crimes suspects (Directives 680 and 681/2016).[11]

[9]Published, *inter alia*, in Il diritto dell'informazione e dell'informatica (2001), p. 710; Giustizia civile (2002) I, p. 437; Foro italiano (2001) I, c. 1299 (with notes by Palmieri, Pardolesi and Granieri).

[10]Published in Guida al diritto (2016), pp. 43, 66.

[11]See above fn. 6 and 7.

hoeren@uni-muenster.de

2.3 Countervailing Interests: Rights of Workers

Since 1970 Italy has enacted stringent rules on surveillance of workers while at work. At that time the main concern was video-surveillance in factories and offices. Digital equipment was unknown. The Article 4 of the "Statuto dei lavoratori"[12] states that such a form of remote control can be introduced only for organizational reasons, and to protect safety of workers and of working premises. Such devices can be introduced after negotiation with the trade unions.

It is clear that such a regulation makes little sense in a digitalized context, in which workers are constantly connected with their employer's platform on which they perform many of their tasks.

The *Garante* attempted to discipline the processing of sensitive data (i.e. data which require a specific written authorization by the interested person) through specific guidelines issued in 2006 and still in force.[13]

However, the most controversial area has been, and still is, that of the use of data stored by the employer as evidence of the workers violation or his or her duties, such as to justify the termination of contract.

The main elements one can extract from the rich case law are related to the right for the employer to inspect the e-mails sent or received by the employee on the firm's e-mail account (in favour *Cassazione* 23 February 2012, n. 2722[14]).

Such activity of data processing has been considered lawful when put into place by the employer for the protection in court of rights which have been challenged (*Cassazione* 11 July 2013, n. 17204[15]).

2.4 Countervailing Interests: Media Reporting

The main area of conflict that has arisen over the last 20 years is between data protection—mostly seen in its privacy aspect—and journalist activity.

The *Garante*, already in 1998, attempted to immunize the press from the application of data protection laws, especially under the requirement of consent of the interested person. This brought to a Code of self-regulation which actually has a binding nature, but in only one direction, in the sense that it is generally applied to

[12]Law 20 May 1970, n. 300.

[13]Deliberazione n.53 del 23 novembre 2006 "Line e guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati" (available at www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364939).

[14]Published in Foro italiano (2012) I, c. 1421; and in Rivista italiana di diritto del lavoro (2013) 1, II, p. 113.

[15]Published in Diritto e giustizia online 11 July 2013.

hoeren@uni-muenster.de

exclude liability of the media.[16] This has not prevented a great number of cases being brought in front of both the *Garante* and the courts.

The problem—from a strictly legal point of view—is that data protection has to be seen as one of the legal reactions against the growing invasion of the individual sphere by technologies and by enterprises. One needs to, constantly, set the balance between competing values and needs.

Although it may be said that, in general, the result is in favour of the media, which is mostly exonerated from complying with the numerous data protection regulations which vex all other enterprises, there are still areas in which the equilibrium is instable, although this can be decided only on a case-by-case approach.

The most significant cases have been decided by the *Garante* who, time by time, has forbidden the publication by the press of highly sensitive data, mostly concerning health conditions or sexual conduct (*e.g. Garante* decision 7 February 2002, n. 46079 on a person affected by Creutzfeldt-Jakob disease; *Garante* decision 13 November 2013, n.2749736 on persons allegedly involved in child prostitution investigation).

2.5 Countervailing Interests: Right to Be Forgotten

The right to be forgotten has been recognized—albeit not in a complete form—by the CJEU decision in the *Google Spain* case. It should be noted however that already in 2012 the Corte di Cassazione (decision 5 April 2012, n. 5525[17]) on the basis of data protection laws had stated that news archived in a journalistic database had to be updated with more recent information, if any; and that individuals had a right that news related to decades before should fall in oblivion.

The principle has been repeatedly affirmed in decisions by the *Garante*, who has ordered, as remedy, that of de-indexing the news so that it may not be ordinarily found through search engines.

2.6 Countervailing Interests: Transparency of Economic Activity

Following a European trend, both the *Garante* and the courts have recognized ample exceptions to data protection legislation when data is processed by public credit reporting agencies. In particular, it has been considered compliant with data protection principles both the availability of data concerning the bankruptcy of companies,

[16]Provvedimento del Garante del 29 luglio 1998 "Codice di deontologia relativo al trattamento dei dati personalinell'esercizio dell'attività giornalistica".

[17]Published in Il diritto dell'informazione e dell'informatica (2012), p. 452 (with note by Frosini at p. 911).

hoeren@uni-muenster.de

and the names of their managing directors (*Cassazione* 14 June 2017, n. 19761[18]) or concerning the creditworthiness of individuals who in the past had defaulted (*Cassazione* 25 January 2017, n. 1931[19]: the available remedy is removal of a name improperly inserted in database).

2.7 New Fields: "Data Consumers"

The dominant—both in case law and in legal doctrine—view that data protection is a non-patrimonial personality right, has overshadowed the very clear economic dimension of data-driven industries.

These aspects have been gradually emerging not through the *Garante*, but through decisions taken by the Italian Competition Authority (*Autorità Garante per la Concorrenza ed il Mercato*—AGCM) which is empowered also with consumer protection.

In the *Samsung* decision (PS10207 of 27 January 2017[20]) the AGCM fined Samsung €3M for unfair commercial practices consisting in omitting informing consumers that the special prices for the purchase of handsets included compulsory registration on the Samsung platform and provision of personal data for marketing purposes.

In the *WhatsApp I* case (CV154, 12 May 2017[21]) practically all the standard clauses in the WA general terms and conditions were struck down as unfair inasmuch they conferred unlimited rights to WA on user data. And in the *WhatsApp II* case (PS10601, 12 May 2017[22]) WA was fined €3M for having transferred without notice all the data concerning its users to its controlling company, Facebook.

The cases show an increasing relationship between data protection and consumer protection, which has a distinctive economic nature. Such a patrimonial approach is bound to increase with the recent Directive on contracts for the supply of digital content and digital services.[23] Such a Directive recognizes that in the digital world users enter in contracts with service providers paying, as valuable consideration, with their data.

This, however, creates a conflict between technological practices over the internet, where services are provided on the basis of data collecting devices (typically

[18]Published in Foro italiano (2017) I, 2989 (with note by Pardolesi). The case was decided after a referral to the CJEU (decision 9 March 2017 in Case C-398/15, *Manni v. Camera di Commercio Lecce*).

[19]Published in Responsabilità civile e previdenza (2017), p. 837 (with note by Foglia).

[20]Published on the AGCM https://www.agcm.it/component/joomdoc/allegati-news/PS10207_chiusura.pdf/download.html.

[21]Il diritto dell'informazione e dell'informatica (2017), p. 371 (with note by Giannone Codiglione).

[22]Il diritto dell'informazione e dell'informatica (2017), p. 390 (with note by Giannone Codiglione).

[23]Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

hoeren@uni-muenster.de

cookies), and the GDPR which requires that consent for data processing be given "freely", a term which many—such as the EU Data protection Supervisor—interpret as "without economic incentives".[24]

2.8 New Fields: Commodification of Data

There is a growing conflict (also in Italy) between data protection laws and contract law. The bone of contention is the conflicting notion of "consent" as expressed in data protection laws and in decisions by the Italian *Garante*[25] and "consent" as it has historically been developed in contractual theory. The former is construed in a very strict and formalistic way, significantly limiting the possibilities to use and transfer data legitimately collected. The latter sees data as a commodity that can be legitimately be transferred to third parties, normally on the basis of an adequate consideration represented by the services one receives when using on-line services.

This interpretative clash might lead to a "tragedy of the anti-commons" by which fragmentation of rights over data could determine a paralysis in their exploitation, particularly necessary in a "Big Data" environment.[26]

2.9 Damages

Directive 1995/46, and with it ensuing Italian legislation, establishes strict liability for unlawful protection, in the sense that the burden of proof of lawful treatment is upon the data holder. This has brought to considerable amount of litigation concerning not the existence of an unlawful treatment, generally considered in *res ipsa,* but on the liquidation of damages arising from the tortious act.

Flooded by trivial litigation, mostly raised in front of justices of the peace, the *Cassazione* (decision of 16 July 2014, n. 16133[27]) first set on the plaintiff the burden

[24]EDPS, Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, n. 4/2017, p. 9. See also EDPS, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the digital economy (2014), Brussels, p. 8ff. A much more firm position has been taken by the EU Article 29 Data Protection Working Part, Guidelines on consent under Regulation 2016/679 (28.11.2017–10.4.2018): "As data protection law is aiming at the protection of fundamental rights, an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service" (at para. 3.1.2).

[25]See Thobani S (2016) I requisiti del consenso al trattamento dei dati personali, Rimini.

[26]See Resta G, Zeno-Zencovich V (2018) Volontà e consenso nella fruizione dei servizi in rete, in Rivista trimestrale diritto e procedura civile, p. 351.

[27]Published in Foro italiano (2015) I, c. 120.

hoeren@uni-muenster.de

of proving actual damage suffered from the unlawful processing of data, and subsequently fined the plaintiff for frivolous litigation (*Cassazione* 8 February 2017, n. 3311: the complaint concerned ten unsolicited e-mails).[28]

It would therefore appear that the preferred remedies in the field of personal data are more of specific performance nature (injunctions, de-indexing, removal etc.) than of a compensatory nature.

References

Bravo F (2018) Il "diritto" a trattare dati personali nello svolgimento dell'attività economica. Cedam – Wolters Kluwer, Milan

Califano L, Colapietro C (eds) (2018) Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679. Editoriale Scientifica, Naples

De Franceschi A (2017) La circolazione dei dati personali tra privacy e contratto. ESI, Naples

Di Resta F (2018) La nuova 'Privacy europea': I principali adempimenti del regolamento UE 2016/679 e profili risarcitori. Giappichelli, Turin

Finocchiaro G (ed) (2017) Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali. Zanichelli, Bologna

Pizzetti F (2016) Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679. Giappichelli, Turin

Riccio GM, Scorza G, Belisario E (eds) (2018) GDPR e normativa privacy. Wolters-Kluwer, Alphen aan den Rijn

[28]Published in Diritto & Giustizia (2017) 9.2.2017 (with note by Valerio).

hoeren@uni-muenster.de

Data Protection in the Internet: Japanese National Report

Taro Komukai

1 Introduction

1.1 Purpose of This Report

This report provides an overview of the data protection system in Japan, as a national report for the "Data Protection in the Internet" session held at the Congress of the International Academy of Comparative Law in Fukuoka in 2018.[1]

The privacy and data protection system in Japan has been established by reference to systems of other countries, including the European Union (EU) and the United States. It has become, however, a thing of its own that reflects national circumstances and culture. Recently, there have been some rapid changes such as reform of the basic law on data protection, establishment of an independent supervisory authority, and agreement with the EU for mutual data circulation.

This national report's purpose is to show the current situation and characteristics of privacy and data protection in Japan. To contribute effective comparative analysis, it was created according to items presented by the general reporter.

[1]This report is also going to be published in "Japanese Reports for the 20th International Congress of Comparative Law (ICCLP Publications No.14)", International Center for Comparative Law and Politics, Graduate School of Law and Politics, the University of Tokyo, May 2019.

T. Komukai (✉)
Nihon University, College of Risk Management, Tokyo, Japan
e-mail: komukai.taro@nihon-u.ac.jp

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_10

hoeren@uni-muenster.de

1.2 Organization of This Report

The organization of this report is as follows:
Section 1: Introduction
Section 2: General Data Protection Framework in Japan
Section 3: Specific Problems Concerning Data Protection in the Internet
Section 4: International Dimension of Data Protection
Section 5: Conclusion

2 General Data Protection Framework in Japan

2.1 Applicable Rules

In Japan, the right to privacy is recognized as a fundamental right derived from the Constitution's general rule stated in Article 13, which establishes people's right to the pursuit of happiness.[2]

The fundamental law on personal data protection in Japan, the Act on the Protection of Personal Information (APPI), was enacted in 2003, and part of its stated purpose is "to protect an individual's rights and interests". Although the right to privacy is guaranteed by Article 13 of the Constitution and the protection of such a right could have been included in the purpose of the APPI, it is not clearly mentioned in the provisions because the scope of the right to privacy is still controversial in Japan.

The APPI establishes basic Japanese policy for data protection and imposes obligations on the enterprises that process personal data, defined in the act as "personal information handling business operators" (hereinafter "Business Operators"). As the APPI was amended in 2015 and the amended act entered into force in 2017, this report will be based on the provisions of the APPI as amended in 2015 unless otherwise noted.

As for the public sector, there are two other acts: the Act on the Protection of Personal Information Held by Administrative Organs, and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies.

The Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (the My Number Act) covers the handling of personal data related to individual numbers that are a type of national ID, known as "My Number". This number is allocated to each person and is processed for administrative procedures in

[2]Article 13 of the Constitution of Japan states the following: "All people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs." Source: The Ministry of Justice, Japanese Law Translation Database System, http://www.japaneselawtranslation.go.jp. Accessed 6 Nov 2018.

hoeren@uni-muenster.de

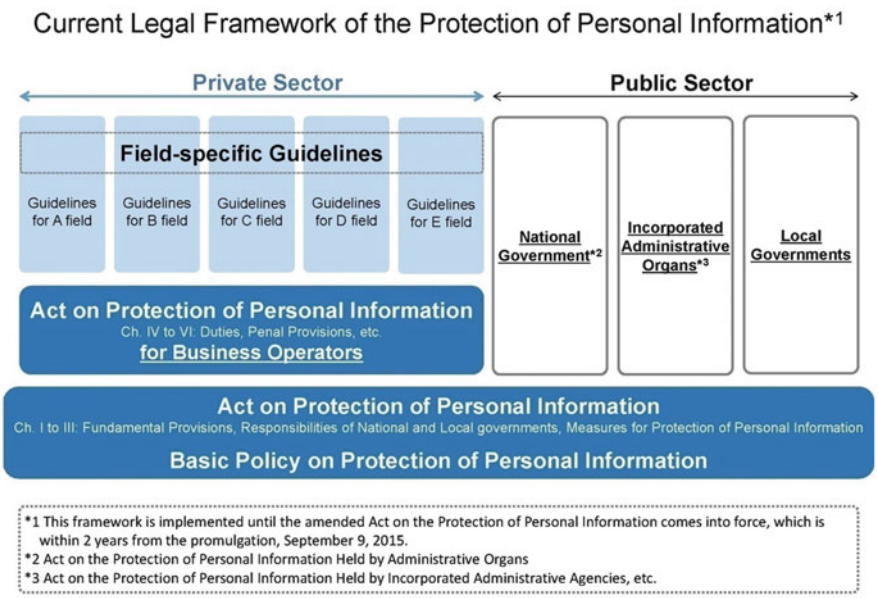

Fig. 1 Legal framework in Japan (Source: The Personal Information Protection Commission, "Current Legal Framework of the Protection of Personal Information", http://www.ppc.go.jp/en/legal/)

the fields of social security, tax, and disaster response. The My Number Act sets forth special protections for information associated with My Numbers.

Additionally, more than 2000 local governments and municipalities have their own ordinances for personal data protection.

Figure 1 illustrates the legal framework for personal data protection in Japan.

Regarding the leakage of personal data, there have been court decisions that permit tort liability claims against Business Operators for negligence in information management (see Sect. 3.5). The Supreme Court has ruled that "common information for personal identification" such as student ID numbers, addresses, names, telephone numbers, etc. is also "subject to legal protection and unauthorized disclosure could be illegal" (Waseda University case[3]).

2.2 Notion of Personal Data

Article 2 of the APPI classifies personal information into three main categories: (1) personal information (general information that can identify specific individuals);

[3]Saiko Saibansho [Sup. Ct.], Sep. 12, 2003, 1823 Hanji 3 (Japan).

hoeren@uni-muenster.de

(2) personal data (where data has been systematically organized to facilitate a search for particular personal information); and (3) retained personal data (personal data retained for more than 6 months).

The most comprehensive category of these is the "personal information" group, which defines personal information as information relating to a living individual containing (i) a name, date of birth, other descriptions, etc., whereby a specific individual can be identified (including that which can be readily collated with other information, thereby identifying a specific individual); or (ii) an individual identification code.[4]

When handling personal information in general, Business Operators must specify the purpose of the use (Article 15), confine the use to said purpose (Article 16), adhere to the appropriate method of gathering the personal information (Article 17), and provide notice or publication of the purpose of use (Article 18).

Regarding personal data, it is also necessary to ensure accurate and updated data (Article 19), the presence of safety control measures (Article 20), supervision of employees (Article 21), supervision of contractors (Article 22), and consent of the data principal in providing data to a third party.

When handling retained personal data, Business Operators shall make public their name or appellation, the purpose of use, the procedures for disclosure, etc. (Article 24), and they are obliged to respond to requests from the data principal regarding disclosure, correction, or suspension of use (Articles 25–27).

The 2015 amendment established two new categories: special care-required personal information and anonymously processed information.

Special care-required personal information means personal information that includes a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other description that is prescribed by cabinet order as information that requires special care so as not to inflict unfair discrimination, prejudice, or other disadvantages on the principal (Article 2(3)). Special care-required personal information shall not be acquired without obtaining the principal's consent in advance (Article 17).

[4] Article 2(1) states the following: "'Personal information' in this Act means information relating to a living individual that falls under any of the following items:

(i) information containing a name, date of birth, other description, etc. (meaning any and all matters – excluding an individual identification code – stated, recorded, or otherwise expressed using voice, movement, or other methods in a document, drawing, or electromagnetic record (meaning a record kept in an electronic, magnetic, or other form that cannot be recognized through the human senses; the same shall apply in the succeeding paragraph (ii) and in Article 18, Paragraph 2 (hereinafter "same")) whereby a specific individual can be identified (including that which can be readily collated with other information and thereby identify a specific individual); or

(ii) information containing an individual identification code."

Source: The PPC, Amended Act on the Protection of Personal Information (Tentative Translation), https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf. Accessed 6 Nov 2018.

hoeren@uni-muenster.de

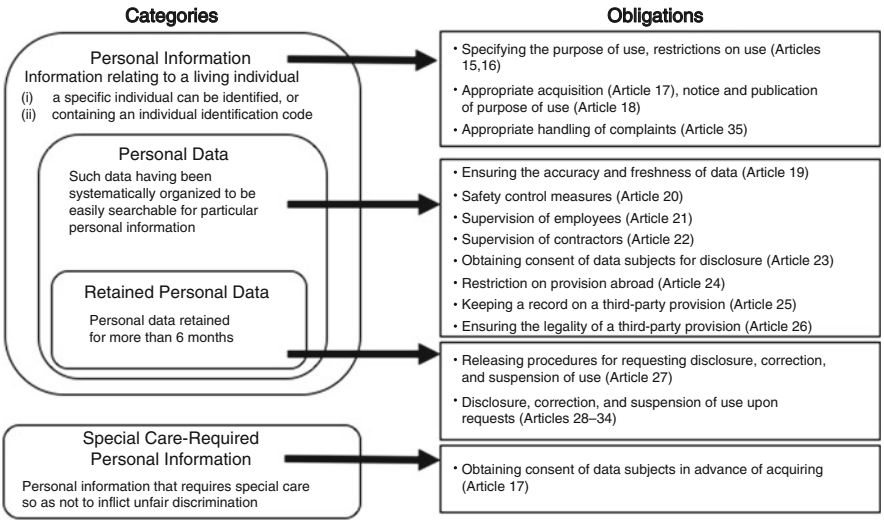

Fig. 2 Categories of personal information and associated obligations [Source: Komukai (2018)]

Anonymously processed information means information relating to an individual that can be produced from processing personal information, precludes the identification of a specific individual by taking proper actions as prescribed, and precludes the ability to restore the personal information (Article 2(9)). Operators are permitted to provide anonymously processed information to a third party without obtaining a principal's consent in advance as long as they comply with the procedure and obligations set forth in the APPI (Articles 36–39).

Figure 2 presents the categories and the obligations associated with each.

2.3 Supervisory Authority

In January of 2016, the Personal Information Protection Commission (PPC), an independent monitoring and supervising body responsible for the overall protection of personal information, was established.

The PPC is the general supervisory authority under the APPI. Before the PPC's authority was established in May 2017, the competent ministers of each industry to which Business Operators belonged had supervisory authority as regulatory bodies. Even though the PPC's authority has been established, it can still delegate reporting, hearing and on-site inspection authority to the business jurisdictional minister and the minister must then report the results to the PPC (Article 44).

The PPC has authority to supervise the handling of personal information under the APPI, information associated with numbers under the My Number Act, anonymously processed information handled by administrative organs, etc. The PPC does

hoeren@uni-muenster.de

not have general authority to enforce the Act on the Protection of Personal Information Held by Administrative Organs, the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, or the ordinances of local governments and municipalities.

2.4 Self-Regulation Instruments

To promote appropriate self-regulation for each industry and field of business, the PPC accredits private organizations based on Articles 47–58 of the APPI. Accredited personal information protection organizations are in charge of processing complaints concerning personal information and are expected to develop guidelines, take necessary measures, and make recommendations to ensure that operators within their self-regulation authority comply.

The PPC publicly announces the personal information protection guidelines submitted by the accredited personal information protection organizations and, if necessary, collects a report from or issues an order to organizations. 44 organizations have been accredited as of October 29, 2018.[5]

3 Specific Problems Concerning Data Protection in the Internet

3.1 Personal Data Processed by Electronic Means

Most of the "personal data" in the APPI are personal data processed by electronic means and subject to regulations for that category.

As for the telecommunications business, The Ministry of Internal Affairs and Communications (MIC), which supervises the telecommunications industry, publishes guidelines to help telecommunications carriers comply with the Telecommunications Business Law and the APPI.[6]

[5]PPC Webpage, Accredited Personal Information Protection Organizations, https://www.ppc.go.jp/. Accessed 6 Nov 2018.

[6]The PPC supervises the processing of personal information in general under the APPI and in the context of electronic communications, as well. The MIC supervises the processing of information handled by telecommunication carriers, especially those associated with confidential information protected by secrecy of communications under the Telecommunications Business Law.

hoeren@uni-muenster.de

Table 1 Spam e-mail regulations in Japan

	Act on Regulation of Transmission of Specified Electronic Mail	Act on Specified Commercial Transactions
Objects of the regulation	E-mails sent as a means of advertisement	E-mails that advertise mail order sales
Obligations	• Opt-in (Article 3) • Obligation of senders' information labeling (Article 4) • Prohibition of transmission using fictitious electronic mail address (Article 5) • Prohibition of transmission under false sender information (Article 6) • Refusal of provision of telecommunications services (Article 11)	• Opt-in (Article 12-3(1)) • Prohibition of transmission to persons who refuse to receive e-mails that advertise mail order sales (Article 12-3(2)) • Obligation to make record of opt-in participants (Article 12-3(3)) • Obligation of senders' information labeling (Article 12-3(4))

3.1.1 Processing of Personal Data in the Context of Services Provided at a Distance by Electronic Means

Two laws were introduced in 2002 that regulate spam e-mail: the Act on Regulation of Transmission of Specified Electronic Mail (regulating e-mails sent as a means of advertisement), and the amended Act on Specified Commercial Transactions (regulating mail order businesses).

The Act on Regulation of Transmission of Specified Electronic Mail and the Act on Specified Commercial Transactions provide for an opt-in system. An opt-out system was adopted at the time of their introduction in 2002, but as the transmission of spam e-mails increased, an opt-in system was introduced in the 2008 revisions, which also include stronger enforcement provisions and penalties.

To protect spam e-mail recipients, the two acts provide regulations as shown in Table 1.

3.1.2 Protection of Minors' Personal Data Processed by Electronic Means

There are no special protections for the personal information of minors. The Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People was enacted on June 11, 2008, and the act aims to encourage the voluntary efforts of related industries to prevent young people under the age of 18 from coming into contact with harmful information.

hoeren@uni-muenster.de

3.1.3 Right to the Erasure of Personal Data Processed by Electronic Means

There are no statutory laws or guidelines regulating the "right to erasure" or the "right to be forgotten" in Japan; however, there have been some court cases in which search engines have sought to eliminate search results related to past information because of privacy infringement, defamation, etc. In some cases, even facts published legitimately in the past were considered to infringe on privacy or be grounds for defamation for specific reasons.

The Supreme Court held that a search service provider is obligated to delete search results only in the event that the legal interests realized by deleting are clearly superior to the legal interests of providing the search results, and the social importance of the search engine in the internet era should also be considered when comparing the legal interests.[7]

3.1.4 Protection of Employees' Personal Data Processed by Electronic Means

There is no statute or other law stipulating special regulations concerning the personal information of employees. There are two cases where the Tokyo District Court held that monitoring employees' e-mails is inevitable for companies, to a certain extent, in particular situations.[8]

Regarding the monitoring of employees to supervise workers and regarding trustees who handle personal data as part of other security control measures, the guidelines of the Ministry of Health, Labour, and Welfare (MHLW) and the Ministry of Economy, Trade, and Industry (MITI) require strict compliance with the specification of the purpose of monitoring, expressly informing workers of it, stipulating the purpose in the in-house regulations in advance, etc.[9]

There are no statutes or court decisions that provide guidelines on the private use of electronic means by employees. Regarding the private use of social media by state public officials, the MIC issued focus points on June 28, 2013.[10]

[7]Saiko Saibansho [Sup. Ct.], January 31, 2017, 2328 Hanji 10 (Japan).

[8]Tokyo Chiho Saibansho [Tokyo Dist. Ct.], Dec. 3, 2001, 826 Roudo Hanrei 76 (Japan); Tokyo Chiho Saibansho [Tokyo Dist. Ct.], Feb. 26, 2002, 825 Roudo Hanrei 50 (Japan).

[9]The Ministry of Health, Labour, and Welfare and Ministry of Economy, Trade, and Industry, Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information, Announcement No. 2 of October 9, 2009 (Tentative Translation), http://www.meti.go.jp/policy/it_policy/privacy/0910english.pdf. Accessed 6 Nov 2018.

[10]The MIC, Focus Points Regarding the Private Use of Social Media by State Public Officials, http://www.soumu.go.jp/menu_news/s-news/01jinji02_02000084.html. Accessed 6 Nov 2018.

hoeren@uni-muenster.de

3.1.5 Security Obligations and Data Breach Notifications Concerning Data Processed by Electronic Means

The APPI requires Business Operators to take appropriate safety control measures, supervise their employees (Article 21), and supervise contractors (Article 22) when they handle "personal data".

The Telecommunications Business Law obligates telecommunications facilities to comply with the technical standards stipulated in "Section 4 of Telecommunications Facilities". However, the law aims to ensure the security of the entire telecommunications business in general rather than the protection of personal information specifically.

There is no provision that requires data breach notifications in the APPI. The "Policies Concerning the Protection of Personal Information" set forth by the Japanese Cabinet in 2004 "in accordance with" the APPI state "in the case of incidents such as data leakage, it is important for business operators handling personal information to disclose information about the incident to the extent possible in order to prevent secondary damage or similar cases". Many business operators have disclosed information regarding data leaks in accordance with this policy. Additionally, in 2017, the PPC announced guidelines[11] recommending that operators report immediately to the responsible person and take necessary measures to prevent expansion of the damage caused by the leakage.

As for the My Numbers, Article 29(4) of the My Number Act obligates relevant institutions (primarily governmental agencies) to report data breaches to the PPC.

3.2 Data Protection in the Electronic Communications Sector

The Telecommunications Business Law stipulates special protections concerning "confidential communications handled by telecommunications carriers".[12]

Confidential aspects of communications include information such as their sender, where and when they were communicated, etc., as well as their contents (Cabinet Legislation Bureau, Issue No. 24, Dec. 9, 1963). Traffic data held by telecommunications carriers and the source and destination network addresses in the packet headers on packet communication systems they transmit are also protected as confidential information associated with communications.

[11]The PPC, Guidance for Responding to Cases Such as Personal Data Leaks, etc., (Announcement No. 1 of 2017 by the Personal Information Protection Committee), https://www.ppc.go.jp/personal/legal. Accessed 6 Nov 2018.

[12]Provisions concerning confidential information protected by secrecy of communications are set forth in the Constitution of Japan (Article 21(2)), the Telecommunications Business Act (Article 4 and Article 179), the Radio Law (Article 109 and Article 109(2)), and the Cable Telecommunications Act (Articles 9 and 14).

hoeren@uni-muenster.de

Telecommunications businesses that are subject to this regulation must be in "the business of providing telecommunications services in order to meet the demands of others", and telecommunications service is defined as "intermediating the communications of others through the use of telecommunications facilities or any other acts of providing telecommunications facilities for the use of communications by others"[13] (Article 2). The MIC considers businesses on the internet such as closed chats, dating sites, e-mail operation hosts, and e-mail hosts using foreign servers, etc. as telecommunications carriers. As for comprehensive services such as "portal sites" or "SNS's" (Social Networking Sites), which include various sites, the MIC must review their concrete specifications to determine whether or not they are telecommunication carriers.[14]

Telecommunications carriers are not permitted to use information that includes confidential information protected by secrecy of communications unless the consent of the user is obtained or there is other justification such as self-defense, necessity, or legitimate operations to maintain a stable network. Thus, they are not permitted to conduct constant monitoring of the route of network packets to detect attacks. Because the importance of cyber defense is increasing, the MIC has been trying to define cases in which telecommunications carriers can legally use information that includes confidential information protected by secrecy of communications in its guidelines. Even for criminal investigations, authorities are required to obtain an interception warrant, a seizure warrant, or to submit to other statutory procedures before acquiring information that includes confidential information protected by secrecy of communications.

The Telecommunications Business Law obligates telecommunications carriers to report without delay to the Minister for Internal Affairs and Communications, and includes the reason or cause when a violation regarding confidential information protected by secrecy of communications has occurred with respect to telecommunications activities (Article 28).

The Minister for Internal Affairs and Communications may order the improvement of business activities if there are obstacles to ensuring the confidentiality of communications with respect to the methods telecommunications carriers use to conduct business activities (Article 29 of the Telecommunications Business Law). Those who violate such an order shall be punished by a fine of not more than 2 million yen (Article 186).

Moreover, information handled by telecommunications carriers is generally required to be highly protected even if it is not considered a confidential communication.

[13]The MIC, Telecommunications Business Act (Translation by the MIC), http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_2.pdf. Accessed 6 Nov 2018.

[14]The MIC, Manual on Entry into Telecommunications Business [Supplementary Edition] - Concept and Case Study on Necessity of Notification, etc. (August 18, 2005), http://www.soumu.go.jp/main_content/000477428.pdf. Accessed 6 Nov 2018.

hoeren@uni-muenster.de

The MIC provides guidelines[15] that require telecommunications carriers to make efforts to restrict the collection of personal information as much as possible to when it is necessary to provide communication services (Article 6) and to limit the purpose of use so as not to exceed the necessary range of providing telecommunication services (Article 4(3)). The guidelines also require telecommunications carriers to carefully handle some types of information such as communication records, itemized billing, caller identification, location data, non-payment user information, subscriber information related to spam mail, and telephone numbers.

3.3 Data Protection and Digital Forensics

Although the APPI calls for an individual's consent to provide personal data to a third party, it may also be provided in cases defined as exceptions in the applicable laws and regulations (Article 23). Therefore, investigation authorities can access personal data in general based on a search warrant (Article 218 of the Code of Criminal Procedure) and investigation-related inquiries (Article 197 of the Code of Criminal Procedure).

To acquire information that includes confidential communications, it is indispensable for investigation authorities to obtain a communications interception warrant (Article 3 of the Act on Wiretapping for Criminal Investigations), a search warrant (Article 218 of the Code of Criminal Procedure), or to follow other statutory procedures. Regarding the geographic location data processed by mobile carriers, a search warrant is required as well (MIC Guideline 35-1).

The Code of Criminal Procedure sets forth procedures for investigating authorities to access records on a cloud server used by a seized computer by copying the record to the seized computer or other recording medium (Article 218(2)).

A warrant shall contain the scope of the information to be copied from the electromagnetic records with regard to the recording medium connected via telecommunication lines to the computer that is to be seized.

Interception in the above-referenced act is defined as receiving communications that are currently being exchanged between parties without notice in order to know their contents.

Investigation authorities may request in writing that the electronic communications operator refrain from deleting the communications record. In such a case, investigation authorities must specify the necessary record and period of time, not to exceed 30 days (Article 197(3) of the Code of Criminal Procedure). The period may be extended up to 60 days (Article 197(4)).

[15]The MIC, "Guidelines for the Protection of Personal Information Handled by Telecommunications Businesses". (April 18, 2017), http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html. Accessed 6 Nov 2018.

hoeren@uni-muenster.de

Investigation authorities may request to retain communications records including origination and destination, date and time, and other history of transmission information (Article 197(3)).

The request is not restricted to a particular charged offense. A public prosecutor, a public prosecutor's assistant officer, or a judicial police officer may request retention when they deem it necessary to execute a seizure.

According to the exclusionary rule or the fruit of the poisonous tree theory, data cannot be used as evidence in a trial when it is deemed to be illegally collected evidence.

3.4 Data Protection and Electronic Surveillance for Security and Defense Purposes

The Act on Wiretapping for Criminal Investigations stipulates the procedures concerning the interception of communications made by investigation authorities.

As for tracing by installing a GPS device to a suspect's car without notice, the Supreme Court held that such an investigation must be conducted under legitimate, statutory procedures and new legislation is necessary.[16]

There is no legislation addressing the processing of personal information for national security or defense purposes. Although Article 23 of the APPI requires operators to obtain a principal's consent in advance before providing personal data to a third party, operators are permitted to provide such information in a case "based on law and regulations" or "in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent". Therefore, if the processing satisfies one of these conditions, information can be acquired even without the consent of the principal.

3.5 Remedies and Sanctions

The PPC has the authority to require reports, make onsite inspections (Article 40), provide guidance, give advice (Article 41), make recommendations, and issue orders (Article 42) to the Business Operators. There are punishment provisions for not complying with an order of the PPC (Article 84), making false statements, or for a lack of reporting (Article 85). When an employee commits a violative act in relation to the business of a corporate body, a fine will be imposed on both the employee and the corporate body (Article 87).

Damages for data leakage are claimed based on tort law as set forth in the Civil Code. Article 709 stipulates that "a person who has intentionally or negligently infringed upon any right of others or legally protected interest of others shall be

[16]Saiko Saibansho [Sup. Ct.], March 15, 2017, 2333 Hanji 4 (Japan).

hoeren@uni-muenster.de

Table 2 Court decisions on personal data protection in Japan

Data Controller	Cases	Compensation (yen/plaintiff)
The City of Uji[a]	Negligence in data security which caused data theft, including information from the Basic Resident Registrar by a part-time worker of a contractor	15,000
Waseda University[b]	Providing a list of 1400 student participants of an event to the Tokyo Metropolitan Police Department for security purposes without consent	5000
Yahoo! BB[c]	Negligence in data security which caused customer data theft by a former employee and his acquaintance illegally accessing a server	6000
Tokyo Beauty Center (TBC)[d]	Negligence in data security for questionnaire and response data stored without access control on a web server	22,000

[a]Osaka Koto Saibansho [Osaka High. Ct.], Dec. 25, 2001, 265 Hanrei Chihoujichi 11 (Japan); Saiko Saibansho [Sup. Ct.], Jul. 11, 2002, 265 Hanrei Chihoujichi 11 (Japan)
[b]Saiko Saibansho [Sup. Ct.], Sep. 12, 2003, 1823 Hanji 3 (Japan)
[c]Osaka Chiho Saibansho [Osaka Dist. Ct.], May 19, 2006, 1948 Hanji 122 (Japan); Osaka Koto Saibansho [Osaka High. Ct.], Jun. 21, 2007, Unpublished (Japan)
[d]Tokyo Koto Saibansho [Tokyo High. Ct.], Aug. 28, 2007, Unpublished (Japan)

liable to compensate for damages resulting in consequence". As for mental or psychological harm, one can make a claim for compensation under Article 710. Additionally, those who employ others for a certain business shall be liable for damages inflicted on a third party by their employees with respect to the execution of said business based on Article 715. Table 2 presents information on a few court decisions regarding data leakage.

Violations of the handling of confidential information protected by secrecy of communications by a telecommunications carrier are subject to imprisonment with work of not more than 2 years or a fine of not more than 1 million yen. If a person engaging in a telecommunications business violates the provisions of confidential information protected by secrecy of communications, he or she shall be punished by imprisonment with work of not more than 3 years or a fine of not more than 2 million yen (Article 179 of the Telecommunications Business Act).

Under the Act on Regulation of Transmission of Specified Electronic Mail, the Minister for Internal Affairs and Communications may order senders of advertisements or promotional mail to take appropriate action when it is necessary to prevent disturbances in the transmission and reception of electronic mail (Article 7). A violation of such order and the prohibition of transmission under false sender information are subject to imprisonment with work for a term not exceeding 1 year or a fine not exceeding 1 million yen (Article 34). Additionally, when an employee is acting within the scope of the business of a corporation, a fine not exceeding 30 million yen will also be imposed on the corporation (Article 37).

As for the Act on Specified Commercial Transactions, violations of the opt-in rule, the prohibition of transmissions to persons who refuse to receive e-mails that advertise mail order sales, and obligations to make a record of opt-in participants are

hoeren@uni-muenster.de

subject to a fine not exceeding 1 million yen (Article 72(1)(4)). Violations of senders' information labeling or fraudulent advertising is subject to imprisonment with work for a term not exceeding 1 year or a fine not exceeding 2 million yen (Article 72(2)). The above-referenced violations are also subject to an order for the suspension of business by competent ministers (Article 15).

4 International Dimension of Data Protection

4.1 Territorial Scope of Rules on Data Protection

In principle, the APPI and other rules apply to personal information handled inside the jurisdiction of Japan.

4.2 Applicability of Data Protection Rules to Foreign Entities

The provisions of the APPI that set forth the obligations of a business operator handling personal information shall also apply to operators who acquire the personal information of a person in Japan in relation to supplying that person goods or services and handle the personal information in a foreign country (Article 75 of the APPI[17]).

4.3 Specific Conditions Applicable to the Transfer of Personal Data to a Foreign Jurisdiction

A personal information handling business operator shall, in the case of providing personal data to a third party in a foreign country, in advance, obtain a principal's consent to the effect that he or she approves of the provision of the information to a third party in a foreign country with the exception of the following: (1) to a third party establishing a system conforming to the standards prescribed by the rules of the

[17] Article 75 states: "The provisions of Article 15, Article 16, Article 18 (excluding paragraph (2)), Article 19 through Article 25, Article 27 thorough Article 36, Article 41, Article 42, paragraph (1), Article 43 and the following Article shall also apply in those cases where a personal information handling business operator who in relation to supplying a good or service to a person in Japan has acquired personal information relating to the person as a principal who handles in a foreign country the personal information or anonymously processed information produced by using the said personal information." Source: The PPC, Amended Act on the Protection of Personal Information (Tentative Translation), https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf. Accessed 6 Nov 2018.

hoeren@uni-muenster.de

PPC as necessary for continuously taking action as required by the APPI; (2) to a third party in a foreign country where a personal information protection system is established and recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests in accordance with the rules of the PPC; or (3) in cases where it falls under the exception rule of prohibiting the provision of such information to third parties (Article 23).

As for the relationship with the EU, agreement to recognize each other's personal data protection systems as equivalent was made in July of 2018. Completion of the relevant internal procedures required for this framework for mutual and smooth data transfers between Japan and the EU is scheduled to become operational by autumn 2018.[18]

4.4 Applicable Law for Liability of Damages Caused by the Unlawful Processing of Personal Data

As for tort liability, the law of the place where the damage occurred is generally applicable. If damage such as privacy infringement occurs in Japan, the Japanese law on tort liability will be applied (Article 17 of the General Law on the Application of a Law[19]).

5 Conclusion

5.1 Data Protection in Japan

Four points are thought of as important in the data protection system in Japan.

First, although the right to privacy is recognized as a fundamental right derived from the Constitution's general rule in Japan, whether data protection is required as a constitutional right is controversial, and it does not explicitly appear in the purpose stated in the APPI.

Second, the structure of the data protection system is rather complex with several pieces of legislation such as the APPI, acts for the public sector, and many ordinances.

[18]Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Tokyo, 17 July 2018, https://www.ppc.go.jp/files/pdf/300717_pressstatement2.pdf. Accessed 6 Nov 2018.

[19]Article 17 states: "The formation and effect of a claim arising from a tort shall be governed by the law of the place where the result of the wrongful act occurred; provided, however, that if the occurrence of the result at said place was ordinarily unforeseeable, the law of the place where the wrongful act was committed shall govern." Source: The Ministry of Justice, Japanese Law Translation Database System, http://www.japaneselawtranslation.go.jp. Accessed 6 Nov 2018.

hoeren@uni-muenster.de

Third, while the APPI requires Business Operators to identify and publish the purpose of use, it does not stipulate the principal's consent or justification, such as legitimate interest in general. However, in the case of handling special care-required personal information, providing personal data to a third party, or changing the purpose of use, Business Operators need to obtain pre-existing principal's consent and they are not allowed to justify it with legitimate interest.

Fourth, protection of the secrecy of communications has a wide range of application and strict restriction in comparison with other countries. The broad base of information, which includes not only content of communications but also metadata such as traffic and location data processed by a wide range of businesses on the internet, is subject to restriction of use.

5.2 Data Protection in the Internet

Emerging computing technologies using the internet have brought various concerns associated with data protection. Development of big data, IoT and AI technologies make it more difficult to assure control by principals or data subjects. Regulations such as data portability, right to erasure, right to be forgotten, as well as profiling regulation in the EU's General Data Protection Regulation (GDPR) were proposed in response to the situation brought by new technologies.

When thinking about introducing such regulations into Japan, it is important to consider the difference in approach between the EU and Japan in reflecting the will of data subjects. While regulation in the EU is straightforward in strengthening control by data subjects on all kinds of data, the Japanese system varies depending on the data's nature. For example, while regulations in Japan do not require a principal's consent to collect and use personal information in general, they do require explicit consent in advance for some situations such as providing to third parties or using secret communications including metadata.

Needless to say, the Japanese legal system for data protection also faces difficulties in reflecting the will of data subjects under the situation caused by emerging new technologies, and it is important to catch up and reduce the risk of such change, balancing the Japan-specific background of regulation and international harmonization.

References

Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Tokyo, 17 July 2018. https://www.ppc.go.jp/files/pdf/300717_pressstatement2.pdf. Accessed 6 Nov 2018

Komukai T (2018) Introduction to informational law: law on digital network, 4th edn. NTT Publishing, Tokyo

hoeren@uni-muenster.de

The MIC (2005) Manual on entry into telecommunications business [supplementary edition] - concept and case study on necessity of notification, etc. (August 18, 2005). http://www.soumu.go.jp/main_content/000477428.pdf. Accessed 6 Nov 2018

The MIC. Focus points regarding the private use of social media by state public officials. http://www.soumu.go.jp/menu_news/s-news/01jinji02_02000084.html. Accessed 6 Nov 2018

The MIC. Telecommunications Business Act (translation by the MIC). http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_2.pdf. Accessed 6 Nov 2018

The Ministry of Health, Labour, and Welfare and Ministry of Economy, Trade, and Industry, Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information, Announcement No. 2 of October 9, 2009 (Tentative Translation). http://www.meti.go.jp/policy/it_policy/privacy/0910english.pdf. Accessed 6 Nov 2018

The Ministry of Justice, Japanese Law Translation Database System. http://www.japaneselawtranslation.go.jp. Accessed 6 Nov 2018

The PPC. Guidance for responding to cases such as personal data leaks, etc., (Announcement No. 1 of 2017 by the Personal Information Protection Committee). https://www.ppc.go.jp/personal/legal. Accessed 6 Nov 2018

The PPC. Amended Act on the Protection of Personal Information (Tentative Translation). https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf. Accessed 6 Nov 2018

hoeren@uni-muenster.de

Data Protection in the Internet: The Portuguese Case

Alexandre Sousa Pinheiro

1 General Data Protection Framework

In Portugal, the relevant laws applicable regarding data protection matters are:

(i) Law no. 41/2004, of 18 August 2004 (transposing the Directive 2002/58/CE) with the amendments introduced by Law no. 32/2008, of 17 July 2008 (transposing Directive 2006/24/CE) and Law no. 46/2012 (transposing Directive 2009/136/CE).
(ii) Law no. 58/2019, of 8 August 2019, which ensures the implementation, in the national legal system, of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR).
(iii) Law no. 59/2019, of 8 August 2019, which approves rules on the processing of personal data for the purpose of prevention, detection, investigation or prosecution of criminal offenses or the enforcement of criminal sanctions, and transposes Directive (EU) 2016/680.

Personal data are protected in Portugal as a specific right by the Portuguese Constitution since 1976 (Article 35).[1]

The protection of personal data is required by the Constitution (Article 35/2), and is regulated by Law no. 58/2019, of 8 August 2019. This Law is applicable to data processing undertaken in national territory, as well as to that undertaken abroad whenever: (1) it is undertaken within the activity of an entity established in Portugal;

[1]For an overview on this topic, see Pinheiro (2015).

A. S. Pinheiro (✉)
University of Lisbon, Faculty of Law, Lisboa, Portugal
e-mail: josepinheiro@fd.ulisboa.pt

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_11

hoeren@uni-muenster.de

or (2) it affects data holders located in Portugal and such data processing is covered by Article 3 (2) of GDPR[2]; or (3) it affects data registered in Portuguese consulates, the holders of which are Portuguese citizens residing abroad (Article 2).

In the field of electronic communications Law no. 41/2004 is applicable. According to Article 2, the scope of this law covers the processing of personal data within the context of public communications networks. The purpose of the law is to specify the domestic rules on data protection in respect of electronic communications (Article 1/2).

The providers of electronic communications must notify the Portuguese Data Protection Authority, without further delay, of the occurrence of any events that may affect the security of personal data (Article 3-A).

Article 35/2 of the Constitution states that an independent administrative entity must be created to guarantee the protection of personal data.

The Portuguese Data Protection Authority, the *Comissão Nacional de Proteção de Dados*—CNPD (National Data Protection Commission), is defined by Law no. 58/2019 as an independent administrative entity endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, in order to protect human rights and the fundamental freedoms and guarantees of individuals in the area of personal data treatment (Article 4/1).

As a consequence thereof, in matters of data protection there is only one supervisory body in Portugal—the CNPD.

Article 6 of Law no. 58/2019 designates the CNPD as the national supervisory authority for the purposes of article 57 of the GDPR.

The CNPD is further entrusted with the following assignments: (1) to issue non-binding opinions on legislative and regulatory measures on data protection, as well as on legal instruments under preparation in European and International institutions on the same matters; (2) to monitor compliance with the GDPR and other legislative and regulatory provisions on data protection; (3) to make available a list of processing operations which are subject, pursuant to Article 35 (4) of the GDPR, to an impact assessment; (4) to draw up and submit to the European Data Protection Board a draft of requirements for the accreditation of monitoring bodies pursuant to Articles 41 and 43 of the GDPR; (5) to cooperate with the Portuguese Accreditation Institute (IPAC). (Article 6 (1) of the Law).

The CNPD also exercises the powers foreseen in Article 38 of the GDPR (Article 6 (2) of the Law).

Article 15 (1) provides that the CNPD shall encourage the drawing up of codes of conduct concerning specific activities. The Portuguese Association of Direct Marketing approved in 2003 a Code of Conduct applicable in matters of personal data processing, based on a previous opinion approved by the Portuguese DPA.[3] According to the said code, companies are required to erase personal data collected

[2]On which see, in Portuguese, Pinheiro et al. (2018).

[3]http://www.amd.pt/codigoconduta.pdf.

hoeren@uni-muenster.de

in the context of sales and promotions when this required by costumers (right of opposition). Companies should keep an updated a list of costumers who oppose to direct marketing activities.

As a result of the described legal framework, personal data processing is generally governed by the GDPR in Portugal. Law no. 58/2019 has, however, set out some specific provisions in this respect, which seek to complement the provisions of that EU Regulation. These include the following: (1) Minors' consent for the processing of personal data is only lawful when they have at least 13 years of age (Article 16); (2) Personal data of deceased persons is also subject to protection (Article 17); (3) Portability of data as provided for in Article 20 at the GDPR only comprises data provided by their holders (Article 18); (4) Video-surveillance may not take place in certain areas, such as public roads, ATM digitization zones or reserved areas in which the privacy of users should by respected (Article 19); (5) Employers may process data of employees for the purposes provided for in the Labour Code, the employee's consent not being required insofar as the processing results in a legal or economic advantage for him or is covered by Article 6 (1) (b) of the GDPR (Article 28); (6) The processing of health and genetic data is governed by the "need to know" principle (Article 29); and (7) Any person who has suffered damage due to the unlawful processing of data or any other act in breach of the GDPR or national Law on data protection is entitled to compensation from the controller or processor of such data, unless they demonstrate that the fact that has caused the damage is not attributable to them (Article 33).

Some of the provisions of Law no. 58/2019 triggered a heated debate and met with opposition from the Portuguese supervisory body, the CNPD. On September 3, 2019, the CNPD approved Decision no. 494/2019, which declares the inapplicability of several provisions of Law no. 58/2019 on the ground that they are manifestly incompatible with European Union law and, in particular, with the GDPR. The CNPD stated that, taking into account the principle of the primacy of European Union law, in future cases it will not apply those specific provisions. These include rules concerning the scope of Law no. 58/2019, the restriction of the access right, and the powers of the CNPD to apply administrative sanctions.

2 Personal Data Processed by Electronic Means

In Portugal, the processing of personal data by electronic means is also generally governed by the GDPR, which is complemented in this respect by some of the provisions of Law no. 58/2019 and other specific laws, such as the Labour Code.

The Labour Code (approved by Law no. 7/2009, of 12 February 2009, and subsequently amended) states that an employer cannot use distance surveillance means—like CCTV cameras—at the workplace by using technological equipment, which envisages the control of the professional performance of the employee (Article 20). Only reasons of safety regarding people or goods, or special demands connected to the specific activity may justify such a control. The use of these means

hoeren@uni-muenster.de

is considered as treatment of sensitive data and their use must be authorized by the CNPD.

There are some examples of case law in the field of "personal data processed by electronic means".

According to Article 5 of Law no. 41/2004, as amended by Law no. 46/2012, of 29 August 2012, the storage of data in the equipment of a user is only allowed in the case of a previous consent, based on full and clear information given in compliance with Law no. 67/98, notably identifying the purposes of the data processing.

This provision was approved basically in order to regulate the use of "cookies".

The requirement of a previous consent is not applicable: (1) when the storage is based on the purpose of sending a message through a network or (2) when it is necessary in order to provide an information society service (Article 5/2).

In respect of minors, the Court of Appeal (*Tribunal da Relação*) of Évora decided in 2015[4] that parents should not post photos or images in social networks that could identify sons or daughters. According to the court, this was the only proportional way to safeguard children's rights of privacy and data protection in cyberspace.

One of the reasons invoked by the court in order to justify its decision was that children driven by curiosity are especially vulnerable to sexual exploitation, due to their acting without the necessary awareness as to the consequences of their behaviour online.

Insofar as the right to be forgotten is concerned, the CNPD ruled in its decision no. 536/2016 (not publicly available) that a search engine must erase search results related to a person that had been accused and was a target of public attention 8 years earlier for the reason of being a suspect of committing a crime. However, in that case the data subject was not convicted for the practice of any crime. The decision of Portuguese DPA was adopted in on the basis of rules applicable to public personalities.

In the field of marketing, Law no. 41/2004 is applicable with the amendments introduced by Law no. 46/2012.

Article 13-A of Law no. 41/2004, introduced by Law no. 46/2012, enshrines an opt-in system for unsolicited electronic messages sent for the purposes of direct marketing. A previous consent by subscribers or users is required, especially for messages sent in the context of systems without human intervention (section 1).

In what concerns legal persons, an opt-out system is applicable, whereby subscribers may object to future communications once they are enrolled in a list updated by *Direção Geral do Consumidor* (General Directorate for Consumer Affairs) (Article 13-B, section 2).

In spite of Article 13-A/1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or service, in accordance with the Portuguese Data Protection Act, the same natural or legal person may use these electronic contact details for direct

[4] http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/7c52769f1dfab8be80257e830052d374?OpenDocument.

hoeren@uni-muenster.de

marketing of its own similar products or services, provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the moment of their collection and on the occasion of each message in case the customer has not initially refused such a use (Article 13-A, section 3).

The practice of sending electronic mail for purposes of direct marketing, which disguise or conceal the identity of the sender, on whose behalf the communication is sent, and which do not have a valid address to which the recipient may send a request that such communications cease, is in any case forbidden (Article 13-A, section).

Article 13-B, under the title of "lists created for unsolicited messages", establishes the obligation for legal persons that work in the field of direct marketing to keep an updated list of data subjects that do not want to receive unsolicited messages for the said purpose and a list of people who did not oppose to being recipients of those messages.

Data subjects may be freely included in such lists. However, this requires filling in a form in the web page of *Direção Geral do Consumidor*.

According to the Portuguese Labour Code (Article 20), personal data obtained by distance surveillance means may only be kept during the necessary time in order to achieve its purposes and must be destroyed as soon as the employee concerned is transferred to another workplace, or upon termination of the employment contract.

The Portuguese Labour Code sets forth that the employee is entitled to confidentiality regarding the contents of private messages and the access to non-professional information that he or she sends, receives or consults, notably by e-mail (Article 22).

The Portuguese DPA adopted Decision no. 1638/2013[5]—which is mandatory in administrative field and has been highly influential in court decisions—which concludes that:

(i) the employer should define in detail the level of tolerance regarding employees' use of their telephones and the forms of control adopted, keeping in mind that a strict ban on personal communications is not allowed;
(ii) in certain areas, confidentiality is necessary in order to perform a professional activity according to the law (as is the case, *e.g.,* of lawyers, health professionals, and journalists), so it is not possible for the employer to monitor their communications;
(iii) in cases where a detailed invoice is used, employers should ask the operator to delete the last four numbers of all communications made;
(iv) notwithstanding the rules adopted by employers, they are not allowed to open the communications of employees without their knowledge and consent;
(v) getting access to the communications of employees is always a measure of last resort, even in cases where companies can be affected by the content of electronic communications; in such cases access may only be allowed in the presence of the employee or his/her representative;

[5] https://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf.

hoeren@uni-muenster.de

(vi) the employer shall not undertake a permanent and systematic control of its employees' access to the internet;
(vii) any limitations on employees' use of the internet shall be done in a global way, i.e., not individualized, in relation to all accesses within the employer's organization, with reference to the web connection time; and
(viii) the employer is entitled to process data about the most visited websites, but without identifying the place of origin of the access. A certain level of tolerance is expected in relation to employees' use of the internet for private purposes, in particular if the use occurs outside working hours.

The Portuguese DPA adopted Decision no. 7680/2014,[6] concerning the processing of personal data collected by geolocation technologies in a labour context. According to the *Comissão Nacional de Proteção de Dados*:

(i) the technology of geolocation, notably GPS devices, processes personal data in a way that may affect private life;
(ii) by using remote control devices, it could be possible for employers to develop a permanent control of employees, during their working time and even in their leisure time;
(iii) the consent given by employees is not, in general, relevant to authorize the processing of personal data by employers because it is not considered as being free in the context of a labour contract; and
(iv) personal data collected by geolocation technologies cannot be used in order to evaluate the performance of an employee (Article 20 of the Portuguese Labour Code).

Some courts, however, have a different perspective.

The Supreme Court of Justice (*Supremo Tribunal de Justiça*) decided that data collected by GPS devices is not considered as being the object of "distance surveillance" because this expression is only applicable to CCTV cameras (ruling of *the Supremo Tribunal de Justiça* of 13 November 2013).[7]

The Court of Appeal of Guimarães decided that data collected by GPS devices cannot be used for the purposes of evaluating the performance of employees but may be used in disciplinary proceedings (ruling of 3 March 2016).[8]

Law no. 41/2004 contains several rules on data breaches and the security of personal data processed by electronic means.

According to Article 3, companies that make electronic communications services accessible to all must adopt all appropriate technical and organizational measures to protect personal data (section 1).

[6] https://www.cnpd.pt/bin/orientacoes/DEL_7680-2014_GEO_LABORAL.pdf.

[7] http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e32eab3444364cb980257c2300331c47?OpenDocument.

[8] http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/302fdd824b16519780257f85004f8071?OpenDocument.

hoeren@uni-muenster.de

The provider of a public network of communications must ensure a level of security that is appropriate to the risks posed by the processing and the nature of the data to be protected (section 2).

The *Autoridade Nacional de Comunicações* (ANACOM) has as its mission regulating the communications sector, including electronic communications and, within this context, it has the duty to approve recommendations on the best policies to be adopted in the areas of security of personal data and data breaches (section 3). Having regard to the state-of-the-art measures and the cost of their implementation, such recommendations must be based on a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The recommendations of ANACOM must take into consideration the opinions issued by the Portuguese DPA (section 8).

Article 3-A of Law no. 41/2004 provides that companies responsible for making the electronic communications services accessible to the public shall notify the Portuguese DPA of a personal data breaches without delay (section 1). The notification of the Portuguese DPA shall include the consequences of data breaches, and the measures adopted to remedy them (section 8).

This notification must be sent to subscribers or users whenever it may affect them negatively (section 2).

A negative effect on personal data exists whenever the breach may result, in particular, in the theft of identity, fraud, physical harm, significant humiliation or damage to reputation (section 3).

Irrespective of the above, if a person/entity is affected by a breach of Law no. 67/98, it is entitled to file a claim to the Portuguese DPA and/or file a civil lawsuit in order to seek compensation for damages (section 6).

Th said notification must include a reference to the nature of the breach of personal data, information on where further information may be obtained and the recommendation issued by ANACOM (section 7).

Companies that make available networks and electronic communications services shall guarantee the inviolability of communications and traffic data involved therein (Article 4/1).

The use of tapping and storing devices, and other means of monitoring and intercepting electronic communications and traffic data involved may only be used with the prior consent of the data subject or when mandatory by law (Article 4/2).

It is however allowed, with prior consent of the data subject, to record and to store electronic communications and traffic data in the context of lawful contract practices in order to prove if/or how a contract was concluded (Article 4/3).

It is also allowed to record electronic communications made to public bodies in the context of emergency situations (Article 4/4).

Article 32 of the Portuguese Data Protection Act provides that the Portuguese DPA shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the provisions of this Act, taking account of the specific features of the various sectors (section 1).

hoeren@uni-muenster.de

3 Data Protection in the Electronic Communications Sector

In its ruling no. 403/2015, of 27 August 2015, the Constitutional Court assessed whether Article 78 (2) of the Parliamentary Decree no 426/XII, entitled "Legal System of the Republic's Information System", complied with Article 34(4) of the Portuguese Constitution.

The rule in question states that officials of the Security Information Service and the Strategic Defence Information Service may, in undetermined circumstances, gain access to banking and tax data, data on communications traffic, location or other data connected with communications that are needed in order to identify the subscriber or the user, or to find and identify the source, destination, date, time, duration and type of communication, as well as to identify the telecommunication facilities or its location whenever this was deemed necessary, suitable and proportional in a democratic society, with the aim of fulfilling the legal tasks of information services, subject to a necessary prior authorisation from a Preliminary Supervision Committee.

For its part, Article 34 (4) in the Constitution states that the interference of public authorities in the correspondence, telecommunications and other means of communication is forbidden, except in cases related to criminal proceedings, as provided for in the law.

In its answer to the first questions raised in this respect, the Constitutional Court affirmed that the prohibition to interfere in communications, as laid down in Article 34(4) in the Constitution, covers the traffic data referred to above; it also covers the exception mentioned in the final part of the provision which may only occur within the framework of the legal provision related to criminal proceedings (which is the exception that is constitutionally acceptable). When quoting case-law and legal writings on the subject, the Constitutional Court *inter alia* indicated that the necessities related to criminal investigation and to obtaining evidence justify reducing individual rights to the communications in question. However, such necessities require the legal authorities' evaluation in terms of needs, suitability and proportionality in order to avoid that they violate the principle of the least possible interference and of proportionality. Therefore, any evidence thus obtained may be considered as null and void on the basis of Article 32(8) of the Constitution and of Article 189 of the Code of Criminal Procedure. Indeed, notwithstanding the quality of its members, the Preliminary Supervision Committee (*Comissão de Controlo Prévio*) is not a legal authority; rather, it is an administrative body so that its intervention is not included in the sphere of a criminal proceeding.

On these grounds, the Constitutional Court decided that the decree approved by the Parliament was unconstitutional.

However, on 19 July 2017 the Parliament approved Organic Law no. 4/2017, published in the Portuguese Republic's Official Journal on 25 August 2017.

According to this act, information services officials are entitled to access communication data, if authorized and controlled by judges of the Supreme Court.

The Constitutional Court will have to decide, probably next year, whether this law is compatible with the Portuguese Constitution.

hoeren@uni-muenster.de

In its Decision no. 79/2014, the CNPD applied a fine to an electronic communication company, in the amount of €4,503,000, because it did not ensure the compliance with the security rules imposed by Law no. 41/2004.[9]

The main powers of the *Autoridade Nacional de Comunicações* are set out in Law no. 5/2004, of 10 February 2004, as amended, and comprise the following:

(i) Obtaining the necessary information in order to exercise its powers: "Entities subject to obligations pursuant to the present law shall submit to ANACOM all information, including financial information, in respect of their activity, in order that ANACOM may exercise all its competences provided for in the law (Article 108/1)";
(ii) ANACOM may adopt interim measures whenever it has evidence of any breach of the requirements set out in Articles 27, 28, 32 and 34 which represent an immediate and serious threat to public policy, public security or public health or which may create serious economic or operational problems to other providers or users of electronic communications networks or services, in which case it may take urgent interim measures to remedy the situation prior to reaching a final decision, setting the period during which the measures shall be in force (Article 111);
(iii) ANACOM is charged with monitoring compliance with the provisions of the said law and its implementing regulations, through its monitoring agents or representatives duly certified by the Board of Directors, without prejudice to the competences conferred upon other entities, including the Inspectorate General of Economic Activities (IGEA), the Directorate General of Customs (DGC), the National Commission for Data Protection (NCDP), the Consumer Institute and competent authorities in competition matters (Article 112);
(iv) Article 113 defines breaches and their respective fines. The breaches provided for in this law are punishable with a fine from €500 to €3740 and from €5000 to €5,000,000, depending on whether they concern natural or legal persons, respectively (section 1). When the breach results from failure to comply with a legal duty or an order of the National Regulatory Authority (the "NRA"), the application of sanctions or the compliance therewith does not exempt the offender from complying with the duty or order, where such compliance remains possible (section 3).
(v) Additional sanctions (provided for in Article 114) are: (a) Loss in favour of the State of objects, equipment and illicit devices, in the event of breaches provided for in subsections qqq) and rrr) of section 1 of Article 113; (b) Prohibition from the exercise by the offender of its activity for up to 2 years, for breaches provided for in subsections a), h), l), n), p), x) and z) of section 1 of Article 113; (c) Forfeiture of the right to participate in tenders or auctions promoted under the scope of the present law for up to 2 years, for breaches provided for in subsections l), p), x) and z) of Article 113.

[9]Processo n.º 13112/2/20191.

hoeren@uni-muenster.de

(vi) The law provides for the payment of penalties. Notwithstanding other applicable sanctions, in case of non-compliance with decisions of the NRA that impose administrative sanctions or that order, in the exercise of legally assigned powers, the adoption of certain behaviours or measures by undertakings that provide electronic communications networks and services, the NRA may impose, where justified, a compulsory penalty payment, notably in the cases set forth in subsections a), e), f), g), p), v), x), z), gg), mm), pp), rr), ss), tt), zz), aaa), ccc), fff), hhh), lll), nnn), sss), ttt) and vvv) of section 1 of Article 113 (Article 116/1).

4 Data Protection and Digital Forensics

The law applicable on these matters is Law no. 109/2009, of 15 September 2009 (Cybercrime Law). The types of crimes provided for therein are the following:

(i) Computer-related forgery—Whoever, with the purpose of deceiving someone else in the context of a legal relationship, enters, alters, erases or suppresses computer data, or commits any other form of interference with the automatic processing of data resulting in false data or documents, with the intent that it be considered or acted upon for legal purposes as if it were authentic, shall be punishable by imprisonment of up to 5 years or by fine ranging between 120 and 600 days (Article 3/1);

(ii) Damage caused to programs or other computer data—Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, deletes, alters, fully or partially deteriorates, damages, suppresses or renders unusable or inaccessible other people's programs or other computer data or by any other means seriously hinders their functioning, shall be punishable by imprisonment up to 3 years or by fine (Article 4/1);

(iii) Computer-related fraud—Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, hinders, prevents, interrupts or seriously disrupts the functioning of a computer system by entering, transmitting, deteriorating, damaging, altering, deleting, preventing access or suppressing programs or other computer data or by any other means interferes in a computer system, shall be punishable by imprisonment up to 5 years or by fine up to 600 days (Article 5/1);

(iv) Illegal access—Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, accesses a computer system, shall be punishable by imprisonment up to one year or by fine up to 120 days (Article 6/1);

(v) Illegal interception—Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, intercepts by technical means transmissions of computer data to, from or within a computer system, shall be punishable by a term of imprisonment up to 3 year or by fine (Article 7/1);

hoeren@uni-muenster.de

(vi) Illegal reproduction of protected programs—Whoever illegally reproduces, discloses or communicates to the public a legally protected computer program, shall be punishable by imprisonment up to 3 years or by a fine (Article 8/1).

In terms of interception of communication data, Law no. 109/2009 is applicable without prejudice to the regime laid down in Law no. 32/2008, of 17 July, which provides for the following:

(i) Seizure of emails or similar communication records—"Whenever, in the course of a computer system search, or of another legitimate means of access to a computer system, emails or similar communication records are found, which stored in that computer system or in another system and which can be lawfully accessed from the former, the competent judicial authority shall authorize or order the seizure of data deemed to be of major interest to uncover the truth or to collect evidence, applying as appropriate the regime of seizure of correspondence provided for in the Criminal Procedure Code" (Article 17).
(ii) Interception of communications

- The interception of communications shall be permitted in proceedings for criminal offences: (a) Provided for in the said law; or (b) Committed by means of a computer system or which require the collection of electronic evidence, where such criminal offences are provided for in Article 187 of the Criminal Procedure Code.
- Interception and recording of transmission of computer data shall only be authorized during the investigation stage, where there are reasons to believe that this measure is essential to the uncovering of the truth or that, otherwise, it would be impossible or very difficult to obtain evidence, on the basis of a substantiated order from the examining judge, further to a request from the Public Prosecutor.
- The interception may concern the recording of data on the content of communications or aim only at the collection and recording of traffic data, and the order referred to in the preceding (Article 18).

In what concerns data retention, Law no. 32/2008, of 17 July 2008, is applicable.[10]

The scope of the law comprises the "Retention and transmission of traffic and location data on both natural persons and legal entities, and of the related data necessary to identify the subscriber or registered user, for the purpose of the investigation, detection and prosecution of serious crime by competent authorities, transposing to the national legal order Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending Directive 2002/58/EC of the European Parliament and of the Council of 12 July

[10] https://www.anacom.pt/render.jsp?contentId=976199.

hoeren@uni-muenster.de

2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector." (Article 1/1).

The providers of publicly available electronic communications services or of public communications networks must retain the following categories of data: (a) Data necessary to trace and identify the source of a communication; (b) Data necessary to trace and identify the destination of a communication; (c) Data necessary to identify the date, time and duration of a communication; (d) Data necessary to identify the type of communication; (e) Data necessary to identify users' communication equipment or what purports to be their equipment; (f) Data necessary to identify the location of mobile communication equipment (Article 4/1).

The providers referred to in section 1 of Article 4 must retain data provided for therein for a one-year-period from the date of the communication (Article 6).

The Portuguese Data Protection Act contemplates the following specific crimes:

(i) "Non-compliance with obligations relating to data protection" which consists of: (a) omitting the notification or the application for authorisation referred to in Articles 27 and 28; (b) providing false information in the notification or in applications for authorisation for the processing of personal data or makes alterations in the latter which are not permitted by the legalisation instrument; (c) misappropriating or using personal data in a form incompatible with the purpose of the collection or with the legalisation instrument; (d) promoting or carrying out an illegal combination of personal data; (e) failing to comply with the obligations provided for in this Act or in other data protection legislation when the time limit fixed by the CNPD for complying with them has expired; (f) continuing to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act after notification by the CNPD not to do so, shall be liable to up to one year's imprisonment or a fine of up to 120 days (Article 43);

(ii) "Undue access", which consists of a person acting without due authorisation in order to gain access by any means to personal data prohibited to it, such person being liable to up to one year of imprisonment or a fine of up to 120 days. The penalty shall be increased to the double of the maxima when access: (a) is achieved by violating technical security rules; (b) allows the agent or third parties to obtain knowledge of personal data and (c) provides the agent or third parties with a benefit or material advantage (Article 44);

(iii) "Invalidation or destruction of personal data", which consists of acting without due authorisation, erasing, destroying, damaging, deleting or changing personal data, making them non usable or affecting their capacity for use, the agent being liable to up to 2 years of imprisonment or a fine of up to 240 days. The penalty shall be increased to the double of the maxima if the damage caused is particularly serious (Article 45);

(iv) "Qualified non-compliance", which concerns any person who, after being notified to do so, does not interrupt, cease or block the processing of personal data, such person being subject to a penalty corresponding to the crime of qualified non-compliance (Article 46);

hoeren@uni-muenster.de

(v) "Violation of the duty of secrecy" which corresponds to a person bound by professional secrecy rules according to the law, without just cause and without due consent revealing or disclosing personal data, totally or in part, such person being liable to up to 2 years of imprisonment or a fine of up to 240 days (Article 47).

References

Pinheiro AS (2015) Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional. AAFDL, Lisbon

Pinheiro AS, Coelho CP, Duarte T, Gonçalves CJ, Gonçalves CP (2018) Comentário ao Regulamento Geral de Proteção de Dados. Almedina, Coimbra

hoeren@uni-muenster.de

Data Protection Regulations: Overview of the Romanian Legislation and Deficiencies

Elena Lazar and Dragos Nicolae Costescu

1 Introduction

1.1 Subject-Matter, Purpose and Scope of the Present Report

The object of this paper is an in-depth study and analysis of the current legal framework in the field of data protection, with the intention of showing to what extent an appropriate level of protection is achieved compared to the provided European level of protection. The correct regulation, interpretation and application of European data protection legal norms by all member states, including Romania, is not possible if they are not known and well understood. By European data protection norms we understand both Directives (that need to be transposed in the national legislation) and Regulations (directly applicable at national level). Taking into account the fact that the current Romanian framework on Data Protection is quite recent, it should be interpreted in the light of the national and European case law.[1] The paper also seeks to highlight the practical effects of the entry into force, the European normative framework, which is much more developed than it appears at a first glance.

[1] See Custers et al. (2017).

E. Lazar (✉) · D. N. Costescu (✉)
University of Bucharest, Bucharest, Romania
e-mail: lazar.elena@drept.unibuc.ro; dragos@bnpa.ro

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_12

hoeren@uni-muenster.de

1.2 Organization of the Report

This report is divided into four chapters.

After the introduction provided in Sect. 1, Sect. 2 will give an overview of the general data protection framework and its provisions in the Romanian legal system, presenting the novelties that came up with it. For this purpose, that chapter will examine the applicable rules and the provisions of the laws regulating the National Supervisory Authority for Personal Data Processing activity, the provisions of the law on electronic commerce, the provisions of the law regarding on the measures for the application of Regulation (EU) 2016/679 and lastly the provisions of the law on the regulation of personal data processing by the structures/units of the Ministry of Administration and Interior in the activities of preventing, investigating and fighting crimes, as well as maintaining and securing public order.

Section 3 will be analysing the status of specific areas on the field of data protection—health data and employment data.

Section 4 will provide an overview of the Romanian Data retention law.

2 The General Data Protection Framework

The new legislation proves to be quite complex and compared to the former Romanian data protection regulation/law,[2] which has been operating for almost 15 years without any major changes brought to it during these years, GDPR[3] (General Data Protection Regulation) came up with many revolutionary changes in the collecting, processing and storing of personal data. These include, among others:

a) An increase in penalties for breaches of personal data protection rules. Compared to the current situation, where maximum fines amount to 50,000 lei, the Regulation sets out the DPA (Data protection authority) may impose a fine of up to 83,610,000 lei (around 20 million EUR), or 4% of the total worldwide turnover;
b) Expanding the current and introducing new individual's rights, including the right to request restrictions to the scope of the processing of personal data, the right to data portability, the right to be provided with a copy of the personal data at no charge and the right "to be forgotten" (*droit a l'oublie*);

[2]See Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed, published in the Official Gazette no. 790 from 12 December 2001.

[3]See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, 4.5.2016, repealing Directive 95/46/EC.

hoeren@uni-muenster.de

c) The obligation to formally notify the intent to process personal data is revoked, and on the contrary, the obligation to keep internal records of personal data that are being processed is introduced;
d) The obligation for companies to establish a job position of a data protection officer under certain conditions;
e) The rules for technical and organizational measures aimed at protecting personal data are refined;
f) The data controller will have a new duty to assess the impact of the data processing on the personal data protection and if necessary, to consult the supervisory authority on a mandatory basis;
g) Any breach of personal data security and the individuals concerned will have to be immediately notified to the DPA.

2.1 The Applicable Rules in Romania

On the 31st of July 2018, Law no. 190/2018[4] on the measures for the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) entered into force. This law establishes the measures necessary for the implementation at national level, mainly, of the provisions of Article 6 (2), Article 9 (4), Articles 37-39, 42, 43, Article 83 (7), Article 85 and Articles 87-89 of the GDPR.

Also, the Law no. 129/2018 for amending and supplementing Law no. 102/2005[5] regarding the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing and for repealing Law no. 677/2001 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data has entered into force (the *"DPA Authority Law"*).

The National Supervisory Authority for Personal Data Processing (NSAPDP) issued *Decision no. 133 of the 3rd of July 2018* on the approval of the procedure for receiving and solving complaints. This Decision was published in the Official Journal of Romania no. 600 of the 13th of July 2018, Part I and entered into force on the date of the publication. This decision approves the procedure for receiving and solving complains, set out in Annex no. 1, as well as the complaint form in

[4]See Law no. 190 of 18 July 2018 on the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and repealing Directive 95/46/EC, published in the Official Gazette no. 651 from 26 July 2018.

[5]See Law no. 102 of 3 May 2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, published in the Official Gazette no. 947 from 9 November 2018.

hoeren@uni-muenster.de

electronic format, provided in Annex no. 2. Also, in the Official Gazette of Romania no. 892 of 23 October 2018, it was published the decision no. 161 of the National Supervisory Authority for Personal Data Processing (NSAPDP) regarding the approval of the Investigation Procedure.

Romanian legislation on data protection also includes law no. 238 of June 10, 2009 regarding the regulation of personal data processing by the structures/units of the Ministry of Administration and Interior in the activities of preventing, investigating and fighting crimes, as well as maintaining and securing public order, law that should be read in the light of the provisions of the Criminal Code[6] and Criminal Procedural Code.[7]

Lastly, in the electronic communication sector we have the law no. 506 of 17 November 2004 on the processing of personal data and the protection of privacy *in the electronic communications sector*, and the law no. 235 of 12 October 2015[8] for amending and completing the Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector and repealing law no. 82 of June 13, 2012 on the retention of the data generated or processed by the providers of public electronic communications networks and of the providers of publicly available electronic communications services, whose provisions will be analysed in separate section in the present paper (Sect. 4).

2.2 *The General Provisions of the Romanian Laws on Data Protection*

2.2.1 The Provisions of the Laws Regulating the National Supervisory Authority for Personal Data Processing Activity

Like previously mentioned, the activity of NSAPDP is regulated by LAW no. 102 of 3 May 2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing and Law no. 129/2018 for amending and supplementing Law no. 102/2005[9] regarding the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing.

[6]See Law no. 286/2009 on the New Criminal code, published in the Official Gazette no. 510 from 24 July, 2009.

[7]See Law no. 135/2010 on the New Code of Criminal Procedure, published in the Official Gazette no. 486 from 15 July 2010, in force since 1 February 2014.

[8]See Law no. 235 of 12 October 2015 for amending and completing the Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, published in the Official Gazette no. 767 from 14 October 2015.

[9]See Law no. 102 of 3 May 2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, published in the Official Gazette no. 391 of May 9, 2005.

hoeren@uni-muenster.de

NSAPDP authority carries out its activity completely independent and impartial. The supervisory authority shall monitor and control with regard to their legitimacy, all personal data processing, subject to this law. In order to achieve this purpose, the supervisory authority exerts the following attributions:

a) Issues the standard notification forms and its own registers; authorizes personal data processing in the situations set out by law;
b) May dispose, if it notices the infringement of the provisions of the present law, temporarily suspending the data processing or ending processing operations, the partial or total deletion of processed data and may notify the criminal prosecution bodies or may file complaints to a court of law;
c) Informs the natural or legal persons that work in this field, directly or through their associative bodies on the need to comply with the obligations and to carry out the procedures set out by this law;
d) Keeps and makes publicly accessible the personal data processing register;
e) Receives and solves petitions, notices or requests from natural persons and communicates their resolution, or, as the case may be, the measures which have been taken;
f) Performs investigations—*ex officio*, or upon requests or notifications;
g) Is consulted when legislative drafts regarding the individual's rights and freedoms are being developed, concerning personal data processing;
h) May draft proposals on the initiation of legislative drafts or amendments to legislative acts already enforced, in the fields linked to the processing of personal data;
i) Collaborates with the public authorities and bodies of the public administration, centralizes and analyses their yearly activity reports on the protection of individuals with regard to the processing of personal data, issues recommendations and assents on any matter linked to the protection of fundamental rights and freedoms regarding the processing of personal data, on request of any natural person, including the public authorities and bodies of public administration; these recommendations must mention the reasons on which they are based and a copy must be transmitted to the Ministry of Justice; when the recommendation or assent is requested by the law, it must be published in the Official Gazette of Romania, Part I.

The entire staff of the supervisory authority has the obligation of permanently keeping the professional secrecy, except for the cases set out by law, regarding the confidential or classified information they have access to in carrying out their duties, even after termination of their legal employment relations with the supervisory authority.

Investigations may be triggered by default or by complaint. This means that the NSAPDP may take notice of certain violations of personal data protection law. *Ex-officio* investigations may be carried out:

hoeren@uni-muenster.de

a) At the proposal of the NSAPDP control departments;
b) At the proposal of the NSAPDP president or vice-president through a written resolution;
c) At the proposal of other departments within the NSAPDP;
d) Following the transmission of personal data breach notifications;
e) For the verification of data and information regarding the processing of personal data, obtained by the NSAPDP from sources other than the ones that are the subject of a complaint, including those based on notifications or information received from another supervisory authority or from another public authority;
f) For international cooperation, as well as for cooperation with the other supervisory authorities in the Member States, in the field of personal data protection, including in the framework of joint operations and mutual assistance.

What is interesting is that when you file a personal data privacy violation notification to an authority (because you have a legal obligation to do it in certain cases), the authority may use the information you send to initiate an investigation against you. In fact, in some situations, it would be the equivalent of a self-denouncement.

Is the investigation limited to a complaint/*ex officio*? The answer to this question is no. The NSAPDP may initiate an investigation based on clues/complaints, but it may verify any other aspect related to personal data protection. This means that even if the subject of the complaint is unfounded, they may find other irregularities to sanction companies.

In field investigations, the NSAPDP control staff carries out the following activities: going to the headquarters/domicile/office or other locations where the audited entity operates; presenting the badge and power of attorney, according to the situation, to the representatives of the audited entity who will ensure the involvement of the persons who are to provide relevant information about the controlled field. The persons designated by the controlled entity/The Data Protection Officer take(s) part in the carrying out of the control, by providing the information and documents requested by the control team, and they sign the resulting control papers; in the cases provided by the law, presenting the legal authorization issued by the President of the Bucharest Court of Appeal or by a judge delegated by it; requesting the registration of the travel order and of the power of attorney, if applicable; entering the data provided in art. 3 par. (2) of the Law no. 252/2003[10] on program counters into the program counter of the audited entity, if applicable; presenting the objectives of the investigation; verifying all aspects related to the subject of the investigation by requesting any information related to the control objectives; verifying any document, equipment or data storage medium necessary to carry out the investigation; removing the documents, in a certified copy made by the controlled entity, or the relevant documentation related to the aim of the control and attaching them to the verification/sanctioning report; drawing up the verification/sanctioning report, by

[10]See Law no. 252 of 10 June 2003 on the Single Control Register Published in the Official Gazette no 429 from 18 June 2003.

hoeren@uni-muenster.de

highlighting the situations presented by the audited entity, the statements of its representatives and own findings, and applying contravention sanctions or other types of corrective measures, where applicable; applying a fine if the amount does not exceed the equivalent in lei of 300,000 euro; applying the remedies prescribed by the law; elaborating a remediation plan in the situations stipulated by the law; making the necessary recommendations to remedy the identified deficiencies where necessary; communicating/handing over to the audited entity a copy of the verification/sanctioning report.

What is the legal authorization? If the control is in any way prevented, the NSAPDP may request a legal authorization, a sort of warrant, to the President of the Bucharest Court of Appeal or to a judge delegated by it. It must be added here that a copy of the legal authorization must be communicated to the audited entity before the commencement of the investigation.

As with the Competition Council's[11] control procedure, NSAPDP inspectors may hear the people they consider relevant (who could provide clues or more information about the audit).

According to the GDPR, the sanctions are: the reprimand and the fine. Despite this fact, in some cases, the NSAPDP may issue also warnings.

If there is a fine of less than 300,000 Euro, the sanction is applied by means of a verification/sanction report written by the control staff. If there is a fine that exceeds 300,000 Euro, the sanction is applied by means of a decision made by the President of the National Supervisory Authority, based on the statement and on the report of the control personnel.

Moreover, the NSAPDP may order, by decision of the President, a penalty payment of up to 3000 lei for each day of delay, calculated from the date established by the decision, in case of non-compliance with the corrective measures applied or in case of tacit or express refusal to supply all information and documents requested in the investigative procedure or in case of refusal to submit to the investigation, according to the law. Furthermore, the decision of the president of the NSAPDP is enforceable.

2.2.2 The Provisions of the Law 506/2004 on Electronic Commerce

This Law establishes the specific conditions for safeguarding the right to privacy with respect to the processing of personal data in the electronic communications sector. The provisions of this Law shall apply to the providers of public electronic communications networks and of publicly available electronic communications services, as well as to the providers of value added services and of directories of subscribers who, in the frame of their commercial activity, are processing personal data. This Law shall not apply to the processing of personal data carried out:

[11]The Competition Council, an autonomous body, administers and implements the Competition Law (No. 21/1996), which aims to protect, maintain and stimulate competition and a normal competitive environment in order to promote the interests of consumers.

hoeren@uni-muenster.de

a) In the frame of the activities in the field of national defence and national security, performed within the limits and subject to restrictions set out by the legal provisions in force;
b) In the frame of the activities concerning the fight against crime and the keeping of public order, as well as in the frame of other activities in the areas of criminal law, performed within the limits and subject to restrictions set out by the legal provisions in force.

The law operates with two categories of data:

a) Traffic data—any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
b) Location data—any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

There is no specific definition of "communication data", but only the definition of communication[12]—any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service; this does not include the information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

According to article 4 of the same law:

(1) The confidentiality of communications and the related traffic data by means of public electronic communications networks and publicly available electronic communications services is guaranteed;
(2) Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data are prohibited, except for the following cases:

a) These operations are carried out by the users who participate in that communication;
b) The users who participate in that communication have previously given their written consent;
c) These operations are carried out by the competent authorities, under the conditions set out by the legal provisions in force.

2.2.3 The Provisions of the Law No. 190/2018 on the Measures for the Application of Regulation (EU) 2016/679

On the 31st of July 2018, Law no. 190/2018 on the measures for the application of Regulation (EU) 2016/679 entered into force, shedding some light over the data protection framework,

We will show below what the main changes are or, in other words, the additions to the EU Regulation.

[12]See article 2.

hoeren@uni-muenster.de

The law defines the following: national identification number—the number by which a natural person is identified in certain record systems and which is of general applicability, such as: the personal identification code, the ID series and number, the passport number, the driving license number, the social security number.

Thus, almost any number that helps to officially identify an individual is a national identification number.

The task that serves the public interest is defined by this law as including those activities of political parties or of organizations of citizens belonging to national minorities, of non-governmental organizations, which serve the achievement of objectives provided by constitutional law or by international public law, or the functioning of the democratic system, including encouraging citizens to participate in the decision-making process and in the preparation of public policies, respectively promoting the principles and values of democracy.

Public authorities/bodies are advantaged by the new law and in addition they have 90 days at their disposal from the date of communication of the official report of the contravention, to remedy the detected irregularities and to fulfil their legal obligations.

By far the most heated discussions with regards to the new law have been generated by processing personal social numbers (CNPs) or ID data.

Grounds for processing personal data according to GDPR: consent, concluding or executing a contract, fulfilling a legal obligation, vital interests, public interest, legitimate interest.

If the operator chooses to process based on legitimate reason, it is necessary to appoint a DPO (Data Protection Officer). We hereby quote the law provision in order to avoid confusion:

> Art.4 – (1) The processing of a national identification number, including by collecting or disclosing documents containing it, can be made in the situations provided by Art. 6 paragraph (1) of the General Data Protection Regulation.
>
> (2) The processing of a national identification number, including by collecting or disclosing documents containing it,
>
> the purpose of Article 6 (1) (f) of the General Data Protection Regulation, namely the achievement of legitimate interests pursued by the operator or a third party, shall be the establishment by the operator of the following safeguards:
>
> For the purposes provided by Art. 6 par. (1), item f) of the General Data Protection Regulation, namely achieving the legitimate interests followed by controller or by a third party, safeguards shall be made provided that the controller institutes the following:
>
> b) Appointing a data protection representative, in compliance with the provisions of Art. 10 of the present law;
>
> c) Setting out storage limitation periods, according to the nature of the data and the processing purpose, as well as specific periods when personal data need to be deleted or revised for deletion purposes;
>
> d) Periodical training regarding the obligations of the persons processing personal data, under the direct authority of the controller or the processor.

hoeren@uni-muenster.de

When addressing the issue of legitimate interest, if we do not have a legal obligation (provided by the law in a broad sense, such as law, decision, ordinance, local council decision etc.), we will have to follow the other legal bases mentioned above.

For example, displaying the CNP on tax invoices or in the "customer" or "representative" field may fall into another legal category than the legitimate interest, so appointing a DPO will be necessary. This is not the case though when we ask an employee for the CNP to write up the employment contract, as this is an obligation stated by the labour code.[13]

If a data operator considers it beneficial to its work to process a national identification number to the detriment of the interests of natural persons, it will be able to do so, on grounds of the legitimate interest, even if it affects the latter's rights if one were to assess them. In other words, the legitimate interest scheme looks like this:

Processing personal data in the context of employment relations and the processing of health data will be analyzed separately in distinct sections.

2.2.4 The Provisions of the Law No. 238/2009 Regarding the Regulation of Personal Data Processing by the Structures/Units of the Ministry of Administration and Interior in the Activities of Preventing, Investigating and Fighting Crimes, as Well as Maintaining and Securing Public Order

This law regulates the automatic and non-automatic processing of personal data for the purpose of carrying out activities for the prevention, investigation and combating of crimes, as well as for the maintenance and ensuring of the public order by the structures/units of the Ministry of Administration and Interior (M.A.I), according to their competencies.

To carry out the activities provided above, the structures/units of M.A.I. collects personal data, with or without the consent of the person concerned, under this law.

In addition, the collection of personal data without the consent of the person concerned shall only be made if this measure is necessary to prevent imminent danger at least to the life, physical integrity or health of a person or property, as well as to combat a particular offence.

The procedure involving the collection of personal data for carrying out the activities provided in art. 1 par. (1) of this law, shall be performed by the staff of the M.A.I. only for the purpose of fulfilling his/her duties and limited to the data necessary to be collected for the purposes previously mentioned. Global collection of data and not limited in time is not permitted.

Personal data held by the M.A.I. for the purposes set out by the present law may be transferred to the following recipients if there is an express legal provision in the

[13] https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes.

hoeren@uni-muenster.de

national legislation or in a treaty ratified by Romania, if there are legal provisions regulating police cooperation or international judicial cooperation in criminal matters or when the transfer is necessary to prevent a serious and imminent danger to the life, physical integrity or health of a person or property, as well as to combat a serious crime provided by law, in compliance with Romanian law:

a) The police, judicial or other competent authorities of the Member States or the bodies or institutions of the European Union with competence in the field of police or judicial cooperation in criminal matters;
b) The International Criminal Police Organization—Interpol or other similar international institutions;
c) Third-country police bodies.

Personal data stored in performing the activities provided by this law shall be erased or transformed into anonymous data when it is no longer necessary for the purposes for which it was collected or, as the case may be, blocked under the law.

The structures/units of the MAI, as operators, are liable for the damage caused to the data subject due to the processing of personal data, even if the damage was caused by the processing, according to the law, of inaccurate personal data provided by a competent authority of a Member State. If the structures/units of M.A.I. are obliged, under the law, to pay damages for damages caused to the data subject as a result of the processing of inaccurate personal data provided by a competent authority of a Member State, they are obliged to order the necessary measures for the recovery of the sums paid as indemnity to the authority that provided the data.

Like previously mentioned, the processing of data in the context of prevention, investigation and combating crimes:

Regulated in art. 138 of the Code of Criminal Procedure,[14] the methods of technical surveillance appear as follows:

a) Intercepting communications or any type of remote communication—intercepting, accessing, monitoring, collecting or recording communications via the telephone, computer system or any other means of communication;
b) Access to a computer system—entry into a computer system or means of storing computer data either directly or remotely through specialized programs or through a network in order to identify evidence;
c) Video, audio or video surveillance—photographing people, observing or recording their conversations, movements or other activities;
d) Locating or tracking by technical means—using devices that determine the location of the person or object to which they are attached;
e) Obtaining data on financial transactions of a person—operations to ensure the knowledge of the content of financial transactions and other transactions performed or to be performed through credit institutions or other financial entities, as well as obtaining from an institution credit or other financial entity

[14]See Law no. 135/2010 on the New Code of Criminal Procedure, published in the Official Gazette no. 486 of 15 July 2010.

hoeren@uni-muenster.de

of documents or information in its possession relating to the transactions or operations of a person;

f) Retaining, surrendering or searching for postal items—Checking by physical or technical means letters, other postal items or objects transmitted by any means.

Technical oversight/surveillance represents the activity of gathering evidence in the criminal investigation phase by using technical means capable of discovering and storing information and circumstances that lead to the establishment of the truth in a criminal proceeding and to the criminal liability of those who have participated in the commission of a crime.

Technical surveillance is carried out using one of the methods listed above, namely: interception of communications or any type of remote communication; access to a computer system; video, audio or video surveillance; location or tracking by technical means.

In order for the technical surveillance to be available, the following conditions must be met cumulatively: existence of reasonable suspicion about the preparation or commission of an offence listed in the legal texts; the measure be proportionate to the restriction of fundamental rights and freedoms, given the particularities of the case, the importance of the information or evidence to be obtained or the seriousness of the offence; evidence could not otherwise be obtained or obtaining them would entail particular difficulties that would prejudice the investigation or there is a danger to the safety of persons or valuable goods. Technical supervision may be ordered during criminal prosecution, for a maximum of 30 days at the request of the prosecutor, by the judge of rights and freedoms from the court having jurisdiction to hear the case at first instance or from the appropriate court in its grade, in whose district is found the headquarters of the prosecutor's office, which includes the prosecutor who made the request.

The measure of technical supervision may be prolonged, for duly justified reasons, by the judge of rights and freedoms from the competent court, at the motivated request of the prosecutor, each extension not exceeding 30 days.

3 The Status of Specific Areas Regarding Data Protection in the Internet

3.1 Status of Processing of Sensitive Data: Genetic, Biometric and Health Related Data

Sensitive personal data is personal data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

hoeren@uni-muenster.de

Consent to process sensitive personal data must be explicit.[15] The general restrictions on consent, set out above, will also apply. This suggests a degree of formality, such as ticking a box containing the express words "I consent". It is unlikely explicit consent could be obtained through a course of conduct.

A *controller* must provide *data subjects* with a privacy notice setting out how the individual's personal data will be processed. The privacy notice must contain the *enhanced transparency information*. In Romania, the Laws do not provide any further details in this respect.

Genetic, biometric, or health-related data processing for the purpose of automated decision-making or profiling is permitted according to the Law 190/2018 previously analysed with the explicit consent of the data subject, or if the processing is carried out under explicit legal provisions, by establishing appropriate measures to protect the legitimate rights, freedoms and interests of the data subject.[16]

This is particularly important because, in the course of the debates regarding this law, there was a change that limited the processing of the above-mentioned data, excluding automated decision-making or profiling, even with the express consent of the data subjects. This would have meant that most medical technology applications lately would have had to move to another Member State in order to carry out their activity (such as applications that automatically identify whether a melanoma is cancerous or not, without the initial intervention of a physician).

What does "health research" mean? "Health research" can be defined as one of the following types of scientific research for human health purposes:

a) Research aimed at understanding normal and abnormal functioning of the molecules, cells, organs and organisms;
b) Research that specifically addresses innovative strategies, devices, products or services for the diagnosis, treatment or prevention of human illness or injury;
c) Research aimed at improving the diagnosis and treatment (including rehabilitation and palliation) of human illnesses and injuries, and at improving the health and quality of life of individuals;
d) Research aimed at improving the efficiency and effectiveness of healthcare professionals and the healthcare system;
e) Research aimed at improving the health of the population as a whole or that of any part of the population through a better understanding of how social, cultural, environmental, occupational and economic factors determine the state of health.

[15] See Handbook on European Data Protection Law, Luxembourg Publications Office of the European Union, 2017, available at https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2014/07/handbook-european-dp-law/Handbook-dp-law-EN.pdf.

[16] Article 3: Processing of genetic data, biometric data or health data

(1) The processing of genetic, biometric or health data for the purpose of automated decision-making or profiling is permitted with the explicit consent of the data subject or if the processing is carried out under explicit legal provisions, with the establishment of appropriate measures to protect the rights, freedoms and legitimate interests of the data subject.

hoeren@uni-muenster.de

An operator who processes or continues to process personal data for health research purposes must implement the following "appropriate and specific measures"[17]:

a) Provisions to ensure that personal data are not processed in a manner that causes or is likely to cause harm or damage to the data subject;
b) Suitable governance structures, including: (i) the ethical approval of health research by a research ethics committee (if any); (ii) mentioning the involved operator; (iii) compliance by associate operators to Article 26 of GDPR; (iv) specification of all empowered persons; (v) specification of any third-party financing or otherwise supporting the project; (vi) the specification of any other person with whom they intend to share any personal data (including pseudonymised or anonymous data) and the purpose of such sharing; and (vii) the provision of training courses in the field of data protection law and practices to people conducting health research;
c) The following processes and procedures: (i) an assessment of the implications of data protection in health research; (ii) if the assessment indicates a high risk to the rights of individuals, an impact assessment of the data protection should be performed; (iii) data minimization measures (*e.g.* pseudonymisation); (iv) access control to prevent unauthorized consultation, modification, disclosure or deletion of personal data; (v) audit logs; (vi) security measures; (vii) the anonymisation, archiving or destruction of personal data after the completion of the health research; and (viii) other technical and organizational measures to ensure compliance with the GDPR;
d) The arrangements for ensuring the transparent processing of personal data;
e) "Explicit consent" of the data subject before the processing of his or her personal data for a specific purpose of the health research or, more generally, in this field.

3.2 Protection of Employees' Personal Data Processed by Electronic Means

Perhaps one of the most debated issues in the Romanian practice are the following two: the possibility of introducing integrity tests for employees and the issue related to the monitoring and surveillance at the work place.

With regards to the first issue, there are no provisions in the Romanian Data protection laws related to it, so accordingly employers have tried to interpret the laws and make assumptions.

In addition, the object of integrity testing, Romanian employers assumed the following:

a) Integrity tests should be conducted in good faith and will be conducted with respect for human rights and fundamental freedoms, human and professional dignity of the tested employees;
b) Integrity tests should not contain elements that may affect the image of the tested person;

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012SC0072.

hoeren@uni-muenster.de

c) Integrity tests should be conducted without causing employees under test to commit criminal and/or disciplinary deeds.

By interpreting the provisions of the Law 190/2018, the processing of personal data for integrity testing on employees may only be carried out under the legitimate interest of employers, unless the interests or fundamental rights and freedoms of employees that require the protection of personal data prevail.

The personal data processing accessory for integrity testing based on employer's legitimate interest will be the employee's right of opposition, for reasons related to the particular situation in which it is located, which will have to be guaranteed to them. Employers will have the obligation to cease processing for integrity tests if it does not demonstrate that it has legitimate interests that outweigh the rights and interests of the data subjects to continue the business (*i.e.* passing the balance test as described below and adequately documenting it).

In this respect, we mention that the other processing grounds are not a solution for the processing of personal data related to integrity testing, as follows:

a) Obtaining the consent of the employees in this situation is not a solution because it will be vitiated, being considered as not being freely expressed in view of the subordination relationship between the employee and the employer; Performing these integrity tests is not a necessary requirement for the employment contract between employers and employees, as an option of the employer;
b) Processing is necessary to fulfil a legal obligation that it is the operator's responsibility—we contend that we did not identify such an obligation that would apply to employers;
c) The results of these integrity tests do not come to protect the employee's vital interests, but rather as a means of protecting the employer's interests; Conducting these tests is not a public interest task and no exercise of public authority, most employers (excepting public authorities) being an eminently private entity that does not perform activities of public interest and has not been invested with public authority.

In order for the employer to be able to rely on its legitimate interest, it must, first of all, determine such an interest which, in our view, can be structured in the form of—ensuring the economic integrity of employer or the property it owns (e.g. buildings, money, goods, etc.) and the need to prevent or detect any possible fraudulent actions, corruption, or any other possible violation of applicable law (including criminal law). By reference to fundamental rights, this interest can also be subsumed in the form of—the defence of employer's right of ownership, which, in the field of labour law, finds expression both in the employer's right to determine its way of organization and functioning, determine how to verify the fulfilment of the obligations of its employees.

hoeren@uni-muenster.de

With regards to the second issue on the monitoring, article 5[18] of the Law 190/2018 states that when electronic monitoring systems and/or video surveillance systems are used in the workplace, the processing of personal data of employees in order to achieve the legitimate interests pursued by the employer is possible only if:

a) The legitimate interests pursued by the employer are duly justified and prevail over the interests or rights and freedoms of the data subject[19];
b) The employer has made the mandatory, full and explicit prior notice of the employees;
c) The employer consulted the trade union or, as the case may be, the representatives of the employees before the introduction of the monitoring systems;
d) Other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proved their effectiveness;
e) The length of storage of personal data is proportional to the purpose of the processing, but not more than 30 days, except in cases expressly regulated by the law or in duly justified cases.

The law requires employers to provide Labour Force Information (ITM), particularly with regard to personal data (employee information) that the employer holds, how they are used and with whom this information is shared. Employers must provide more detailed information than those currently required in existing EU data protection laws and must also ensure that their privacy notices accurately reflect their data processing workforce, according to the provisions of the law 190/2018.

Employers can provide privacy notices to their staff in any way they deem appropriate. For example, the privacy notice could be included in the salary leaflets or electronically communicated through the company's intranet or via email.

With regards to this matter of monitoring employees at work, on 12 January 2016, the European Court of Human Rights (the "Court") issued its judgment in the case of Bărbulescu v Romania, pursuant to application no. 61496/08.[20] In this decision, the Court ruled that, although there is privacy at the workplace and employers have no legal right to track their employees' communications, such interference might be acceptable in certain conditions.

Mr. Bărbulescu, the applicant was in charge of sales for a private company, for which purpose he was instructed by his employer to create a Yahoo Messenger account having as purpose chat communication and created by the employee at the request of the employer for the purpose of responding to clients' enquiries. The employee declared that he was using the account only for professional purposes (both under the internal regulation and at the separate request of the employer).

In order to check the manner in which professional tasks of Mr. Bărbulescu were completed, the employer monitored Mr. Bărbulescu's Yahoo Messenger account from the company's computer and alleged that the applicant, by using the company's

[18]Processing of personal data in the context of employment relationships.

[19]See Sandru and Alexe (2018).

[20]See the Judgement of ECHR, application no. 61496/08, 12 January 2016.

hoeren@uni-muenster.de

computer and the account he was instructed to create, for personal purposes, had breached express provisions assumed under the internal regulation, and thus, the employer terminated his contract.

The decision to terminate the contract was challenged by Mr. Bărbulescu before the competent Romanian courts, alleging that the employer had breached the applicant's right to private life and specifically, secrecy of correspondence. The Bucharest Court of Appeal finally ruled that, since the employee claimed during disciplinary proceedings that he had not used Yahoo Messenger for personal purposes, the employer was entitled to check the content of communication, as this was the only method for the employer to verify the defence.

Mr. Bărbulescu complained in front of the Court that his employer's decision to terminate the contract had been based on a breach of his right to respect for his private life and correspondence, protected under Article 8 of the European Convention on Human Rights.

In accordance with its constant case law, the Court considered that communications through Yahoo Messenger account should be included in the notion of "private life" and "correspondence" under Article 8 of the European Convention on Human Rights.[21]

The Court examined whether the right to respect for private life and correspondence is balanced with the employer's interest and decided that the employer had a legitimate interest because the following reasons were cumulatively met: the communications of the applicant were only accessed in the framework of disciplinary proceedings, as a result of the applicant's own allegations of not using the Yahoo Messenger account for personal purposes; the monitoring itself was limited to the Yahoo Messenger account, not extending to other communications from that account or other records from the computer; the domestic courts did not attach particular weight to the actual content of the applicant's communications, they relied on the transcript only to the extent that it proved the applicant's disciplinary breach, namely that he had used the company's computer for personal purposes during working hours.; the applicant did not convincingly explain why he had used the Yahoo messenger account for personal purposes.

The Court concluded that although there is privacy at the workplace and employers have no legal right to track their employees' communications, such interference might be acceptable if the right to respect for private life and correspondence is balanced with the employer's interest.

As the judgement was appealed, the Grand Chamber issued, on 5 September 2017, its ruling[22] reversing the decision of the Fourth Section of the Court and finding a violation of Article 8 of the European Convention on Human Right. In particular, the Grand Chamber held that although Bărbulescu had been informed of the ban on personal internet usage laid down in the employer's internal regulation, national courts had not taken into consideration whether he had been duly informed

[21] https://www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF.

[22] See the Judgement of ECHR, Grand Chamber, Application no. 61496/08, 5 September 2017.

hoeren@uni-muenster.de

prior to the monitoring of his communications that such monitoring was to take place as well as the extent and nature of the same, including the fact that the employer could access the content of such communications. Further, the Grand Chamber recognized that, although the contracting states to the ECHR have a significant margin of appreciation in establishing a legal framework governing an employer's regulation of private communications in the workplace, they must ensure that adequate and sufficient safeguards against abuse are in place. It also recognized that national courts had failed to guarantee appropriate remedies.

If the solution of the Grand Chamber does not surprise us, it is clear that the Court draws here the outlines of a very protective status of the employee with respect to his privacy in the context of a company.[23] The Court has thus just noted the positive obligations of the State to ensure to persons the guarantee of the enjoyment of a right enshrined in the Convention (Article 8).

4 Data Retention in Romania

A new law (no. 235/2015) amending the legislation governing the processing of personal data and privacy in the electronic communications sector was published in the Official Gazette on 14 October 2015 and has entered into force.

4.1 Purpose of the New Retention Law

The New Retention Law has been enacted to implement a Romanian Constitutional Court decision from 2014 which declared unconstitutional the local legislation transposing Directive 2006/24/EC[24] that ruled out the fact that the previous legislation could give rise to abuses in accessing and using retained data. The Court of Justice of the European Union invalidated this Directive in 2014, on the grounds that its provisions infringe fundamental rights concerning the respect for privacy and the protection of personal data, being considered in breach of privacy according to CJEU Joined Cases C-293/12 and C-594/12 decision from 8 July 2014. The European Court of Justice (CJEU) annulled the data retention directive, but this did not make national data retention legislations (whether or not enacted as implementation of the annulled directive) automatically invalid.[25]

[23] See Lazar (2018).

[24] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[25] https://observatory.mappingtheinternet.eu/page/data-retention-legislation-europe.

hoeren@uni-muenster.de

4.2 The Grounds of Invalidation of the Directive 2006/24/CE and the Outcome at National Level

The Data Retention Directive required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities. Such data included the calling telephone number and name and address of the subscriber or registered user, user IDs, Internet Protocol addresses, the numbers dialled, and call forwarding or call transfer records. The retention period could last for a minimum period of six months and up to two years, and the sole purpose of processing and storing the data was to prevent, investigate, detect, and prosecute serious crimes, such as organized crime and terrorism.[26] The content of the communications of individuals was not retained.

The case arose before the CJEU as preliminary questions from the High Court of Ireland and the Constitutional Court of Austria. In its preliminary ruling, the ECJ stated that the retention of data in order to allow access by the competent national authorities constitutes processing of data and therefore affects two basic rights of the Charter of Fundamental Rights: (a) the right to private life guaranteed by article 7, and (b) the protection of personal data guaranteed by article 8.[27]

Furthermore, article 52(1) of the Charter requires that any limitation on the exercise of rights guaranteed by the Charter must be provided by law and must respect the essence of such rights.[28] Any limitations are subject to a proportionality test and can be imposed only if they are necessary and meet the objectives of general interest as recognized by the EU or the need to protect the rights and freedoms of others.

The CJEU then proceeded to examine whether the interference by national authorities was *proportionate to the objective pursued*. In this regard, according to the settled case law, the standards to be met are that of being "appropriate" and "necessary" in order to achieve the objectives. The Court went on to state that the way too broad application of the Directive, since retention of data affects not only persons whose data may contribute to the initiation of legal proceedings, but also those for whom there is not a shred of evidence to suggest that their conduct might be connected to a serious crime. It also observed that no one is exempted from this rule; it even applies to those whose communications are subject to professional secrecy, according to national rules. As far as the period of retention, which runs from six months up to two years, the CJEU noted that the Directive did not set any objective criteria to determine the appropriate period of retention "to what is strictly necessary".[29]

[26] See art. 5 of Directive 2006/24/EC.

[27] https://ec.europa.eu/info/sites/info/files/edri_2017_en.pdf.

[28] https://www.loc.gov/law/help/eu-data-retention-directive/eu.php.

[29] *Ibidem*.

hoeren@uni-muenster.de

The Court reasoned that, based on the above, the Directive does not establish clear and precise rules that regulate the "extent of interference with the fundamental rights of Art. 7 and 8 of the Charter". Therefore, it concluded that the Directive "*entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what it is strictly necessary*".[30]

Romania adopted Law 298/2008[31] after the deadline imposed by the Directive, and used the extension norm which allowed the Member States to postpone application of this Directive to the retention of communications data relating to internet access, internet telephony and internet e-mail, until 15 March 2009. The strong public debate around the law soon resulted in a legal action filed by an NGO which challenged the constitutionality of the law. The Romanian Constitutional Court (RCC) was the first to decide[32] a law on data retention as contrary to the Constitution (see below), the decision being seen as a success of the civic society. On the other hand, this constitutional event produced a legislative gap on Romania's obligation to transpose Directive 2006/24/EC, as one of the major reasons of unconstitutionality stated by the RCC referred to the providers' obligation to continuously retain traffic, localization and identification data for six months. The Romanian legislator was thus confronted with two types of apparently incompatible obligations: the constitutional obligation of the Parliament (art. 147[33]) to comply with the RCC decision and amend accordingly the legal provisions; the obligation of double nature based on the Constitution (art. 148[34]) and the EU treaties (art. 258[35] of TFEU). As Romania

[30]See the judgement of CJEU, Digital Rights Ireland Ltd. (C-293/12), 16 May 2014 para. 65.

[31]Official Gazette, Part I, no. 780 of 21.11.2008.

[32]Decision no. 1.258/2009 (Official Gazette, Part I, no. 798 of 23.11.2009).

[33]Art. 147 (1): The provisions of the laws and ordinances in force, as well as those of the regulations, which are found to be unconstitutional, shall cease their legal effects within 45 days of the publication of the decision of the Constitutional Court if, in the meantime, the Parliament or the Government, as the case may be, cannot bring into line the unconstitutional provisions with the provisions of the Constitution. For this limited length of time the provisions found to be unconstitutional shall be suspended de jure. Art. 147 (4): Decisions of the Constitutional Court shall be published in the Official Gazette of Romania. As from their publication, decisions shall be generally binding and effective only for the future (http://www.cdep.ro/pls/dic/site.page?den=act2_2&par1=5#t5c0s0a147).

[34]Art. 148 (2): As a result of the accession, the provisions of the constituent treaties of the European Union, as well as the other mandatory community regulations shall take precedence over the opposite provisions of the national laws, in compliance with the provisions of the accession act. Art. 148 (4) The Parliament, the President of Romania, the Government, and the judicial authority shall guarantee that the obligations resulting from the accession act and the provisions of paragraph (2) are implemented (http://www.cdep.ro/pls/dic/site.page?den=act2_2&par1=6#t6c0s0a148).

[35]Art. 258 TFEU: If the Commission considers that a Member State has failed to fulfil an obligation under the Treaties, it shall deliver a reasoned opinion on the matter after giving the State concerned the opportunity to submit its observations. If the State concerned does not comply with the opinion within the period laid down by the Commission, the latter may bring the matter before the Court of Justice of the European Union.

hoeren@uni-muenster.de

faced with the threat that the European Commission would bring infringement proceedings against it,[36] after more than two years since the RCC decision and the implicit revocation of the Law 298/2008, the Parliament passed a new law for transposing Directive 2006/24/EC (Law 82/2012), in order to avoid a negative decision of the CJEU. But, as a result of the invalidation of the Directive, like all the other Member States, Romania had to repeal the law transposing the Directive 2006/24/EC.

4.3 The Provisions of the New Romanian Retention Law

Although the Law 82/2012 managed to improve in a certain manner some technical provisions previously criticized by the RCC, still did not provide a satisfactory level of protection of individuals' rights as the procedure for obtaining the retained data is not very clearly regulated and was later on declared non-constitutional by the RRC decision.[37]

The New Retention Law no. 235/2015 which represent more of a supplement to the law 506/2004 previously analysed, seeks to regulate access to data held by providers of public networks for electronic communications and providers of electronic communications services. In addition, it aims at providing objective criteria for regulating: the access and use of personal data by public authorities and institutions, in particular the provisions relating to the obligation to obtain prior authorization issued by courts for such access. Previously such authorization by the courts was not required. We need to emphasise that this authorization is different from the one analysed in Sect. 2.2.4.[38]

The Law introduces the concept of 'equipment identification data' in addition to the previously existing concepts of traffic data and location data (both of which have to be retained by the Providers). However, privacy specialists already consider 'equipment identification data'[39] as already included in the obligation to retain traffic and location data. This refers to technical data held by the Providers concerning the localization of the user's communication equipment used by the Providers for the

[36]The European Commission initiated the procedure for the infringement by letter C(2011) 4111 of 16 June 2011, in the case 2011/2089, for not implementing the data retention directive, in which Romania was asked to communicate the measures for national transposition of Directive 2006/24/EC, within two months.

[37]CCR decision 440 from July 2014.

[38]See Bibicu et al. (2015).

[39]1. In Article 2 (1), a new letter, letter b1) shall be inserted after point (b), with the following wording: "b1) equipment identification data – the technical data of the providers of publicly available communications services and of the provider of public electronic communications networks that allow the identification of the location of their communication equipment processed for the purpose of transmitting a communication over a network of electronic communications or for the purpose of invoicing the value of the transaction;"

hoeren@uni-muenster.de

purposes of invoicing, preventing commercial disputes or transmitting communications by way of an electronic communication network.

Thus, the New Retention Law appears to introduce non-clarity to the types of data to be retained by the Providers. Aside from Retained Data, the Providers have no further obligations to use such retained data, except for specific requests made according with the relevant legislation.[40]

The Providers must delete and transform the Retained Data into anonymous when such data is no longer needed, but no later than three years as of the date of the communication (*i.e.*, the date of exchange or transmission of information between users via a publicly available electronic communications service).[41] Retained Data from prepaid users of Providers may be processed only for a period of three (3) years from the date of communication.

An increase in the above period may be requested by courts, prosecution units, national defence and security bodies. Such a request must be accompanied by a notice regarding the necessity of retaining such data for purpose of identifying and conserving evidence (i) during on-going criminal investigations (regardless of the type of criminal offence investigated) or (ii) for national defence and security reasons. In such case, the data cannot be kept by the Providers for more than five (5) years from the date of the request or until the court delivers a final ruling.[42]

Access to Retained Data may be granted only in accordance with the legal restrictions with the prior authorization of the court, in which case the Providers must communicate the requested Retained Data within a maximum of 48 h as of the competent public authorities' request. An exception from the above-mentioned approval conditions and timeframe is provided for state bodies with powers in national security and defence (*e.g.* internal specialized bodies within the Romanian Intelligence Service, the Ministry of National Defence, the Ministry of Justice, the Ministry of internal Affairs), as per the specific legislation in this respect. This approval process was implemented by the Law in response to the Constitutional Court's decision. The Court had criticized the fact that the Previous Retention Law permitted access to Retained Data without a court approval.

Responses to requests for access to Retained Data may be given in hard copy or in electronic format. All requests and responses submitted in electronic format must be signed with a certified electronic signature.[43] This obligation may give rise to certain timing and money wise issues if the Provider does not have the possibility to use a certified electronic signature.

If the Retained Data is given in hard copy, this may result in increased time and costs relating to preparing the information for transfer, transferring it to the requesting entity and reviewing and storing such information. The Providers have a confidentiality obligation when processing requests for access to Retained Data.

[40] See Bibicu et al. (2015).

[41] See article 5 (1).

[42] See Bibicu et al. (2015).

[43] See Bibicu et al. (2015).

hoeren@uni-muenster.de

5 Concluding Remarks

The present research on the legal framework of data protection presented in this paper might offer opportunities and perhaps a more clear view over this issue for policymakers, legislators, data controllers and data protection authority from Romania to fully understand the impact of the new EU legislation. On the other hand it shows that although the protection of personal data is harmonized within the EU regulations, differences still exist in the actual protection of personal data. Furthermore there are still really old provisions, which, combined with the new framework, create some ambiguity in certain situations.

Taking into account the relatively recent entry into force of the new data protection legislative framework Regulation no. 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as Law no. 190/2018 on the measures implementing the Regulation and the lack of a relevant prior practice of the National Supervisory Authority for Personal Data Processing, its relevant guidelines or guidance or the case law of the courts regarding the subject of the analysis, we emphasise that we cannot rely on a practice of Romanian authorities or courts in relation to the subject under consideration and that we cannot rule out different interpretations of them in relation to the legal provisions analysed.

References

Bibicu B, Gabudeanu L, Saftencu R (2015) Impact of new Romanian data retention legislation on providers of electronic communications. Available at https://www.lexology.com/library/detail.aspx?g=28f26ef3-f109-4179-8140-43ca6c7cfa14. Accessed 5 Oct 2018

Custers B et al (2017) A comparison of data protection legislation and policies across the EU. Comput Law Secur Rev 34(2), April 2018, 234–243. Available at https://www.sciencedirect.com/science/article/pii/S0267364917302856. Accessed 5 Oct 2018

Lazar E (2018) La jurisprudence CEDH post Barbulescu dans le contexte de surveillance des employées – évolution et conséquences. NRDO, no. 1/2018. Available at http://revistadrepturileomului.ro/assets/docs/2018_1/NRDO%202018_1_lazar.pdf. Accessed 10 Oct 2018

Sandru DM, Alexe I (2018) The implementation of the General Data Protection Regulation 2016/679. Experience from Romania, in the Legislation of the European Union on Personal Data, University Press, 2018

hoeren@uni-muenster.de

Singapore Report: Data Protection in the Internet

Ee-Ing Ong

1 Introduction

In Singapore, personal data protection is governed by the Personal Data Protection Act 2012 ("PDPA").[1] The PDPA is administered and enforced by the Personal Data Protection Commission ("Commission").[2]

The PDPA is the first comprehensive personal data protection legislation in Singapore.[3] Prior to the PDPA, sector-specific statutes covered aspects of personal data protection in a piecemeal fashion.[4] For instance, the Banking Act states that customer information shall not be disclosed by any bank in Singapore save as provided under such act.[5] However, the sector-specific statutes were "of limited scope and application with regard to data protection" as their provisions "typically penalise the unauthorised release of personal information and are not as far reaching as the provisions of the [PDPA]", nor do they "confer private rights of action or direct remedies that are typically available under data protection laws".[6]

[1] No. 26 of 2012. The data protection provisions came into full effect on 2 July 2014: Personal Data Protection Act 2012 (Commencement) Notification 2014 (S 361 of 2014).

[2] PDPA s 5, 6(*g*).

[3] Singapore Parliamentary Debates, Official Report (15 October 2012) vol 89. See also Chesterman (2018), para 2.30.

[4] Chesterman (2018), para 2.30.

[5] Cap 19, 2008 Rev Ed at s 47(1).

[6] Ter (2013), p. 265.

E.-I. Ong (✉)
Singapore Management University School of Law, Singapore, Singapore
e-mail: eeingong@smu.edu.sg

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_13

hoeren@uni-muenster.de

The PDPA is intended to be aligned with international standards on data protection.[7] At the same time, however, it presents a "light touch" regime which establishes a "minimum data protection standard".[8] In the event of a conflict, other laws shall prevail over the PDPA.[9]

Other key statutes which affect personal data are also discussed in this report:

- Computer Misuse Act ("CMA")[10];
- Criminal Procedure Code ("CPC")[11];
- Cybersecurity Act[12];
- Electronic Transactions Act ("ETA")[13];
- Protection from Harassment Act ("POHA")[14];
- Protection from Online Falsehoods and Manipulation Act 2019 ("POFMA")[15];
- Public Sector (Governance) Act 2018 ("PS(G)A")[16];
- Spam Control Act ("SCA")[17]; and
- Telecommunications Act.[18]

2 General Data Protection Framework

2.1 Overview

The PDPA governs the collection, use and disclosure of personal data, in any form, by *organisations*, in a manner that balances the "right of individuals to protect their personal data" with the "need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances".[19]

[7] Singapore Parliamentary Debates, Official Report (15 October 2012) vol 89. See also Chesterman (2018), para 2.47.

[8] Chik (2013), p. 558 (discussing PDPA s 4(6)).

[9] Chik (2013), p. 558 (discussing PDPA s 4(6)).

[10] Cap 50A, 2007 Rev Ed.

[11] Cap 68, 2012 Rev Ed.

[12] No 9 of 2018.

[13] Cap 88, 2011 Rev Ed.

[14] Cap 256A, 2015 Rev Ed.

[15] No 18 of 2019.

[16] No 5 of 2018.

[17] Cap 311A, 2008 Rev Ed.

[18] Cap 323, 2000 Rev Ed.

[19] PDPA s 3. There is no specific right of privacy in Singapore, although the usual common law protections for privacy apply, *e.g.* the law of confidence and defamation. See Chan and Lee (2016). Certain privacy-related rights also exist under other legislation such as the Protection from Harassment Act (Cap 256A, 2015 Rev Ed) and the Copyright Act (Cap 63, 2006 Rev Ed). See Goh and Aw (2018).

hoeren@uni-muenster.de

The PDPA covers *all* personal data, whether in electronic or other form.[20] "Personal data" means "data (whether true or not) about an individual who can be identified (a) from that data; or (b) that data and other information to which the organisation has or is likely to have access".[21] However, the PDPA does not apply to: personal data about an individual in a record that has existed for at least 100 years[22]; data about a deceased individual[23]; business contact information[24]; and anonymised data.[25]

The PDPA focuses on organisations. An "organisation" is broadly defined, and includes any "individual, company, association or body of persons" whether or not formed under Singapore law, or resident, or having a place of business in Singapore.[26] The PDPA generally *excludes*: individuals acting in a personal or domestic capacity; public agencies (including the Singapore Government and governmental organisations)[27]; and employees acting in the course of their employment.[28] Some exceptions also apply for data intermediaries, which are organisations, which process personal data on behalf of other organisations.[29]

2.2 Obligations

Organisations Under the PDPA, there are ten general categories of data protection, each an "Obligation" on an organisation:

- *Consent*: No collection, use, or disclosure of personal data about an individual without that individual's consent as obtained through specified procedures (see Sect. 2.2.1).[30]

[20]PDPC Advisory Guidelines on Key Concepts paras 5.2, 5.30.

[21]PDPA s 2(1).

[22]PDPA s 4(4)(*a*).

[23]PDPA s 4(4)(*b*). The individual must have been deceased for more than 10 years.

[24]PDPA s 4(5).

[25]PDPC Advisory Guidelines on Key Concepts para 5.3; Advisory Guidelines for Selected Topics chapter 3.

[26]PDPA s 2(1).

[27]The Singapore Government and governmental organisations (and employees thereof) are prohibited from disclosing confidential information obtained in the course of their work by, among others, the Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap 319, 2004 Rev Ed) and the Official Secrets Act (Cap 213, 2012 Rev Ed). See also discussion on the Public Sector (Governance) Act 2018.

[28]PDPA s 4(1)(*b*).

[29]PDPA s 2(1). Data intermediaries are discussed elsewhere in this report.

[30]PDPA ss 13–16.

hoeren@uni-muenster.de

- *Limited Purpose*: Collection, use or disclosure of personal data only for purposes that a reasonable person would consider appropriate and if the individual has been notified of such purposes (see Sect. 2.2.2).[31]
- *Notification*: To inform an individual of the purpose of the collection, use or disclosure of personal data.[32] Most recently, there has been a proposal for deemed consent by notification (see Sect. 2.2.1).
- *Access*: To give an individual access to personal data held by or under the control of the organisation, including information about how such personal data was or may have been used or disclosed within a year before the date of the request (see Sect. 2.2.3).[33]
- *Correction*: To correct an error or omission regarding personal data about that individual (see Sect. 2.2.4).[34]
- *Accuracy*: To ensure that personal data collected by or on behalf of the organisation is accurate and complete (see Sect. 2.2.4).[35]
- *Protection:* To protect personal data in the organisation's possession or under its control through reasonable security arrangements (see Sect. 3.1).[36]
- *Limited Retention*: To stop retaining personal data as soon as it is reasonable to assume that the purpose for which the data was collected is no longer served by such retention and retention is no longer necessary for legal or business purposes (see Sect. 2.2.5).[37]
- *Limited Transfer*: No transfer of personal data outside Singapore, unless the transferred personal data will enjoy protection comparable to the protections under the PDPA (see Sect. 4.2).[38]
- *Accountability*: To implement data protection policies and practices, make information about its policies and procedures publicly available, and appoint a data protection officer (see Sect. 2.2.6).[39]

There are no specified standards for the Obligations. Instead, organisations may collect, use and disclose data "for purposes which a reasonable person would consider appropriate in the circumstances".[40] A "reasonable person" is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgement in the particular circumstances.[41]

[31]PDPA s 18.
[32]PDPA s 20(1).
[33]PDPA s 21(1).
[34]PDPA s 22.
[35]PDPA s 23.
[36]PDPA s 24.
[37]PDPA s 25.
[38]PDPA s 26.
[39]PDPA ss 11–12, PDPC Advisory Guidelines on Key Concepts para 10.2.
[40]PDPC Advisory Guidelines on Key Concepts para 9.3. See, *e.g.*, PDPA ss 11(1), 18, 24, 25.
[41]PDPC Advisory Guidelines on Key Concepts para 9.5.

hoeren@uni-muenster.de

Government Agencies Data sharing by Singapore government agencies is governed under the *Public Sector (Governance) Act 2018* or PS(G)A[42] (and not the PDPA). The PS(G)A is intended to be in alignment with the PDPA, including to "significantly improve the protection and safeguard of such shared data".[43] Under this act, where a "data sharing direction"[44] is given, a Singapore public sector agency is generally authorised to share information under its control with another Singapore public sector agency.[45] However, such direction must not be inconsistent with any other written law.[46]

2.2.1 Consent

At present, the PDPA remains largely a consent-based regime (although this may evolve over time).[47] Organisations may not collect, use or disclose an individual's personal data unless the individual has given, or is deemed to have given, his consent (save for the exceptions discussed below).[48] And an individual has not given consent unless he/she has been notified of the purposes of the collection, use or disclosure of the personal data; has given consent for such purposes; and has been provided (on request) with the business contact information of a person who can answer the individual's questions about the collection, use or disclosure of the personal data.[49]

An organisation collecting personal data about an individual from another organisation without the individual's consent shall provide such other organisation with sufficient information regarding the purpose of such collection, to allow such other organisation to determine if the disclosure would be in accordance with the PDPA.[50]

The PDPA does not prescribe the manner of obtaining consent, although it is "good practice" to obtain written consent.[51] However, an organisation shall not

[42]See n 16. The PSG(A) will likely be administered by the Prime Minister's Office. See Public Consultation on the Public Sector (Governance) Bill. https://www.reach.gov.sg/participate/public-consultation/prime-ministers-office/public-service-division/public-consultation-on-the-public-sector-governance-bill. Accessed 30 August 2019. Media Factsheet On The Public Sector (Governance) Bill. http://www.nas.gov.sg/archivesonline/data/pdfdoc/20180108011/Media%20factsheet%20on%20the%20Public%20Sector%20-%20Governance-%20Bill.pdf. Accessed 30 August 2019.

[43]Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.

[44]"Data sharing direction" means a direction issued under the PS(G)A regarding "sharing of information or re-identification of anonymised information under the control of a Singapore public sector agency". PS(G)A s 2(1).

[45]PS(G)A s 6(1).

[46]PS(G)A s 11(1).

[47]See *e.g.* Chesterman (Introduction) (2018), paras 1.6–1.8; Tan (2018), para 5.12.

[48]PDPA s 13.

[49]PDPA s 14(1) read with s 20(1).

[50]PDPA s 20(2).

[51]PDPC Advisory Guidelines on Key Concepts para 12.5.

hoeren@uni-muenster.de

require consent as a condition of providing a product or service "beyond what is reasonable to provide the product or service", or obtain consent by providing "false or misleading information" or "using deceptive or misleading practices".[52] Indeed, consent obtained under such circumstances is invalid.[53]

Factors in determining whether it is reasonable for an organisation to require consent as such a condition of providing a product or service include: the amount and type of personal data sought; the purpose of the collection, use or disclosure of the personal data; the nature of the item being provided, including whether there is any benefit tied to the item (*e.g.* whether the item is being provided without monetary payment to the organisation); and what a reasonable person would consider appropriate in the circumstances.[54]

When Consent Is Not Required Consent is not required if: (a) the individual is deemed to have given consent; or (b) an exception applies.[55]

(a) Deemed Consent. An individual is deemed to have consented to the collection, use or disclosure of his/her personal data for a purpose if the individual voluntarily provides such data to the organisation for that purpose, and it is reasonable that the individual would voluntarily provide the data.[56] Additionally, if the individual gives (or is deemed to give) consent for disclosure of his/her personal data by one organisation to another organisation for a particular purpose, he/she is deemed to consent to the collection, use or disclosure of such data for such purpose by that other organisation.[57]

Pursuant to a public consultation in July 2017, there will be an additional category of consent termed *"Deemed Consent by Notification"*.[58] This will be allowed where:

- the organisation notifies individuals of the purpose of collecting, using and disclosing their data;
- the individual is provided a reasonable time period to opt-out but does not opt-out within the time period; and

[52]PDPA s 14(2).

[53]PDPA ss 14(2)-(3).

[54]PDPC Advisory Guidelines on Requiring Consent for Marketing Purposes para 5.2. For example, "organisations may provide offers, discounts or lucky draw opportunities to individuals that are conditional on the collection, use or disclosure of their personal data for specified purposes". PDPC Advisory Guidelines on Requiring Consent for Marketing Purposes para 7.2.

[55]PDPA s 13.

[56]PDPA s 15(1).

[57]PDPA s 15(2). For instance, if an individual booking a taxicab is asked for his/her name and telephone number in order to inform him/her of the taxicab number, and the individual voluntarily provides such information, then the individual is deemed to have consented to the taxicab company using his/her name and number to notify him/her when the taxicab arrives. However, the individual is not deemed to have consented to the use of his/her name and number for other purposes, *e.g.* the marketing of a limousine service run by the cab company. PDPC Advisory Guidelines on Key Concepts para 12.24.

[58]Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy Part II.

hoeren@uni-muenster.de

- such collection, use or disclosure is not likely to have any adverse impact on the individuals.[59]

However, the organisation must also conduct a risk and impact assessment, such as a data protection impact assessment, to ascertain whether such collection, use or disclosure is likely to have any adverse impact on the individual.[60]

(b) Exceptions. Consent is not required if the collection, use or disclosure of data is: necessary for any purpose that is "clearly in the interests of the individual" and if consent cannot be obtained in a timely manner or the individual would not reasonably be expected to withhold consent[61]; for an emergency threatening the life, health or safety of any individual[62]; for personal data which is publicly available[63]; in the national interest[64] or necessary for investigation or proceedings[65]; necessary for evaluative purposes[66]; or necessary to recover debt owed from an individual to the organisation or vice versa,[67] or to provide or obtain legal services.[68] Other exceptions apply, *e.g.* regarding personal data for business asset transactions[69]; credit bureaus[70]; employment purposes[71]; news activities[72]; and research purposes.[73]

Pursuant to a public consultation in July 2017, there will be an additional exception for *"Legitimate Interests"*.[74] Organisations will be able to collect, use or disclose personal data where there is a need to protect legitimate interests that will have economic, social, security or other benefits, so long as the benefits to the public clearly outweigh any adverse impact to the individuals involved.[75] Organisations wishing to use this exception will also need to conduct a risk and impact assessment

[59]Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy Part II.

[60]Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy para 4.2.

[61]PDPA Second Schedule s 1(*a*), Third Schedule s 1(*a*), Fourth Schedule s 1(*a*) (save that there is no requirement for disclosure that the individual not reasonably be expected to withhold consent).

[62]PDPA Second Schedule s 1(*b*), Third Schedule s 1(*b*), Fourth Schedule ss 1(*b*)-(*c*).

[63]PDPA Second Schedule s 1(*c*), Third Schedule s 1(*c*), Fourth Schedule s 1(*d*).

[64]PDPA Second Schedule s 1(*d*), Third Schedule s 1(*d*), Fourth Schedule s 1(*e*).

[65]PDPA Second Schedule s 1(*e*), Third Schedule s 1(*e*), Fourth Schedule s 1(*f*).

[66]PDPA Second Schedule s 1(*f*), Third Schedule s 1(*f*), Fourth Schedule s 1(*h*).

[67]PDPA Second Schedule s 1(*i*), Third Schedule s 1(*g*), Fourth Schedule s 1(*i*).

[68]PDPA Second Schedule s 1(*j*), Third Schedule s 1(*h*), Fourth Schedule s 1(*j*).

[69]PDPA Second Schedule s 1(*p*), Third Schedule 1(*j*), Fourth Schedule s 1(*p*).

[70]PDPA Second Schedule s 1(*k*), Third Schedule 1(*j*), Fourth Schedule s 1(*k*).

[71]PDPA Second Schedule s 1(*o*), Third Schedule 1(*j*), Fourth Schedule s 1(*s*). See also Sect. 3.5.

[72]PDPA Second Schedule s 1(*h*), Third Schedule s 1(*j*), Fourth Schedule s 1(*s*).

[73]PDPA Third Schedule s 1(*i*), Third Schedule s 1(*j*), Fourth Schedule s 1(*s*).

[74]Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy Part II.

[75]Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy Part II.

hoeren@uni-muenster.de

to determine whether the benefits outweigh any foreseeable adverse impact to the individual.[76] While the term "Legitimate Interests" tracks the language adopted in the EU's General Data Protection Regulation, the Commission will provide its own guidelines on the term.[77]

Withdrawing Consent An individual may at any time, with reasonable notice, withdraw consent given or deemed given.[78] The organisation shall inform the individual of the likely consequences of such action, but without prohibiting him/her from such action. However, such withdrawal shall not affect any legal consequences from such withdrawal.[79]

Upon withdrawal, the organisation shall also cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing such personal data, subject to exceptions under the PDPA or other law.[80] Withdrawal of consent does not require deletion or destruction of the individual's personal data, save as required under the Limited Retention Obligation (see Sect. 2.2.5).[81]

2.2.2 Limited Purpose

An organisation may collect, use or disclose personal data about an individual only for purposes that "a reasonable person would consider appropriate in the circumstances" and of which the individual has been notified.[82] A purpose that is in violation of law or which would be harmful to the individual concerned is unlikely to be considered appropriate by a reasonable person.[83]

[76]Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy Part II.

[77]Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy (para 5.6).

[78]PDPA s 16(1).

[79]PDPA ss 16(2)-(3). For example, a telecoms service provider provides subscriber services requiring the collection, use and disclosure of personal data. The subscriber provides consent to the above but subsequently withdraws it. Such withdrawal will result in the operator being unable to provide said services, *i.e.* early termination of the service contract; thus the operator should inform the individual of the consequences, *i.e.* incurrence of early termination charges. PDPC Advisory Guidelines on Key Concepts para 12.45. Additionally, where an organisation provides a facility for individuals to withdraw consent, *e.g.* by clicking on an "unsubscribe" link within an e-mail, the organisation should indicate the scope of such withdrawal. For instance, a statement that "[y]ou have unsubscribed successfully from e-mail marketing messages from ABC" means that the individual has only withdrawn consent to marketing messages sent by e-mail, and not by fax. PDPC Advisory Guidelines on Key Concepts para 12.48.

[80]PDPA s 16(4).

[81]PDPA s 16(4); PDPC Advisory Guidelines on Key Concepts para 12.55.

[82]PDPA s 18 read with s 20.

[83]PDPC Advisory Guidelines on Key Concepts para 13.4.

hoeren@uni-muenster.de

2.2.3 Access

An organisation shall provide, on an individual's request: personal data about the individual in the organisation's possession or control; and information about the ways in which such data has or may have been used or disclosed by the organisation within a year before the date of the request.[84] An organisation can charge reasonable fees for access.[85]

Exceptions Access shall not be provided if provision of that data or information could reasonably be expected to: threaten the safety or physical or mental health of another individual; cause immediate or grave harm to the safety or physical or mental health of another individual; reveal personal data about another individual; reveal the identity of an individual who has provided personal data about another individual and the former does not consent to disclosure of his/her identity; or be contrary to the national interest.[86] An organisation shall also not inform an individual that it has disclosed personal data to a law enforcement agency, if such disclosure was made without that individual's consent (as allowed under the Fourth Schedule of the PDPA or other law).[87]

Access is also not required regarding, *e.g.* opinion data kept solely for an evaluative purpose; school examinations; personal data subject to legal privilege; personal data collected, used or disclosed without consent for the purposes of an investigation in progress; "confidential commercial information" that could, in the opinion of a reasonable person, harm the organisation's competitive position; and repetitious requests "that would unreasonably interfere with the operations of an organisation".[88]

However, access shall be given to an individual's personal data and information if such data or information can be stripped of the abovementioned prohibited data and information.[89]

2.2.4 Correction

An individual may request an organisation to correct an error or omission in his/her personal data in the possession or control of the organisation.[90] Unless the organisation is "satisfied on reasonable grounds" that a correction should not be made (in which case it shall annotate the personal data with the correction that was

[84]PDPA s 21(1).

[85]Personal Data Protection Regulations 2014 (S 362 of 2014) s 7(1). See also PDPC Advisory Guidelines on Key Concepts para 15.19.

[86]PDPA s 21(3).

[87]PDPA s 21(4).

[88]PDPA Fifth Schedule s 1.

[89]PDPA s 21(5).

[90]PDPA s 22(1).

hoeren@uni-muenster.de

requested but not made),[91] it shall correct the data and send it to "every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made".[92] Fees may not be charged for such correction.[93]

Exceptions An organisation need not correct an opinion, including a professional or expert opinion.[94] Correction is also not required regarding, *e.g.* opinion data kept solely for evaluative purposes; school examinations; and documents related to a prosecution if proceedings have not been completed.[95]

2.2.5 Limited Retention

Organisations must cease retaining personal data as soon as it is "reasonable" to assume that the purpose for which the personal data was collected is no longer served by such retention, and retention is no longer necessary for legal or business purposes.[96] Thus, an organisation may not retain data "just in case" the data may be needed for other purposes.[97]

An organisation ceases to retain documents containing personal data when it, its agents and its data intermediaries no longer have access to those documents and the personal data they contain, *e.g.* by destroying the documents or anonymizing the data.[98] Documents should be "completely irretrievable or inaccessible" to the organisation.[99] Data in electronic form which is archived or to which access is limited is still considered retained.[100]

Factors to consider in determining whether an organisation has ceased to retain personal data are: whether the organisation has any intention to use or access the personal data; the effort and resources needed to use or access the personal data again; whether third parties have been given access to that personal data; and whether the organisation has made a reasonable attempt to destroy, dispose of or delete the personal data in a permanent and complete manner.[101]

---

[91] PDPA s 22(2) read with s 22(5).

[92] PDPA s 22(2).

[93] PDPC Advisory Guidelines on Key Concepts para 15.39.

[94] PDPA s 22(6).

[95] PDPA Sixth Schedule s 1.

[96] PDPA s 25.

[97] PDPC Advisory Guidelines on Key Concepts para 18.4.

[98] PDPC Advisory Guidelines on Key Concepts para 18.10.

[99] PDPC Advisory Guidelines on Key Concepts para 18.12.

[100] PDPC Advisory Guidelines on Key Concepts para 18.11.

[101] PDPC Advisory Guidelines on Key Concepts para 18.13. See, *e.g.*, *Orchard Turn Developments Pte. Ltd.* [2017] SGPDPC 12 (failure to purge personal data from server led to data breach; retention of data was also unnecessary); *Social Metric Pte Ltd* [2017] SGPDPC 17 (company penalised for, in part, failure to cease retaining personal data); *Jade E-Services Singapore Pte. Ltd.* [2018] SGPDPC 21 (company should not have taken the risk of allowing webpages with personal data to be cached for display).

hoeren@uni-muenster.de

2.2.6 Accountability

This obligation, previously called the "Openness" obligation, was recently amended to incorporate the concept of "Accountability". This refers to how an organisation discharges its responsibility for personal data which it has collected or obtained for processing, or which it has control over. Accountability requires organisations to not only take measures to meet their PDPA obligations, but also to demonstrate that they can meet their obligations when required. These measures include appointing a data protection officer, developing and implementing appropriate data protection policies and practices, and making information about such policies and practices available.[102] This also signals a shift from a compliance-based approach to an accountability-based approach in managing personal data.[103]

2.3 Supervising Authority

The PDPA is administered and enforced by the Commission. The Commission is overseen by the Info-communications Media Development Authority ("IMDA"), and the IMDA in turn comes under the Ministry of Communications and Information.[104]

The Commission may conduct investigations regarding alleged non-compliance of the PDPA,[105] including requiring documents and information, inspecting premises,[106] and imposing certain remedies and sanctions.[107] The Commission shall also: promote awareness of data protection in Singapore; provide advisory services (including to the Singapore Government) regarding data protection; conduct research and educational activities regarding data protection; and manage technical co-operation regarding data protection with foreign, international, and governmental authorities.[108]

[102]PDPC Advisory Guidelines on Key Concepts para 20.1.

[103]PDPC Guide to Accountability under the PDPA.

[104]MCI (2019) Agencies. https://www.mci.gov.sg/agencies. Accessed 30 August 2019.

[105]PDPA s 50.

[106]PDPA Ninth Schedule.

[107]PDPA s 29. See also Sect. 3.10.

[108]PDPA s 6.

hoeren@uni-muenster.de

Finally, the Commission has issued a large number of advisory guidelines on the PDPA[109]: general guidelines, sector-specific guidelines, and guidelines on specific topics. For instance, there are guidelines regarding the protection of personal data for the healthcare,[110] education,[111] social services,[112] and real estate[113] sectors. There are also guidelines on managing data breaches[114] and securing personal data in electronic medium.[115] While these guidelines are not legally binding,[116] they are carefully studied by other government agencies,[117] lawyers,[118] and industry players.[119]

The guidelines are also updated from time to time. For instance, the Commission recently held a public consultation on "Approaches to Managing Personal Data in the Digital Economy", and the results will be implemented in 2018–2019.[120]

2.4 Self-Regulation Instruments

Various industries have incorporated aspects of the PDPA (including the advisory guidelines) into their codes of conduct and industry guides. This includes the Life

[109]PDPC Guidelines.

[110]PDPC Advisory Guidelines for the Healthcare Sector.

[111]PDPC Advisory Guidelines for the Education Sector.

[112]PDPC Advisory Guidelines for the Social Service Sector.

[113]PDPC Advisory Guidelines for the Real Estate Agency Sector.

[114]PDPC Guide to Managing Data Breaches 2.0.

[115]PDPC Guide to Securing Personal Data in Electronic Medium.

[116]PDPC Introduction to the Guidelines para 3.1.

[117]See *e.g.*, Cyber Security Agency of Singapore "PDPC Guides" https://www.csa.gov.sg/gosafeonline/resources/pdpc-guides. Accessed 30 August 2019.

[118]See *e.g.*, Hogan Lovells' report "New PDPC guidance on data management practices in Singapore". https://www.hoganlovells.com/en/publications/new-pdpc-guidance-on-data-management-practices-in-singapore. Accessed 30 August 2019. CNP Law's report on "Personal Data Protection Committee issues sector specific advisory guidelines". https://www.cnplaw.com/personal-data-protection-committee-issues-sector-specific-advisory-guidelines/. Accessed 30 August 2019.

[119]See *e.g.*, the Singapore Council for Estate Agencies' website which contains links to the relevant advisory guidelines, and which encourages property agencies and agents to familiarise themselves with these and other PDPC advisory guidelines. https://www.cea.gov.sg/legislation-guidelines/practice-guidelines-circulars/personal-data-protection. Accessed 30 August 2019. "Singapore: PDPC data management guides 'emphasize accountability'". https://www.dataguidance.com/singapore-pdpc-issues-guides-emphasising-accountability-data-management/. Accessed 30 August 2019. "Personal Data Protection Commission issues advisory guidelines on in-vehicle recording". https://www.opengovasia.com/articles/personal-data-protection-commission-issues-advisory-guidelines-on-in-vehicle-recording. Accessed 30 August 2019.

[120]PDPC Public Consultation for Approaches to Managing Personal Data in the Digital Economy; PDPC Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy.

hoeren@uni-muenster.de

Insurance Association Singapore ("LIA")[121] and The Association of Banks in Singapore ("ABS").[122]

3 Personal Data Processed by Electronic Means

3.1 Services Provided at a Distance

PDPA As stated previously, the PDPA covers all personal data, whether in electronic or other form.[123] The PDPA states that an organisation "shall protect personal data in its possession or ... control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks".[124] The Commission's guidelines reiterate the need to adopt arrangements which are reasonable under the circumstances.[125]

For instance, an organisation should ensure that its security arrangements "fit the nature of the personal data held ... and the possible harm that might result from a security breach"; "identify reliable and well-trained personnel"; "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity"; and "be prepared and able to respond to information security breaches promptly and effectively".[126] Thus in *My Digital Lock Pte Ltd*,[127] the Commission stated that "[r]easonable ... security arrangements when transferring personal data" requires a process where "the personal data is reasonably protected from unauthorised access or interference, until the personal data reaches its intended destination or recipient where other security arrangements on storage would apply".

Guidelines have also been issued in this regard, concerning: the security and protection of personal data stored in electronic medium; good practices for protecting electronic personal data; and enhanced practices that may be adopted.[128]

---

[121]Life Insurance Association Singapore (2015) MU61/15—LIA Code of Practice for Life Insurers on the Singapore Personal Data Protection Act (No. 26 of 2012). https://www.lia.org.sg/media/1229/mu-6115-code-of-practice-on-pdpa.pdf. Accessed 30 August 2019. Life Insurance Association Singapore (2015) MU 62/15—LIA Code Of Conduct For Tied Agents Of Life Insurers On The Singapore Personal Data Protection Act (No. 26 of 2012). https://www.lia.org.sg/media/1230/mu-6215-code-of-conduct-on-pdpa.pdf. Accessed 30 August 2019.

[122]The Association of Banks in Singapore (2015) Code of Banking Practices – The Personal Data Protection Act ("PDPA"). https://abs.org.sg/docs/library/abs-code-banking-practices-pdpa.pdf. Accessed 30 August 2019.

[123]PDPC Advisory Guidelines on Key Concepts paras 5.2, 5.30.

[124]PDPA s 24.

[125]PDPC Advisory Guidelines on Key Concepts para 17.2.

[126]PDPC Advisory Guidelines on Key Concepts para 17.3.

[127][2016] SGPDPC 20 at [25].

[128]PDPC Guide to Securing Personal Data in Electronic Medium para 2.3.

hoeren@uni-muenster.de

For instance, organisations should ensure that computer networks are secure, and personal data encrypted.[129] They should consider, as part of good governance: accountability; standards, policies and procedures; risk management; and classification and tracking of personal data.[130] They should also educate employees on potential threats to, and protection measures for, personal data.[131]

There are also guidelines on preventing accidental disclosure of personal data, including: automating the processing of documents containing personal data and checking these systems regularly; ensuring additional checks following the processing, printing and sorting of documents to ensure that the destination information is correct and matches that of the intended recipient; and establishing a policy for sending compiled sets of personal data of different individuals (*e.g.* through spreadsheets).[132] The use of passwords for documents containing personal data, as well as regular staff training on proper data protection procedures, is also encouraged.[133]

These guidelines reflect the approach taken in several cases decided by the Commission. For instance, in *The Institution of Engineers Singapore*[134] ("IES"), there was a breach of personal data of IES members stored on the organisation's website. While a number of measures had been taken to secure the site, including use of a firewall and anti-virus software, up-to-date software, and limited administrative access, the Commission found the following flaws: no encrypted storage of member passwords; no security audit on the website; no penetrating testing; and no specific arrangements with the website vendors to put in place security measures to safeguard personal data stored on the website.[135] In addition, there were common vulnerabilities with the website (including cross-site scripting); these could have been easily detected through the performance of a vulnerability scan, which was also an industry best practice.[136]

Based on case law, factors that the Commission has taken into account regarding reasonable protection of personal data conveyed and stored through electronic means include[137]: failure to audit systems, carry out penetration tests and test website vulnerabilities[138]; use of outdated software and/or failure to recognise

[129]PDPC Guide to Securing Personal Data in Electronic Medium paras 9.1, 10.3.

[130]PDPC Guide to Securing Personal Data in Electronic Medium para 4.1.

[131]PDPC Guide to Securing Personal Data in Electronic Medium paras 5.1–5.2.

[132]PDPC (2017) Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data pp. 3–4.

[133]Guide to Preventing Accidental Disclosure p. 5.

[134][2016] SGPDPC 02.

[135][2016] SGPDPC 02 at [29]-[30], [33].

[136][2016] SGPDPC 02 at [31]-[32].

[137]See Woon CY (2016) Personal Data Protection Act – Obligation to Protect and Secure Data, and What to Do in Case of Breach. https://dentons.rodyk.com/en/insights/alerts/2016/november/8/personal-data-protection-act-obligations-to-protect-and-secure-data-and-what-to-do-in-case-of-breach. Accessed 30 August 2019.

[138]See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01.

hoeren@uni-muenster.de

vulnerabilities associated with software or hardware[139]; failure to address common website vulnerabilities such as SQL injection vulnerabilities[140] and cross-site scripting[141]; use of the auto-fill function[142]; failure to remove unused user accounts or pages, or limit access to website administration[143]; failure to use encryption and/or strong passwords (or any passwords at all)[144]; and failure to exercise reasonable control of information on the organisation's website.[145]

Other factors (which seem equally applicable to non-electronic data breaches) include: whether personal data was in fact disclosed and, if so, the number of individuals whose personal data was disclosed[146] and the sensitivity of the data involved[147]; and failure to implement adequate data protection procedures and policies (including appointing a data protection officer).[148] Finally, the Commission also considers whether: prompt remedial action was taken[149]; the affected parties were notified of the breach[150]; and if the organisation was cooperative and forthcoming during the Commission's investigations.[151]

In this regard, Singapore suffered its largest cyberattack in July 2018: hackers stole the personal particulars of 1.5 million patients, and the outpatient prescription records of nearly 160,000 patients, from Singapore Health Services Pte Ltd's patient

[139] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Institution of Engineers* [2016] SGPDPC 02.

[140] See *Metro Pte Ltd* [2016] SGPDPC 07.

[141] See *Institution of Engineers* [2016] SGPDPC 02.

[142] See *Full House Communications Pte Ltd* [2016] SGPDPC 08.

[143] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Fei Fah Medical Manufacturing Pte. Ltd.* [2016] SGPDPC 03; *Social Metric Pte Ltd* [2017] SGPDPC 17.

[144] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Institution of Engineers* [2016] SGPDPC 02; *My Digital Lock Pte Ltd* [2016] SGPDPC 20; *Fu Kwee Kitchen Catering Services* [2016] SGPDPC 14; *Smiling Orchid* [2016] SGPDPC 19; *The Cellar Door Pte Ltd* [2016] SGPDPC 22.

[145] *Watami Food Service Singapore Pte Ltd* [2018] SGPDPC [12].

[146] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Institution of Engineers* [2016] SGPDPC 02; *Aviva Ltd* [2016] SGPDPC 15; *Comfort Transportation Pte Ltd* [2016] SGPDPC 17.

[147] See *Aviva Ltd* [2016] SGPDPC 15; *Central Depository (Pte) Limited* [2016] SGPDPC 11; *Challenger Technologies Limited* [2016] SGPDPC 06.

[148] See, *e.g.*, *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Fu Kwee Kitchen Catering Services* [2016] SGPDPC 14; *National University of Singapore* [2017] SGPDPC 05; *Tiger Airways Singapore Pte Ltd* [2017] SGPDPC 06; *M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15.

[149] See *Central Depository (Pte) Limited* [2016] SGPDPC 11; *Challenger Technologies Limited* [2016] SGPDPC 06; *Spear Security Force Pte. Ltd.* [2016] SGPDPC 12; *ABR Holdings Limited* [2016] SGPDPC 16.

[150] See *Institution of Engineers* [2016] SGPDPC 02.

[151] See *Institution of Engineers* [2016] SGPDPC 02; *Fei Fah Medical Manufacturing Pte. Ltd.* [2016] SGPDPC 03; *Yes Tuition Agency* [2016] SGPDPC 05; *Singapore Computer Society* [2016] SGPDPC 09; *Central Depository (Pte) Limited* [2016] SGPDPC 11; *Singapore Management University Alumni Association* [2018] SGPDPC 6.

hoeren@uni-muenster.de

database system.[152] A number of public hearings were held to investigate the breach.[153] The Commission eventually imposed an aggregate financial penalty of $1,000,000 SGD on the two organisations involved.[154] It found several failings, including: staff who fell prey to phishing attacks; easily deduced administrator passwords; failure to apply a systems patch; and an ineffective IT security-incident team.[155] This incident may result in further changes to the rules and guidelines on electronic data protection in Singapore.

PS(G)A: Data Processing Data shared under the PS(G)A will be "for analysis and to develop policies and programmes".[156] Such data will be anonymised and aggregated.[157] As such, "centralised data custodians" will be set up where "raw data from different sources will be matched and anonymised, before being released to relevant agencies for analysis".[158] Moreover, the user of the data will also be held "accountable for the protection and safeguarding of data passed to" it.[159] Unauthorised disclosure and improper use of information shared under the PS(G)A will be punished,[160] as will "unauthorised re-identification of anonymised information".[161] Public servants' access to data will also be prescribed based on security clearance and legitimate need.[162]

3.2 Personal Data on Computers

Singapore also has specific laws involving the investigation of personal data on computers (including web-based servers).

[152]Tham I (2018). Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyberattack. In: The Straits Times. https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most. Accessed 30 August 2019.

[153]*Singapore Health Services Pte Ltd* [2019] SGPDPC 03. Tham I (2018). Hearings on SingHealth cyber breach from Sept 21. In: The Straits Times. https://www.straitstimes.com/singapore/hearings-on-singhealth-cyber-breach-from-sept-21. Accessed 30 August 2019.

[154]*Singapore Health Services Pte Ltd* [2019] SGPDPC 03. The financial penalties imposed against the two organisations involved are, individually, the highest ($750,000 SGD) and second highest ($250,000 SGD) financial penalty amounts imposed by the Commission to date.

[155]*Singapore Health Services Pte Ltd* [2019] SGPDPC 03.

[156]Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.

[157]Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.

[158]Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.

[159]Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.

[160]PS(G)A s 7.

[161]PS(G)A s 8.

[162]Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94. Seow J (2018) New law on data sharing among govt agencies. In: The Straits Times. http://www.straitstimes.com/singapore/new-law-on-data-sharingamong-govt-agencies. Accessed 30 August 2019.

hoeren@uni-muenster.de

Under recent amendments to the Criminal Procedure Code or CPC,[163] the authorities' computer-related powers of investigation were enhanced. Investigators can, as part of an investigation:

- inspect and search, in and from Singapore, any data stored on or available to a computer implicated in the investigation, regardless of whether such computer is inside or outside Singapore (thus this could include web-based email accounts and web storage accounts);
- order a person to provide login information such as usernames and passwords, to gain access to a computer under investigation; and
- prevent a person from accessing a computer or account by changing a password or by other means.[164]

The Computer Misuse Act or CMA[165] also involves personal data on computers. It is an offence to obtain, retain, supply, transmit or make available "personal information" obtained in violation of offences under the CMA.[166] The definition of "personal information" would appear to involve personal data, as it includes:

> any information, whether true or not, about an individual of a type that is commonly used alone or in combination with other information to identify . . . an individual, including . . . biometric data, name, address, date of birth, national registration identity card number. . .[167]

Additionally, personal data located on computers may be affected by the Cybersecurity Act.[168] Under this Act, the relevant authorities may take measures with regard to computers and computer systems which are deemed "critical information infrastructure"[169] and/or affected by cyber security incidents,[170] including scanning the relevant computers for cyber security vulnerabilities.[171] This includes requiring information concerning a computer or computer system (including any data therein) to determine if it is a "critical information infrastructure" ("CII").[172] If there is a cyber security incident, the Commissioner may also take investigatory steps,

[163] See n 11.

[164] CPC s 39(1). See also Singapore Parliamentary Debates, Official Report (19 March 2018) vol 94: "Many people now use web-based email accounts or web storage accounts. Technically, such data may reside in computers outside Singapore, even if the data is accessed from within Singapore. Applicable laws in other countries will be duly considered when such powers are exercised".

[165] See n 10.

[166] CMA s 8A(1). Offences include: causing a computer to perform any function to secure unauthorised access to computer material (CMA s 3); causing a computer to perform any function to secure access to computer material with intent to commit a CMA offence (CMA s 4); unauthorised modification of computer material (CMA s 5); and unauthorised access, use or interception of computer services (CMA s 6).

[167] CMA s 8A(7).

[168] See n 12.

[169] Cybersecurity Act ss 7–16.

[170] Cybersecurity Act s 19.

[171] Cybersecurity Act ss 20(2)(*b*)-(*f*).

[172] Cybersecurity Act s 8.

hoeren@uni-muenster.de

including: scanning the computer(s), preserving the computer(s) by not using it, taking extracts from any electronic record or computer program in the computer(s), and (with the owner's consent) taking possession of the computer(s).[173]

The Commission does not administer the abovementioned statutes. Instead:

- the Criminal Procedure Code is administered by the Ministry of Law and related authorities[174];
- the CMA is administered by the Ministry of Home Affairs[175]; and
- the Cybersecurity Act is administered by the Cyber Security Agency of Singapore.[176]

3.3 Minors

The PDPA does not specify when a minor (an individual less than 21 years-old) may give consent.[177] The rights of parents in respect of their children are also not specified in the PDPA.[178] Instead, whether a minor can give consent, and the rights of parents in respect of their children, would depend on other relevant laws.[179] However, the Commission has specifically issued guidelines on obtaining a minor's consent.[180]

For instance, organisations should consider whether a minor has "sufficient understanding of the nature and consequences of giving consent".[181] The rule of thumb (based in part on the United States Children's Online Privacy Protection Act[182] and the Singapore Employment Act[183]) is that an individual who is at least 13 years old would have sufficient understanding to consent on his/her own behalf.[184] However, where there is reason to believe or it can be shown that a minor aged 13 or over does not have sufficient understanding of the nature and consequences of giving consent, or the minor is under 13, the organisation should

[173]Cybersecurity Act s 20.

[174]Singapore Parliamentary Debates, Official Report (19 March 2018) vol 94.

[175]Singapore Parliamentary Debates, Official Report (3 April 2017) vol 94.

[176]CSA Singapore: Who We Are. https://www.csa.gov.sg/who-we-are/our-organisation. Accessed 30 August 2019.

[177]PDPC Advisory Guidelines for Selected Topics para 7.1.

[178]PDPC Advisory Guidelines for Selected Topics para 7.7.

[179]PDPC Advisory Guidelines for Selected Topics para 7.1 (discussing PDPA s 4(6)(*a*)), para 8.7.

[180]PDPC Advisory Guidelines for Selected Topics paras 7.1–7.13.

[181]PDPC Advisory Guidelines for Selected Topics para 7.6.

[182]15 USC Chapter 91.

[183]Cap 91, 2009 Rev Ed.

[184]PDPC Advisory Guidelines for Selected Topics paras 7.3–7.6.

hoeren@uni-muenster.de

obtain consent from an individual legally able to provide consent on the minor's behalf, such as a parent or guardian.[185]

Deemed Consent While the 13-year-old threshold would still apply, organisations wishing to rely on deemed consent should take extra care to establish whether such minor has sufficient understanding of the purposes for which the organisation is collecting, using and disclosing data and the consequences of giving his/her data.[186] Organisations should also not exercise undue influence to obtain personal data from minors.[187]

3.4 Right to Erasure

There is no specific right to be forgotten. However, the Limited Retention Obligation applies.

3.5 Employees

The PDPA applies to employees' personal data, irrespective of the form of the data.[188] Organisations should treat the personal data of their employees and job applicants "with equal care" and in the same manner as they would treat the personal data of any other individual.[189]

For instance, at *Yes Tuition Agency*,[190] the organisation (a tuition agency) disclosed on its website the national identification numbers and images of individuals who had registered to be tutors.[191] The Commission held that the organisation had breached the Consent Obligation by failing to obtain the tutors' consent for such disclosure.[192] And at *Jump Rope (Singapore)*,[193] the organisation sent an email to

[185]PDPC Advisory Guidelines for Selected Topics paras 7.6, 7.9. The PDPC has also decided a number of cases where minors' personal data were involved. See *e.g.*, *Singapore Taekwondo Federation* [2018] SGPDPC 17 (unauthorized disclosure of minor's national identification numbers via the organisation's website); *Spring College International Pte. Ltd.* [2018] SGPDPC 15 (school posted, without permission, personal data about its minor students on a public social media page to promote its courses).

[186]PDPC Advisory Guidelines for Selected Topics para 7.11.

[187]PDPC Advisory Guidelines for Selected Topics para 7.11.

[188]PDPC Protecting the Personal Data of Job Applicants and Employees p. 1.

[189]PDPC Protecting the Personal Data of Job Applicants and Employees p. 1.

[190][2016] SGPDPC 05.

[191][2016] SGPDPC 05 at [1].

[192][2016] SGPDPC 05 at [15].

[193][2016] SGPDPC 21.

hoeren@uni-muenster.de

various schools notifying them of its blacklisting of the complainant, a former employee; the email included the complainant's name and national identification number. The Commission held that while there can be "valid business or legal reasons" for blacklisting a former employee, even if it requires disclosing his/her personal data, the organisation should at least have notified the former employee of such disclosure; such disclosure should also be "only for purposes that a reasonable person would consider appropriate in the circumstances".[194] In this case, not only was consent not obtained, but there was also no business or legal reason justifying said disclosure, *e.g.* if the complainant's post-employment conduct "had put the [organisation's] trade reputation or potential clients at risk".[195]

Exceptions An organisation may collect, use or disclose employees' personal data without consent if the collection is "reasonable for the purpose of managing or terminating an employment relationship between the organisation and the individual" ("Managing/Terminating Purposes"),[196] or for evaluative purposes ("Evaluative Purposes")[197]; or if the personal data was in a document "produced in the course, and for the purposes, of the [employee's] employment" and "collected for purposes consistent with the purposes for which the document was produced".[198]

Managing/Terminating Purposes include: "[u]sing the employee's bank account details to issue salaries"; "[m]onitoring how the employee uses company computer network resources"; "[p]osting employees' photographs on the staff directory page on the company intranet"; and "[m]anaging staff benefit schemes like training or educational subsidies".[199] Evaluative Purposes include obtaining performance records or other evaluative information to determine an employee's performance.[200]

The difference between the two purposes lies in the requirement to notify employees regarding actions for Managing/Terminating Purposes but not Evaluative Purposes.[201] An organisation shall, on or before collecting, using or disclosing personal data about an employee for Managing/Terminating Purposes, inform him/her of such purpose and (on request) provide the business contact information of a person who is able to answer the employee's questions about such collection, use or disclosure.[202] The manner of notification is not prescribed, but it may be appropriate to notify employees through avenues like "employment contracts, employee handbooks, or notices in the company intranet".[203] Organisations should

[194] [2016] SGPDPC 21 at [10].

[195] [2016] SGPDPC 21 at [12].

[196] PDPA Second Schedule s 1(*o*), Third Schedule s 1(*j*), Fourth Schedule s 1(*s*).

[197] PDPA Second Schedule s 1(*f*), Third Schedule s 1(*f*), Fourth Schedule s 1(*h*).

[198] PDPA Second Schedule s 1(*n*), Third Schedule s 1(*j*), Fourth Schedule s 1(*s*).

[199] PDPC Advisory Guidelines for Selected Topics para 5.21.

[200] PDPC Advisory Guidelines for Selected Topics para 5.18.

[201] PDPC Advisory Guidelines for Selected Topics para 5.24.

[202] PDPA s 20(4).

[203] PDPC Advisory Guidelines for Selected Topics para 5.20.

hoeren@uni-muenster.de

also act based on what a reasonable person would consider appropriate in the circumstances.[204]

Organisations must still ensure that their employees' data is "properly protected, accurate and stored only for the period that it is needed".[205] Organisations must also allow the employee to access[206] and correct[207] his/her personal data, as well as withdraw consent.[208] Two important exceptions to an employer's Access Obligation are if: the data is solely for evaluative purposes[209]; and disclosing the data would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the organisation's competitive position.[210] There is also no need to correct personal data kept solely for evaluative purposes.[211]

CCTVs The PDPA encompasses the use of CCTVs (at a workplace or otherwise), *i.e.* individuals must be informed of the purposes for which their personal data (obtained through the CCTV) will be collected, use or disclosed.[212] Additionally, notices should be placed "so as to enable individuals [including employees] to have *sufficient* awareness that CCTVs have been deployed for a particular purpose", *e.g.* at the entry to a building.[213] However, the exact location of the CCTV need not be revealed.[214] Concerning an access request for CCTV records, such access shall be provided unless an exception applies, *e.g.* if the records may reveal personal data about another individual.[215] (However, access can be given if the organisation masks the personal data of other individuals.[216]) A reasonable processing fee can also be charged.[217] The organisation may also reject access requests which are "frivolous or vexatious", or if the burden of providing access would be unreasonable to the organisation or disproportionate to the individual's interests.[218]

Employee Usage of Personal Data There is no specific legislation or case law on this point. However, in *My Digital Lock Pte Ltd*,[219] the complainant and respondent were engaged in a legal dispute. Respondent's director "A" posted screenshots of the

[204]PDPC Advisory Guidelines for Selected Topics para 5.26.

[205]PDPA ss 23–25; Protecting the Personal Data of Job Applicants and Employees p. 3.

[206]PDPA s 21.

[207]PDPA s 22.

[208]PDPA s 16(1). See also Sect. 2.2.1.

[209]PDPA Fifth Schedule s 1(*a*).

[210]PDPA Fifth Schedule s 1(*g*).

[211]PDPA Sixth Schedule s 1(*a*).

[212]PDPC Advisory Guidelines for Selected Topics para 4.34.

[213]PDPC Advisory Guidelines for Selected Topics para 4.36.

[214]PDPC Advisory Guidelines for Selected Topics para 4.38.

[215]PDPC Advisory Guidelines for Selected Topics paras 4.42–4.43 (discussing PDPA s 21(3)(*c*)).

[216]PDPC Advisory Guidelines for Selected Topics para 4.43(*c*).

[217]PDPR s 7; PDPC Advisory Guidelines for Selected Topics para 4.46.

[218]PDPA s 21(2) read with Fifth Schedule ss 1(*j*)(ii), (v).

[219][2016] SGPDPC 20.

hoeren@uni-muenster.de

complainant's WhatsApp conversations with A (which included the complainant's personal mobile phone number and residential address) on A's Facebook page.[220] A claimed he merely intended to transfer the screenshots to his lawyers.[221] The Commission held that the transfer over Facebook "was wholly inappropriate" and unreasonable, and there "were other ways" to send the screenshots.[222] A could have encrypted or password protected the screenshots, or even "connected his phone to his PC and transferred the file without the need to make use of the open Internet".[223] As A was acting in the course of his employment with respondent, the respondent failed to make reasonable security arrangements to protect personal data in its possession or control, and was in breach of the PDPA.[224]

Additionally, employees who post material on social networks could be subject to defamation claims, both criminal[225] and civil,[226] as well as claims of malicious falsehood.[227] Other claims could include breach of confidence (*e.g.* through the unauthorised posting of private information)[228] and copyright infringement (*e.g.* by posting materials to which the poster does not have the copyright).[229] Employees have also been simply fired for unwise postings on social media.[230]

Vicarious liability may also apply if such employees' actions could be attributed to the employer, whether under the PDPA[231] or other law.[232]

3.6 Security Obligations and Data Breach Notifications

Security obligations are addressed more generally under other parts of Sect. 3.

---

[220][2016] SGPDPC 20 at [4], [13].

[221][2016] SGPDPC 20 at [21].

[222][2016] SGPDPC 20 at [21], [25].

[223][2016] SGPDPC 20 at [25].

[224][2016] SGPDPC 20 at [14], [24]-[26].

[225]Penal Code (Cap 224, 200 Rev Ed) s 499.

[226]See, *e.g.*, *Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd* [2015] SGHC 38 (involving claims of defamation and malicious falsehood through an employee's statements regarding another entity, made via Facebook, emails and text messages).

[227]See *Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd* [2015] SGHC 38.

[228]See Chan and Lee (2016) paras 16.020–16.027.

[229]See *Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd* [2015] SGHC 38. See also Tan B (2011) Social Media in the Workplace: Challenges and Implications. http://www.lawgazette.com.sg/2011-06/131.htm. Accessed 30 August 2019. Sedition Act (Cap 290, 2013 Rev Ed); Public Order Act (Chapter 257A); and the Penal Code (Cap 224, 2008 Rev Ed).

[230]See, *e.g.*, Lai L (2016) Aussie expat fired after offensive Facebook rant. In: The Straits Times. http://www.straitstimes.com/singapore/aussie-expat-fired-after-offensive-facebook-rant. Accessed 30 August 2019.

[231]PDPA s 53(1).

[232]See Chan and Lee (2016), paras 19.001 et seq.

hoeren@uni-muenster.de

3.6.1 Data Breach Obligations

Regarding data breach notifications: Singapore intends to adopt a mandatory data breach notification regime.[233] It has been reported that relevant legislation is intended to be tabled in Parliament in 2019.[234] While such amendments are being prepared, the Commission has issued specific guidelines to be followed.[235] Under these guidelines, the organisation will have up to 30 days to assess the suspected breach.[236] Additionally:

- When there is a data breach that is (a) likely to result in "significant harm" or "impact to the individuals to whom the information relates"; or (b) of a "significant scale" (i.e. the breach involves the personal data of 500 or more individuals), the organisation must notify the Commission within 72 h of establishing any of the above; and
- When there is a data breach that is likely to result in "significant harm" or "impact to the individuals to whom the information relates", the organisation must notify affected individuals "as soon as practicable".[237]

Others The Monetary Authority of Singapore ("MAS") has issued Technology Risk Management Guidelines[238] which are applicable to, among others, banks, finance companies and institutions, insurance companies, financial advisers, and financial holding companies. It provides comprehensive guidelines for securing, both physically and online, the institutions' computer systems, networks, data centres, operations and backup facilities.

[233]PDPC Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy Part III.

[234]Tham I (2018) Breach reporting part of revised data privacy laws to be tabled in Parliament. In: The Straits Times. https://www.straitstimes.com/tech/breach-reporting-part-of-revised-data-privacy-laws-to-be-tabled-in-parliament. Accessed 30 August 2019.

[235]PDPC Guide to Managing Data Breaches 2.0. Issued in May 2019, these guidelines appear to supersede the directions given in the PDPC Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy (issued in February 2018).

[236]PDPC Guide to Managing Data Breaches 2.0, p. 18.

[237]PDPC Guide to Managing Data Breaches 2.0, pp. 18, 32. In the PDPC Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy, it was also stated that an organisation will not have to notify affected individuals of an breach which is the subject of an ongoing or potential investigation under the law, if such notification will: compromise investigations or prejudice enforcement efforts ("law-enforcement exception"); a breach of data which has been encrypted to a reasonable standard, unless the data can be decrypted ("technological protection exception"); and/or an eligible breach if the organisation has taken actions to reduce the potential harm or impact to affected individuals, if the organisation demonstrates that as a result of its actions the breach is not likely to have any significant harm or impact to such individuals. However, as exceptions to notification were not addressed in the PDPC Guide to Managing Data Breaches 2.0, it is unclear whether these exceptions still apply.

[238]Monetary Authority of Singapore (MAS) (2013) Technology Risk Management Guidelines.

hoeren@uni-muenster.de

Specifically, "[e]ffective risk management practices and internal controls should be instituted to achieve", among others, data confidentiality, meaning "the protection of sensitive or confidential information such as customer data from unauthorised access, disclosure, etc".[239] Institutions shall also implement (or ensure that service providers implement) procedures and "to protect the confidentiality and security of its sensitive or confidential information, such as customer data".[240] Institutions should also "keep customers informed of any major incident" and informing the general public "where necessary".[241] While the TRMG are "not legally binding, the degree of observance with the spirit of the [g]uidelines . . . is an area of consideration in the risk assessment of the [institution] by MAS".[242]

Other regulatory agencies may work with the Commission with regard to data protection breaches. For instance, MAS stated that "in cases involving disclosure of banking customers' personal data", it would work with the Commission "to review the matter".[243]

3.7 Electronic Communications

3.7.1 Online Publication of Personal Data

Protection from Harassment (Amendment) Bill

Under the newly introduced (as of writing) Protection from Harassment (Amendment) Bill,[244] it will be an offence of to "publish any identity information" of another person with the intent to, or which is likely to, cause "harassment, alarm or distress" to such person (i.e. the act more commonly known as *doxxing*).[245] "Identity information" means any information that, whether on its own or with other information, identifies or purports to identify an individual, including:

[239]MAS Technology Risk Management Guideline para 4.0.2.

[240]MAS Technology Risk Management Guidelines para 5.1.4.

[241]MAS Technology Risk Management Guidelines para 7.3.9.

[242]MAS Technology Risk Management Guidelines para 1.0.5.

[243]This was in reference to an incident where reporters found, in a public area, a trash bag containing "several corporate statements, loan applications, and internal reports from [a] bank". Lee J (2016) MAS probes case of UOB's unshredded client data. In: The Straits Times. http://www.straitstimes.com/business/companies-markets/mas-probes-case-of-uobs-unshredded-client-data. Accessed 30 August 2019. The outcome of the investigation remains unclear: Koh WT (2016) UOB under MAS probe for failing to protect clients' privacy. In: The Straits Times. http://themiddleground.sg/2016/07/19/uob-mas-probe-failing-protect-client-privacy. Accessed 30 August 2019.

[244]No 11/2019, which will amend POHA.

[245]No 11/2019 s 4.

hoeren@uni-muenster.de

> the individual's name, residential address, email address, telephone number, date of birth, national registration identity card number, passport number, signature (whether handwritten or electronic) or password.[246]

This bill also acknowledges that many of these publications take place electronically: where the information is published online, the court may also require the platform provider to disable access to the offending publication.[247]

POFMA

POFMA is intended to (among other things) prevent electronic communication in Singapore of false statements of fact; such statements could presumably include personal data. It will be an offence to do any act (whether in or outside Singapore), in order to communicate a statement, knowing or having reason to believe that it is false, where: the communication of such statement is likely to be prejudicial to Singapore's security, to public health, or Singapore's friendly relations to other countries; or will incite feelings of enmity between different groups of persons.[248] This includes any statements made using "inauthentic online accounts" or "bots".[249]

3.7.2 Marketing

IP Addresses; Cookies If they can identify individuals, IP addresses and cookies may be considered personal data, and therefore subject to the PDPA.[250] However, there may not be a need to seek consent for the use of cookies to collect, use or disclose personal data where the individual involved is aware of the purposes for such collection, use or disclosure and has voluntarily provided his personal data for such purposes (*e.g.* for transmitting personal data for effecting online communications, and storing information that the user enters in a web form to facilitate an online purchase).[251]

For activities that cannot take place without cookies, consent may be deemed if the individual voluntarily provides the personal data for that purpose of the activity and it is reasonable that he would do so.[252] "Consent may also be reflected in the way a user configures his interaction with the Internet", *e.g.* if he/she configures his browser "to accept certain cookies but rejects others".[253] However, an individual's failure to actively manage his/her browser settings does not imply consent to the

[246] No 11/2019 s 3.

[247] No 11/2019 s 16.

[248] POFMA s 7(1).

[249] POFMA s 7(3).

[250] PDPC Advisory Guidelines for Selected Topics paras 6.1–6.3, 6.6.

[251] PDPC Advisory Guidelines for Selected Topics para 6.8.

[252] PDPC Advisory Guidelines for Selected Topics para 6.8.

[253] PDPC Advisory Guidelines for Selected Topics para 6.9.

hoeren@uni-muenster.de

collection, use and disclosure of his/her personal data by all websites for their stated purpose.[254]

The obligation to obtain consent lies with the organisation collecting such data (whether by itself or through data intermediaries).[255]

Do Not Call Registries The PDPA established a number of "Do Not Call Registries" (each a "DNCR")[256] to which a person may add (or remove) his Singapore *telephone number* (whether personal, business, or otherwise).[257] This is an opt-out system. No marketing messages shall be sent (whether in sound, text, visual or other form (including voice or video calls made through a data service or other electronic means))[258] to a Singapore telephone number which is in a relevant DNCR.[259] Even if a number is not in a DNCR, a marketing message sent to such number must include specific information on the sending individual or organisation,[260] and must not conceal the identity of the sender.[261]

No one shall, as a condition for supplying "goods, services, land, interest, or opportunity" (collectively "services"), require another to give consent for the sending of a marketing message to a Singapore phone number "beyond what is reasonable to provide" such services.[262] Consent given in such circumstances or obtained through providing false or misleading information or by using deceptive or misleading practices is not validly given.[263] Consent given under the DNCR provisions may also be withdrawn at any time.[264]

The DNCR provisions apply where either the sender or recipient is in Singapore when the message is sent or accessed, respectively.[265] The DNCR provisions operate in conjunction with the rest of the PDPA, and organisations must comply with both sets of provisions regarding Singapore telephone numbers.[266]

[254]PDPC Advisory Guidelines for Selected Topics para 6.9.

[255]PDPC Advisory Guidelines for Selected Topics para 6.10.

[256]PDPC Advisory Guidelines on the Do Not Call Provisions para 1.8. The DNCR provisions came into effect on 2 January 2014: Personal Data Protection Act 2012 (Commencement) Notification 2013 (S 708 of 2013).

[257]PDPA ss 39–40; PDPC Advisory Guidelines on Key Concepts para 2.7.

[258]PDPA s 37; PDPC Advisory Guidelines on DNCR Provisions para 1.8.

[259]PDPA s 43(1). There are at present three DNCRs: for voice calls, text messages, and fax messages. Advisory Guidelines on DNCR Provisions para 1.8.

[260]PDPA s 44(1).

[261]PDPA s 45(1). This provision applies to voice calls only.

[262]PDPA s 46(1).

[263]PDPA s 46(2).

[264]PDPA s 47(6).

[265]PDPA s 38.

[266]PDPC Advisory Guidelines on Key Concepts para 2.7.

hoeren@uni-muenster.de

Marketing Emails The Spam Control Act or SCA[267] governs unsolicited commercial communications sent in bulk via electronic mail. Concerning personal data, anyone who receives an unsubscribe request in connection with the sending of an unsolicited commercial electronic message shall not disclose any information contained in such request to any other person, except with the consent of the person whose particulars are contained in the unsubscribe request.[268]

As of 27 April 2018, the Commission was considering a merger of the DNC Provisions of the PDPA and the Spam Control Act under a single act governing "unsolicited commercial messages".[269] This follows similar approaches in jurisdictions such as Hong Kong and the United Kingdom.[270]

3.7.3 Electronic Communications Sector

The PDPA applies generally to the electronic communications sector (see Sect. 2.1). In addition, the Telecommunications Act[271] and the Electronic Transactions Act or ETA[272] (both also administered by the IMDA) touch on certain aspects of personal data protection.

The Commission's guidelines specifically provide some examples of the PDPA as applied to the telecommunications sector.[273] For instance, the guidelines discuss what may constitute "personal data" in the telecommunications context: *e.g.* an individual's mobile telephone number and, if combined with other information, an Internet Protocol ("IP") address and International Mobile Equipment Identity ("IMEI") numbers.[274]

Second, under the Telecommunications Act, a public telecommunication licensee has no liability to anyone due to "any loss of secrecy in communication arising from the use of any telecommunication service" due to "the act or default of another person, or an accident or some other cause" beyond the licensee's control.[275] More specifically with regard to personal data, the act also "sets out certain purposes for which telecommunication operator[s] may collect, use or disclose End User Service

[267] See n 17. The SCA is administered by the IMDA.

[268] SCA s 11 read with Second Schedule s 2(8).

[269] PDPC Combined Regime Proposal 2018.

[270] PDPC Combined Regime Proposal 2018.

[271] See n 18.

[272] See n 13.

[273] PDPC Advisory Guidelines for the Telecommunication Sector.

[274] PDPC Advisory Guidelines for the Telecommunication Sector paras 2.4–2.5. Thus, when a Singapore telecommunications operator provider exchanges personal data with a foreign telecommunications operator to allow the latter to provide mobile services to outbound roamers who are subscribers of the Singapore operator, the Singapore operator will need to comply with the Notification, Consent and Limited Transfer Obligations. PDPC Advisory Guidelines for the Telecommunication Sector para 3.7. See also Sects. 2 and 4.2.

[275] Telecommunications Act s 70(*d*).

hoeren@uni-muenster.de

Information ("EUSI"), some of which qualify as personal data, without consent",[276] including "collection or use of [a] Residential End User's EUSI as ... reasonably necessary for planning requirements in relation to network operations or network maintenance" and "collection, use or disclosure of Residential End User's EUSI as ... reasonably necessary for facilitating interconnection and interoperability ... for the provision of Services".[277] Additionally, regarding the DNCR provisions in the PDPA, a "telecommunications service provider who merely provides a service" that enables a message to be sent shall "be presumed not to have sent the message and not to have authorised the message to be sent".[278]

Finally, the ETA defines "electronic communication" as "any communication that the parties make by means of electronic records", meaning "a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another".[279] Concerning personal data: pursuant to the enactment of the PDPA, the ETA was specifically amended to state that an NSP "shall not be subject to any liability" under the PDPA "in respect of third-party material in the form of electronic records to which [it] merely provides access",[280] including the "temporary and automatic caching of third party material in the form of electronic records (that contains personal data) ... provided that such caching is ... for the purpose of ... merely providing access to the third party material".[281]

Supervisory Authority IMDA has the power to enforce both the Telecommunications Act and the ETA. Under the Telecommunications Act, IMDA shall operate and provide telecommunication systems and services in Singapore and may impose penalties for violations of the act.[282] It may also conduct investigations under the act.[283]

Under the ETA, IMDA shall (among other things)facilitate communications through reliable electronic records; promote confidence in the integrity and reliability of electronic commerce; and implement the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the United Nations on 23rd November 2005.[284] IMDA may

[276]PDPC Advisory Guidelines for the Telecommunication Sector para 4.3.

[277]IMDA (2014) Code Of Practice For Competition In The Provision Of Telecommunication Services 2012 para 3.2.6.2. https://www.imda.gov.sg/~/media/imda/files/regulation%20licensing%20and%20consultations/frameworks%20and%20policies/competition%20management/telecom%20competition%20code/02%202012tccwef2july2014.pdf?la=en. Accessed 30 August 2019.

[278]PDPA s 36(2).

[279]ETA s 2(1).

[280]Personal Data Protection Bill (No 24 of 2012) s 67(2); ETA s 26(1A).

[281]PDPC Advisory Guidelines for the Telecommunication Sector para 4.2.

[282]See, *e.g.*, Telecommunications Act Part II. This includes suspending or cancelling telecommunications licenses.

[283]Telecommunications Act Part VIII. It may also arrest certain wrongdoers thereunder.

[284]ETA s 3.

hoeren@uni-muenster.de

conduct investigations under the ETA,[285] and compound any offences under the act.[286]

3.8 Data Protection and Digital Forensics

The PDPA provides exceptions from the various Obligations due to criminal investigations[287]:

- Collection without consent is allowed if it "is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;"[288]
- Use and disclosure without consent is allowed if such use or disclosure "is necessary for any investigation or proceedings"[289] or disclosed to an officer of a law enforcement agency[290];
- Access is not required for: "a document related to a prosecution if all proceedings related to the prosecution have not been completed"; personal data "subject to legal privilege"; or personal data collected, used or disclosed without consent for an investigation (pursuant to the consent exceptions in Second, Third and Fourth Schedules regarding investigations) if "the investigation and associated proceedings and appeals have not been completed"[291]; additionally, an organisation shall not inform an individual that it has disclosed personal data to a law enforcement agency, if such disclosure was made without that individual's consent (pursuant to the Fourth Schedule or other law)[292]; and
- Correction is not required for a document related to a prosecution "if all proceedings related to the prosecution have not been completed".[293]

More generally, pursuant to an investigation the police may access and inspect computers (including computer networks), as well as decrypt data on computers and networks.[294] See Sect. 3.2 for recent amendments to the Criminal Procedure Code, the CMA, and the Cybersecurity Act.

[285] ETA s 24.
[286] ETA s 36(1).
[287] PDPA s 2(1).
[288] PDPA Second Schedule s 1(*e*).
[289] PDPA Third Schedule s 1(*e*), Fourth Schedule s 1(*f*).
[290] PDPA Fourth Schedule s 1(*n*).
[291] PDPA Fifth Schedule ss 1(*e*), (*f*), (*h*).
[292] PDPA s 21(4).
[293] PDPA Sixth Schedule s 1(*e*).
[294] CPC ss 39–40, read with CMA s 2(1).

hoeren@uni-muenster.de

3.9 Data Protection and Electronic Surveillance for Security and Defence Purposes

A number of statutes discuss the electronic processing of personal data for security and national defence purposes.

First, under the PDPA, an organisation shall not provide an individual with his/her personal data (or information about the ways in which the data has or may have been used or disclosed by the organisation) if the provision of that data or other information could reasonably be expected to "be contrary to the national interest".[295] Additionally, consent is not required for the collection, use or disclosure of personal data where such collection, use or disclosure is in the national interest.[296] National interest includes "national defence, national security, public security, the maintenance of essential services and the conduct of international affairs".[297]

Second, the CMA applies to any unauthorised use of computers and related materials, including any data contained therein, whether the offender or computer or data is in Singapore or not, for any offence which "causes, or creates a significant risk of, serious harm in Singapore".[298] "[S]erious harm in Singapore" involves:

- "a disruption of, or a serious diminution of public confidence in, the provision of any essential service";
- "a disruption of, or a serious diminution of public confidence in, the performance of any duty or function of, or the exercise of any power by" the Singapore government or any Singapore governmental agency; or
- "damage to the national security, defence or foreign relations of Singapore".[299]

An example would be giving the public access to confidential documents belonging to a Singapore governmental ministry.[300]

The Cybersecurity Act also empowers the minister to "authorise or direct any person or organisation" to "take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service" for the "purposes of preventing, detecting or countering any serious and imminent threat to (a) the provision of any essential service; or (b) the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore".[301] This may include the powers to access computers granted

[295] PDPA s 21(3)(*e*).

[296] PDPA Second Schedule s 1(*d*), Third Schedule s 1(*d*), Fourth Schedule s 1(*e*).

[297] PDPA s 2(1).

[298] CMA s 11.

[299] CMA s 11(4).

[300] CMA s 11.

[301] Cybersecurity Act s 23(1).

hoeren@uni-muenster.de

under the Criminal Procedure Code, including the power to investigate personal data on computers (as discussed under Sect. 3.2).[302]

The Cybersecurity Act also authorises (among other things) the taking of measures to prevent, manage and respond to cyber security threats.[303] This has two general components—ensuring the protection of CIIs,[304] and preventing and investigating cyber security incidents.[305]

It is also notable that section 58 of the Telecommunications Act seemingly provides a lower threshold for the minister to give directions to a telecommunications licensee, where it is "requisite or expedient to do so", "on the occurrence of any public emergency, in the public interest or in the interests of public security, national defence, or relations with the government of another country".[306]

Finally, as stated in Sect. 3.7.1, under POFMA it will be an offence to do any act (whether in or outside Singapore), in order to communicate a false statement, where: the communication of such statement is likely to be prejudicial to Singapore's security, to public health, or Singapore's friendly relations to other countries; or will incite feelings of enmity between different groups of persons.[307] This includes any statements made using "inauthentic online accounts" or "bots".[308]

3.10 Remedies and Sanctions

PDPA Enforcement under the PDPA is complaints-based rather than audit-based.[309] However, the Commission may also conduct an investigation under the PDPA on its own motion.[310]

Remedies The Commission may refer a complaint for mediation or direct the parties to resolve the complaint "in the way directed by the Commission".[311] Additionally, in response to a complaint regarding an organisation's non-compliance with the Access or Correction Obligations, the Commission may: confirm a refusal to provide access or direct the organisation to provide such access; confirm, reduce, or disallow

[302]Cybersecurity Act s 23(2).

[303]Cybersecurity Act (long title). See also Sect. 3.2.

[304]Cybersecurity Act ss 7–10.

[305]Cybersecurity Act ss 19–23.

[306]Telecommunications Act s 58. See also Tan KB (2016) Security and privacy must not be traded off against each other. In: Today Online. https://www.todayonline.com/commentary/security-and-privacy-must-not-be-traded-against-each-other. Accessed 18 June 2018.

[307]POFMA s 7(1).

[308]POFMA s 7(3).

[309]Chesterman (2018), para 2.103; PDPA s 50(1).

[310]PDPA s 50(1).

[311]PDPA s 27.

hoeren@uni-muenster.de

a fee imposed in connection with such request, or require a refund of such fee; or confirm a refusal to correct data, or direct the organisation to correct such data.[312]

The Commission may also give a non-PDPA compliant organisation such directions as it sees fit, including to: stop collecting, using or disclosing personal data; destroy personal data collected in contravention of the PDPA; comply with the Commission's directions concerning the Access or Correction Obligations; and pay a penalty not exceeding $1 million SGD (save for breaches which are offences under the PDPA).[313] The Commission may register its directions at a District Court for enforcement purposes.[314]

As of writing, the maximum penalty issued under the PDPA has been $750,000 SGD.[315] In practice the Commission has also issued warnings in cases which it did not deem severe breaches of the PDPA.[316]

Offences It is an offence to request for access to, or to change personal data about another individual without the authority of such individual, conviction under which may result in a fine not exceeding $5000 SGD and/or imprisonment for a term not exceeding 12 months.[317]

An organisation or person commits an offence if (a) with intent to evade a request under the Access or Correction Obligations, it/he/she disposes of, alters, falsifies, conceals or destroys (or directs another person to do any of the above) a record containing (1) personal data or (2) information about the collection, use or disclosure of personal data; (b) obstructs or hinders the Commission in the performance of any function or duty, or the exercise of any power, under the PDPA; or (c) makes a statement or furnishes any information or document, to the Commission which it/he/she knows (or ought reasonably to know) to be false or misleading.[318] Conviction under (a) may result in, for an individual, a fine not exceeding $5000 SGD and otherwise a fine not exceeding $50,000 SGD.[319] Conviction under (b) or (c) may result in, for an individual, a fine not exceeding $10,000 SGD and/or imprisonment for a term not exceeding 12 months, and otherwise a fine not exceeding $100,000 SGD.[320]

Regarding the DNCR provisions, each of the following is an offence which may result in a fine not exceeding $10,000 SGD:

---

[312] PDPA s 28.

[313] PDPA s 29.

[314] PDPA s 30.

[315] *Singapore Health Services Pte Ltd* [2019] SGPDPC 03. The financial penalties imposed against the two organisations involved are, individually, the highest ($750,000 SGD) and second highest ($250,000 SGD) financial penalty amounts imposed by the Commission to date.

[316] See, *e.g.*, *Singapore Computer Society* [2016] SGPDPC 09; *Jump Rope (Singapore)* [2016] SGPDPC 21.

[317] PDPA ss 51(1)-(2).

[318] PDPA s 51(3).

[319] PDPA s 51(4).

[320] PDPA s 51(5).

hoeren@uni-muenster.de

- Sending a marketing message to a Singapore telephone number listed in a DNCR[321];
- In sending a marketing message, failing to include certain contact and other information regarding the sending individual or organisation[322];
- Making a marketing voice call that conceals the identity of the sender[323];
- A telecommunications service provider's failure to report to the Commission all terminated Singapore telephone numbers.[324]

Finally, any person guilty of an offence under the PDPA "for which no penalty is expressly provided" shall be liable on conviction to a fine not exceeding $10,000 SGD and/or imprisonment for a term not exceeding 3 years.[325] If it is a "continuing offence", there shall be "a further fine" not exceeding $1000 SGD for every day or part thereof during which the offence continues after conviction.[326]

Where an offence committed by a body corporate has been committed with the consent or connivance, or is attributable to the neglect of, an officer of such body, both the officer and the body shall be guilty of the offence.[327] Employers are also liable for an employee's acts done in the course of his/her employment, whether or not such act was done with the employer's knowledge or approval.[328] However, it is a defence for an employer to prove that he "took such steps as were practicable to prevent the employee" from doing such act.[329]

The courts have jurisdiction over offences under the PDPA.[330] However, the Commission may compound certain offences thereunder.[331]

Appeals An organisation or individual may apply for reconsideration of the Commission's decision[332] or appeal such decision to the Data Protection Appeal Panel ("DPAP").[333] An appeal against the DPAP's decision may be made regarding a point of law or the amount of a financial penalty imposed to the Singapore High

[321]PDPA s 43(2).

[322]PDPA s 44(2).

[323]PDPA s 45(2).

[324]PDPA s 42(2).

[325]PDPA s 56.

[326]PDPA s 56.

[327]PDPA ss 52(1)-(2). This also applies to partnerships and unincorporated associations. PDPA ss 52(3)-(4).

[328]PDPA s 53(1).

[329]PDPA s 53(2).

[330]PDPA s 54.

[331]PDPA s 55; Personal Data Protection (Composition of Offences) Regulations 2013 (S 759 of 2013).

[332]PDPA s 31(1).

[333]PDPA s 33 read with ss 34(1)-(2). If an application for reconsideration is made, an appeal on the same matter shall be deemed to be withdrawn: PDPA s 34(2).

hoeren@uni-muenster.de

Court.[334] Further appeal to the Court of Appeal may be made, in the same manner as for High Court decisions made "in the exercise of its original civil jurisdiction".[335]

Private Actions There is a right of private civil action by any person who suffers loss or damage "directly as a result of" a PDPA breach by an organisation.[336] A claimant may obtain damages, injunction or declaration, or such other relief as the court sees fit.[337] However, if the Commission has made a decision in respect of such breach, no private action may be brought until all appeals regarding such breach are exhausted.[338]

Criminal Procedure Code It is an offence to breach the new computer-related powers of investigation under the aforementioned amendments to the Criminal Procedure Code (by obstructing an investigation or failure to comply with an order).[339] The offender may receive a fine not exceeding $5000 SGD and/or imprisonment for a term not exceeding 6 months.[340] Where the offender is a body corporate, it may receive a fine not exceeding $10,000 SGD.[341]

CMA Under the CMA, obtaining, retaining, supplying, transmitting or making available "personal information" obtained in violation of certain CMA offences[342] may result, for first time offenders, in a fine not exceeding $10,000 SGD and/or imprisonment for a term not exceeding 3 years; and on subsequent convictions, to a fine not exceeding $20,000 SGD and/or imprisonment for a term not exceeding 5 years.[343]

"Enhanced punishment"[344] is also available for certain CMA offences[345] involving "protected computers", *i.e.* where the offender knew (or ought reasonably to have known) that the computer or program or data in question was used in directly connection with or was necessary for "the security, defence or international relations of Singapore"; "the existence or identity of a confidential source of information relating to the enforcement of a criminal law"; "the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure"; or "the protection of

[334]PDPA s 35(1).
[335]PDPA s 35(4).
[336]PDPA s 32(1).
[337]PDPA s 32(3).
[338]PDPA s 32(2).
[339]CPC s 39(3).
[340]CPC s 39(3).
[341]CPC s 39(3).
[342]CMA ss 3–6.
[343]CMA s 8A.
[344]CMA s 9.
[345]CMA ss 3, 5–7.

hoeren@uni-muenster.de

public safety including systems related to essential emergency services".[346] Conviction thereunder may result in a fine not exceeding $100,000 SGD and/or to imprisonment not exceeding 20 years.[347] The courts have jurisdiction over all CMA offences[348]; however, the certain offences thereunder may be compounded.[349]

Private Action There is a right of private civil action under the CMA. A court which has convicted a person under the CMA may also order him/her to make compensation to a person "for any damage caused to his computer, program or data".[350] Such claim shall also "not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order".[351]

Cybersecurity Act Regarding measures taken and/or requirements to prevent, detect or counter threats to Singapore's national security, essential services, defences or foreign relations, obstruction of such measures or failure to comply with such requirements is an offence, conviction of which may result in a fine not exceeding $50,000 SGD and/or imprisonment not exceeding 10 years.[352] Additionally, a person with information pursuant to the above measures and/or requirements who uses or discloses such information has committed an offence, conviction under which may result in a fine not exceeding $10,000 SGD and/or imprisonment for a term not exceeding 12 months.[353]

PS(G)A Public servants who share data (including personal data) without authorisation, or who make use of data to benefit themselves, can be fined up to $5000 SGD and/or jailed for up to 2 years.[354] Public servants who re-identify (or cause re-identification of) anonymised data without authorisation are also liable for the same punishment.[355]

POFMA

Anyone who communicates in Singapore a false statement of fact having certain stated effects can be fined up to $50,000 SGD and/or jailed for up to 5 years.[356] Where "inauthentic online accounts" or "bots" are used to accelerate such communication, involved individuals can be fined up to $100,000 SGD and/or jailed for up to 10 years; and non-individuals can be fined up to $1,000,000 SGD.[357]

[346] CMA ss 9(1)-(2).
[347] CMA s 9(1).
[348] CMA s 12.
[349] CMA s 12A.
[350] CMA s 13(1).
[351] CMA s 13(2).
[352] Cybersecurity Act ss 23(4)-(5).
[353] Cybersecurity Act ss 23(8)-(9).
[354] PS(G)A ss 7(1), (3).
[355] PS(G)A s 8.
[356] POFMA s 7(2). See Sect. 3.7.1.
[357] POFMA s 7(3).

hoeren@uni-muenster.de

Protection from Harassment (Amendment) Bill
Anyone who publishes the identity information of a person in contravention of those provisions can be fined up to $5,000 SGD and/or jailed for up to 6 months.[358]

4 Private International Law Rules

4.1 Territorial Scope; Foreign Entities

The PDPA applies to all organisations carrying out activities involving personal data in Singapore.[359] Any organisation that collects personal data overseas and brings it into Singapore is also subject to the PDPA from the time it seeks to collect the personal data (if such collection occurs in Singapore) or brings such data into Singapore.[360] Similarly, electronic data processing by entities seated outside Singapore is still considered under the PDPA, so long as the personal data is located in Singapore. Indeed, the definition of "organisation" includes companies formed under non-Singapore laws and/or resident outside Singapore.[361]

It should be noted that a data intermediary has no obligation under the PDPA save for the Protection Obligation and the Retention Obligation[362] (but these Obligations may also apply to data intermediaries who are overseas[363]). Instead, an organisation that uses a data intermediary shall have the same obligation in respect of personal data processed on its behalf by a data intermediary as if the data were processed by the organisation itself.[364]

Regarding personal data implicated in computer-related crimes: under the CMA, Singapore claims extra-territorial jurisdiction over any person or any data which causes or creates a significant risk of serious harm in Singapore.[365] (See Sect. 3.9 for the definition of "serious harm".) Under the Criminal Procedure Code, investigators can also inspect and search, in and from Singapore, any data stored on or available to a computer implicated in the investigation, regardless of whether the computer is

[358]No 11/2019 s 13. See Sect. 3.7.1.

[359]PDPC Advisory Guidelines on Key Concepts para 11.1.

[360]PDPC Advisory Guidelines on Key Concepts para 11.2. See also Lim (2018), para 8.9: "[t]he reach of the PDPA [was] explicitly extended to those organisations that may not have any presence in Singapore, or which may not even be recognised under the law of Singapore".

[361]PDPA s 2(1).

[362]PDPA s 4(2). See, *e.g.*, *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Challenger Technologies Limited* [2016] SGPDPC 06.

[363]Greenleaf (2018), para 8.55.

[364]PDPA s 4(3). Indeed, it has been said that "Singapore has enacted a form of vicarious liability on Singaporean data controllers for overseas processing". Greenleaf (2018), para 8.55.

[365]CMA s 11.

hoeren@uni-muenster.de

inside or outside Singapore (thus this could include web-based email accounts and web storage accounts).[366]

For the Cybersecurity Act, a computer/computer system has to be located wholly or partly in Singapore to be considered a CII.[367] The PS(G)A does not discuss this issue; however it covers generally data "under the control" of an agency.[368]

4.2 Transfer of Personal Data to Foreign Jurisdictions

No personal data shall be transferred outside Singapore unless the recipient of that data must, under legally enforceable obligations, provide the transferred data with a standard of protection that is at least comparable to the protection afforded under the PDPA.[369] "Legally enforceable obligations" includes obligations imposed on the recipient under: any law; the use of contractual arrangements; and/or binding corporate rules (for intra-corporate transfers only).[370]

The above requirement is also satisfied if, among others: the individual concerned consents to the data transfer; the transfer is necessary for the performance of a contract between the individual and the organisation; the transfer is necessary for a use or disclosure in certain situations where consent is not required under the PDPA; the data is merely in transit through Singapore; or the data is publicly available in Singapore.[371] Additionally, exemptions may be granted.[372]

Certain cross-border agreements may also have implications for foreign transfers of personal data.[373]

[366]CPC s 39(1).

[367]Cybersecurity Act s 7(1)(b).

[368]PS(G)A s 6(1).

[369]PDPA s 26(1); PDPR s 9(1).

[370]PDPR s 10; PDPC Advisory Guidelines on Key Concepts para 19.2.

[371]PDPR s 9(3).

[372]PDPA s 26(2). There are also specific requirements for certain sectors. For instance, a specific data protection regime applies to cross-border transfers of data in the banking industry, as enforced by MAS. Chia (2018), p. 321.

[373]For instance, Singapore has free-trade agreements which include provisions relating to data protection. However, these provisions (if they exist) are generally not specific enough to override the restrictions on cross-border data transfers in the national laws of the parties to these agreements Chia (2018), p. 324. More recently in March 2018, Singapore joined the APEC Cross-Border Privacy Rules ("CBPR") system. This is a framework for the exchange of personal data among participating APEC economies. The Commission is working on a scheme for organisations to be certified under this system, and will likely provide guidance in due course on the operation of the CBPR system in the context of the PDPA's requirements for cross-border transfers of personal data Alfred and Goh (2018) paras 12.42–12.44.

hoeren@uni-muenster.de

References

Alfred D, Goh L (2018) Cross-border issues in data protection. In: Chesterman S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore

Chan G, Lee PW (2016) The law of torts in Singapore. Academy Publishing, Singapore

Chesterman S (2018) Introduction. In: Chesterman S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore

Chia K (2018) Jurisdictional report – Singapore. In: Regulation of cross-border transfers of personal data in Asia. Asian Business Law Institute, Singapore. http://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia. Accessed 13 Sept 2018

Chik W (2013) The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. Comput Law Secur Rev 29:554–575

Goh L, Aw J (2018) Data protection law and privacy in Singapore. In: Chesterman S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore

Greenleaf G (2018) Comparisons with other Asian jurisdictions. In: Chesterman S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore

Lim HYF (2018) Data protection in the employment setting. In: Chesterman S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore

Monetary Authority of Singapore (MAS) (2013) Technology risk management guidelines. http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf. Accessed 12 May 2017

Personal Data Protection Commission Guidelines: Advisory Guidelines on the Do Not Call Provisions. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-the-dnc-provisions-(270717).pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Advisory Guidelines for the Education Sector. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/Finalised-Education-Guidelines_31Aug2018.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Advisory Guidelines for the Healthcare Sector. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/advisoryguidelinesforthehealthcaresector28mar2017.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Advisory Guidelines on Key Concepts in the Personal Data Protection Act. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts-in-the-PDPA-Revised-15-July-2019.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Advisory Guidelines on the Personal Data Protection Act for Selected Topics. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/FINAL-Advisory-Guidelines-on-PDPA-for-Selected-Topics-2-Jan-2019.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Advisory Guidelines for the Real Estate Agency Sector. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/real-estate.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Advisory Guidelines on Requiring Consent for Marketing Purposes. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisoryguidelinesonrequiringconsentformarketing8may2015.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Advisory Guidelines for the Social Service Sector. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/Finalised-Social-Service-Guidelines_31Aug2018-v2.pdf. Accessed 30 Aug 2019

hoeren@uni-muenster.de

Personal Data Protection Commission Guidelines: Advisory Guidelines for the Telecommunication Sector. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/finalised-advisory-guidelines-on-application-of-pdpa-to-telecom-sector.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Combined Regime Proposal 2018. (PDPC Proposes Combined Regime to Regulate Telemarketing and Spam Messages and Enhanced Guidance to Provide Regulatory Certainty). https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Press-Room/2018/Factsheet-on-PDPA-Public-Consult-2-(270418).pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Guide to Accountability under the Personal Data Protection Act. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Accountability.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Guide to Managing Data Breaches 2.0. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Managing-Data-Breaches-2-0.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guidetopreventingaccidentaldisclosurewhenprocessingandsendingpersonaldata200117eb6b44c8844062038829f.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Guide to Securing Personal Data in Electronic Medium. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Introduction to the Guidelines. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/introduction-to-the-guidelines.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Protecting the Personal Data of Job Applicants and Employees. https://www.pdpc.gov.sg/resource/DPO-Connect/March-16/pdf/ProtectingthePersonalDataOfJobApplicants_and_Employees.pdf. Accessed 12 May 2017

Personal Data Protection Commission Guidelines: Public Consultation for Approaches to Managing Personal Data in the Digital Economy. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthedigitaleconomy270717f95e65c8844062038829ff000.pdf. Accessed 30 Aug 2019

Personal Data Protection Commission Guidelines: Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf. Accessed 30 Aug 2019

Tan S (2018) Data protection and new technologies. In: Chesterman S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore

Ter KL (2013) Singapore's personal data protection legislation: business perspectives. Comput Law Secur Rev 29:264–273

hoeren@uni-muenster.de

Data Protection in the Internet: South Africa

Lukman Adebisi Abdulrauf

1 Introduction

In line with global best practice, South Africa has an organized legal framework for the protection of personal information. This comprises of the South African Constitution and a host of other legislation and regulations. The most notable among the legislation is the Protection of Personal Information Act (hereinafter, 'POPI Act' or 'the Act') No 4 of 2013 which was only recently enacted by the South African legislature.[1] This legislation established the Information Regulator which is the institutional framework responsible for implementing the provisions of the POPI Act. This chapter seeks to assess the extent to which personal data is protected on the internet in South Africa. It will therefore focus largely on the provisions of the POPI Act since it is the omnibus data protection framework in the country.

The chapter is divided into five sections. After the introduction, Sect. 2 gives a general background into the data protection framework in South Africa. Here, a brief overview is carried out of the key legislation which comprises the data protection framework on South Africa. The section also analyses the key provisions of the main data protection legislation in South Africa—the POPI Act. Section 3 focuses on the supervisory structure of data protection in South Africa. A brief discussion is carried

This work is based on the research supported by the South African Research Chairs Initiative of the Department of Science and Technology and National Research Foundation of South Africa (Grant No 98338).

[1] Protection of Personal Information (POPI) Act, No 4 of 2013. Also available at http://www.justice.gov.za/legislation/acts/2013-004.pdf.

L. A. Abdulrauf (✉)
Department of Public Law, South African Research Chair in International Constitutional Law, University of Pretoria, Pretoria, South Africa

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_14

hoeren@uni-muenster.de

out of the scope of the powers of the South African Information Regulator. Section 4 considers data protection in specific context such as electronic/automated processing, electronic communications sector, and digital forensics. In Sect. 5, the international dimension of data protection is examined before the chapter concludes with some reflections on the state of data protection on the internet in South Africa.

2 The General Data Protection Framework in South Africa

2.1 Background to the Applicable Rules: The POPI Act

In South Africa, the protection of personal data (information) is realized through a host of legislation. These legislation either have general of sectoral application. Recently, South Africa enacted its omnibus/general data protection legislation which is the Protection of Personal Information Act (hereinafter, 'POPI Act' or 'the Act') No 4 of 2013.[2] This followed extensive deliberations which started since 2000 by the South African Law Reforms Commission (SALRC) when it included 'privacy and data protection' among its research topics.[3] This long process only yielded fruits in 2013 when the Act was adopted by parliament after much expectation and anticipation. Although, the law has been signed by the President of South Africa, it is imperative to state that it is yet to fully come into force. Section 115 of the Act *inter alia* provides that the Act only comes into force "on a date determined by the President by proclamation in the Gazette".[4] The President has, as yet, not so determined. Nevertheless, the Act provides that "Different dates of commencement may be determined in respect of different provisions of this Act or in respect of different class or classes of information and bodies".[5] It is in the light of this section that the President has determined that certain provisions should take effect—for example, the provision which establishes the supervisory authority.[6] Annelise Roos contends that "It is assumed that the Act will enter into force fully once the office of the Regulator has been established and regulations have been issued".[7]

Apart from the POPI Act which is the general legislation on data protection in South Africa, there is quite a number of legislation of sectoral application. These legislation have certain provision that have the implication of protecting individuals' with regard to the processing of their personal information. Notable among the legislation are The Promotion of Access to Information Act,[8] the Electronic

[2] *Ibidem.*

[3] See SALRC (2009).

[4] Section 115 of the POPI Act.

[5] *Ibidem.*

[6] See https://www.saica.co.za/Portals/0/Technical/LegalAndGovernance/37544_pro25.pdf.

[7] Roos (2016b), p. 203.

[8] Act No 2 of 2000.

hoeren@uni-muenster.de

Communications and Transactions Act (ECT Act),[9] the National Credit Act,[10] the Consumer Protection Act[11] and Regulation of Interception of Communications and Provisions of Communication-Related Information Act (RICA).[12]

Notwithstanding the foregoing, the POPI Act applies to the exclusion of any of the above-mentioned legislation where any of the latter has a provision which is inconsistent with any of the objective of the POPI Act.[13] This is however in as much as such other legislation does not have a more extensive provision on the processing of personal information than the POPI Act. If the other legislation has more extensive provision, then such other law applies.

The jurisprudence on privacy and data protection in South Africa is, arguably, still developing and that is why it may be difficult to find any particular case law on the protection of personal information especially with regard to any of the above mentioned legislation. Nevertheless, there are quite a number of cases which have the effect of protecting individuals when there is a violation of certain spheres of their privacy which has to do with their personal or private information. This is especially true in cases on section 14 of the South African Constitution which provides for the right to privacy.[14] For example, in analysing the decision of the South African Court in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*: *In re Hyundai Motor Distributors (Pty) Ltd v Smit,*[15] authors opine that section 14 of the Constitution could also be interpreted as protecting an individual's interest in his/her 'informational self-determination'.[16] Information self-determination is "an interest in restricting the collection, use of and disclosure of personal information".[17]

A number of international (regional) data protection instruments are relevant to South Africa. With regard to the African instruments specifically, there is African Union Data Protection Convention which is an instrument of the African Union of which South African is a member state.[18] However, South Africa has neither signed nor ratified the instrument.[19] Another regional instrument which is also relevant to South Africa is the Southern Africa Development Community (SADC) Model Law

[9]Act 25 of 2002. It must be explicitly stated that the provisions of this Act relating to data protection will be repealed when the POPI Act fully comes into force.

[10]Act 35 of 2005.

[11]Act 69 of 2008.

[12]Act 70 of 2002.

[13]Section 3(3)(a) of the POPI Act.

[14]Section 3(3)(a) of the POPI Act.

[15]No 2001(1) SA 545 (CC).

[16]Currie and de Waal (2013), pp. 302–303.

[17]*Ibidem.*

[18]The African Union Convention on Cyber Security and Personal Data Protection adopted in 2014. Available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

[19]See https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf.

hoeren@uni-muenster.de

on data protection.[20] However, authors opine that all these instruments have no significant influence on data protection in South Africa.[21]

2.2 The Meaning of Personal Data and the Right to Data Protection

According to the POPI Act, personal data (information)[22] is defined as "information relating to an identifiable living, natural person, and where it is applicable, existing juristic person".[23] The Act further gave a non-exhaustive list of personal information.[24] In a unique fashion, the Act made effort to harmonize other legislation relating to data privacy protection with its provisions especially with respect to the definition of personal information. It brought the definition of 'personal information' in the Access to Information Act to that contained in the Act by amending the provision of the latter.[25]

The right to personal data protection in South Africa, unlike some other jurisdictions in Europe, is not an independent right. It is a derivative of the right to privacy which is contained in section 14 of the South African Constitution. Scholars have interpreted the right to privacy to include both substantive privacy right and informational privacy.[26] The latter is that which covers aspects of the right to data protection. The POPI Act is explicit in this regard when it expressly upholds the constitutional right to privacy in its preamble and further provides that "the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information".[27] Notwithstanding the foregoing, other scholars have linked data protection to other human rights like the rights to dignity and personality.[28]

[20]For more incisive discussions on these instruments, Greenleaf and Georges (2014), pp. 18 ff.; Makulilo (2015), p. 78; Abdulrauf and Fombad (2016), pp. 67 ff.

[21]See Roos (2016b), pp. 223 ff.

[22]Although the POPI Act uses the term 'information' rather than 'data'; within the context of data protection law, one may argue that both mean the same thing. However, scholars like Bygrave and Roos have tried to distinguish between both terms. See Roos (2016a), p. 368; Bygrave (2013), p. 20. In this report, I will be using both terms interchangeably.

[23]Section 1, POPI Act.

[24]Section 1, POPI Act.

[25]Section the schedule to the POPI Act.

[26]McQuoid-Mason (2000), p. 248. See also Roos (2012), p. 395.

[27]See Preamble to the POPI Act.

[28]See for example, Neethling et al. (2005), p. 217. This is so even though the right to personality is not an independent right in the South African Constitution.

hoeren@uni-muenster.de

2.3 Categories of Personal Data in the POPI Act

The POPI Act provides a very wide and non-exhaustive list of both sensitive and non-sensitive personal information. In terms of the Act, personal data includes information such as that relating to race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, religion, conscience, belief culture, etc.[29] It includes information relating to education or the medical, financial, criminal or employment history of the person.[30] Personal information also includes, according to the Act, any identifying number, symbol, e-mail address, physical address, biometric information and the name of a person if it appears with other information relating to the person or if the disclosure of the name itself would reveal information about the person.[31] It must be reiterated that this list is not limited to the above mentioned categories.

The POPI Act seems not to discriminate between sensitive and non-sensitive information in its definition as it lumps together both classes. Nevertheless, the Act still makes a special provision for the processing of sensitive information which is termed "special personal information".[32] In terms of the Act, special personal information is personal information which relates to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject or information relating to the criminal behaviour of a data subject in specific contexts.[33]

There is a category of personal information which is completely excluded from the scope of the POPI Act. These are information which processing may present no potent risk on data subject based on the principle of *de minimis* or for public policy purposes. This category includes personal information processed for purely personal or household activity, that has been de-identified, for national security, crime detection and public policy purposes etc.[34]

2.4 The Scope of the POPI Act

The POPI Act covers processing of personal information, as narrowly defined, by both a responsible party who/which is domiciled in South Africa or makes use of means in South Africa. A responsible party, according to the Act, is "a public or private body or any other person who, alone or in conjunction with others,

[29] Section 1 of the POPI Act.

[30] *Ibidem*.

[31] *Ibidem*.

[32] See the whole of Part B of the POPI Act.

[33] Section 26 of the POPI Act.

[34] Section 6 of the POPI Act.

hoeren@uni-muenster.de

determines the purpose of and means for processing personal information".[35] As I have stated above, there are other sectorial legislation which covers the processing of personal information by certain bodies or category of persons. For example, the National Credit Act has provisions on the personal data processing in South Africa's credit sector. Nevertheless, the POPI Act provides that it has an overriding status especially where such other legislation has provision which is inconsistent with it.[36]

Remarkably, the South African POPI Act is unique in that it covers the processing of personal data relating to both natural and juristic persons by any of the above-mentioned entities.[37] This means that legal persons/entities (like corporation) are also entitled to protection from the processing of their personal information under the Act.

3 The Supervisory Authority: The Information Regulator

The supervising authority for the overall processing of personal data in South Africa is the Information Regulator which is established pursuant to section 39 of the POPI Act. In terms of the Act, the Information Regulator is an independent juristic body which has jurisdiction throughout South Africa.[38] This body is only subject to the Constitution and only accountable to the National Assembly.[39]

Furthermore, according to the Act, the Information Regulator consists of a Chairperson and four other persons as ordinary members of the Regulator.[40] Their appointment is either on full time or part time basis depending on the office.[41] Although, the POPI Act is yet to fully come into force, the Information Regulator has already been established and the officials have been appointed by the President.[42] The newly appointed Chairperson is Adv. Pansy Tlakula.[43] Advs. Lebogang Stroom-Nzama and Collen Weapond are the full-time members while Prof Tana Pistorius and Mr Sizwe Snail ka Mtuze are the part-time members.[44]

Before the Act fully comes into force, it is arguable that the court will play the role of enforcing data protection norms especially when it has to do with the processing of personal information in such a way that violates the right to privacy as stipulated under the South African Constitution.

[35]Section 1 of the POPI Act.
[36]Section 3 of the POPI Act.
[37]Section 1 of the POPI Act.
[38]Section 39 of the POPI Act.
[39]Section 39 of the POPI Act.
[40]Section 41 of the POPI Act.
[41]Section 41 of the POPI Act.
[42]See http://www.justice.gov.za/inforeg/about.html.
[43]http://www.justice.gov.za/inforeg/members.html.
[44]http://www.justice.gov.za/inforeg/members.html.

hoeren@uni-muenster.de

With regard to the Access to Information Act which has been listed among the sets of legislation with data protection implications, its provisions are being supervised currently by the South African Human Rights Commission (SAHRC).[45] The SAHRC merely has *de facto* and not *de jure* powers as it cannot enforce the provisions of the Act. The Commission can only give recommendations, submit report and exercise other sort of subtle powers. However, this will seize as soon as the Information Regulator is fully active especially when the act is totally in force. This is because the Information Regulator is to supervise the enforcement of both the POPI Act and the Promotion of Access to Information Act.[46]

3.1 The Structure of the Information Regulator

Generally, the supervision or enforcement of the provisions of the Act is to be carried out by one single supervisory body—the Information Regulator (or 'the Regulator'). This Herculean task is to be performed with the assistance of other entities. For example, it is stipulated in the Act that the Regulator may appoint "a suitably qualified and experienced person" as a chief executive officer to assist with the performance of its duties.[47] Furthermore, the Regulator must establish an Enforcement Committee.[48] The courts also have some enforcement powers under very well-defined circumstances.[49]

There seems to be no explicit provision in the Act which sanctions sectoral supervisory bodies. Nevertheless, the POPI Act has robust provision which enables the Regulator to issue code of conducts with specific sectoral application and supervise sector-specific data processing generally.[50] It would seem that this sector-specific supervisory role of the Regulator is a one-sided affair giving the Regulator so much latitude with regard to sectoral data processing. That may arguably not be the case given that the Act provides that the Regulator may issue a code of conduct on its own initiative "but after consultation with affected stakeholders or a body representing such stakeholders".[51] This does not however derogate form the fact that supervision is to a larger extent by the Information Regulator.

The point must also be made that every institution that falls within the scope of the POPI Act must also appoint an Information Officer who is generally to supervise

[45]Section 83(2) of the Promotion of Assess to Information Act.

[46]Section 39 of the POPI Act.

[47]Section 47 of the POPI Act.

[48]Section 50 of the POPI Act.

[49]See for example secs. 97, 98 and 99 of the POPI Act. However, I have argued elsewhere that the supervisory role of the court is very limited. See Abdulrauf (2016), p. 292.

[50]See Chapter 7 generally of the POPI Act.

[51]Section 61(1) of the POPI Act.

hoeren@uni-muenster.de

and ensure compliance with the provisions of the Act.[52] The Information Officer may also work with the Regulator in certain circumstances towards enforcement.[53]

3.2 The Functions and Powers of the Information Regulator

One outstanding feature of the POPI Act is the extensive provision it makes on the powers vested in the Information Regulator. In terms of section 40 of the Act, the highlights of the main powers, duties and functions of the Regulator are: Firstly, the Regulator is to provide education and give advice on issues relating to Act.[54] Secondly, it is the duty of the Regulator to monitor and enforce compliance with the provisions of the Act.[55] This role includes "undertaking research into, and monitoring developments in" issues regarding ICT. Thirdly, the Regulator is also to consult with interested parties on matters regarding data protection generally.[56] Fourthly, the Information Regulator must handle complaints on data protection violations and attempt to resolve these complaints.[57] Fifthly, it has the power to conduct research and report to Parliament on the suitability of any international instrument, or the need for any legislative amendments on any matter that has to do with data protection.[58] Other powers vested in the Information Regulator are the power to issue codes of conduct and the power to facilitate cross-border cooperation in the enforcement of privacy laws.[59] The Regulator can also "do anything incidental or conducive" to the performance of any of the above mentioned function and exercise powers conferred on it by other legislation.[60] One unique power of the supervisory authority in South Africa is power over matters concerning the Promotion of Access to Information Act.[61]

With regard to sanctioning specifically, the Information Regulator has broad powers. Complaints regarding interference with the protection of personal information of data subject may be handled in several ways by the Regulator. The Regular may first decide to investigate the complaint.[62] After investigating, it may decide to

[52]Section 50(1)(d) of the POPI Act.
[53]See Section 55 of the POPI Act.
[54]Section 40(a) of the POPI Act.
[55]Section 40(b) of the POPI Act.
[56]Section 40(c) of the POPI Act.
[57]Section 40(d) of the POPI Act.
[58]Section 40(e) of the POPI Act.
[59]Section 40(f) and (g) of the POPI Act.
[60]Section 40(1)(h) of the POPI Act.
[61]Section 40(1)(h) of the POPI Act.
[62]Section 76 of the POPI Act.

hoeren@uni-muenster.de

take no action, refer the matter to a regulatory body.[63] It may also settle the matter.[64] The Regulator may also approach the court for a warrant to search premises of a responsible party and seize property.[65] The Regulator may also serve an Information notice to a privacy infringer.[66] The Regulator furthermore has powers to issue an enforcement notice directing a responsible party to take certain steps or refrain from taking steps in terms of violation of a data subject's right.[67] Failure to comply with any of these notices is a criminal offence which is punishable under the Act.[68] A dissatisfied responsible party has the right to appeal to the court.[69]

At the instance of a data subject, a responsible party may institute a civil action for damages in a court for a breach of the provisions of the Act.[70] Furthermore, the Act contains specific offence and penalties such as obstruction of the Regulator and breach of confidentiality.[71] Finally, the Regulator has powers to impose an administrative fine on infringers.[72]

3.3 The Information Regulator and Self-Regulatory Instruments

The Regulator may issue code of conducts which are specifically tailored to meet the needs of sector-specific data processing. These codes of conduct may be issued in consultation with the affected stakeholders or a body representing such stakeholders.[73] I have argued above that this initiative may not be equated with self-regulation since the Regulator seems to have more powers with regards to the form and content of such a code. A proper self-regulation initiative, as the name implies, should allow the industry to make the instruments themselves which may only be ratified/approved by the Regulator. Nevertheless, it would seem that section 65 allows for a proper self-regulation in that it provides that the Regulator may provide written guidelines to assist bodies to develop code of conduct or apply approved codes of conduct.[74]

[63]Section 78 of the POPI Act.
[64]Section 80 of the POPI Act.
[65]Section 82 of the POPI Act.
[66]Section 90 of the POPI Act.
[67]Section 95 of the POPI Act.
[68]Section 103 of the POPI Act.
[69]Section 97 of the POPI Act.
[70]Section 99 of the POPI Act.
[71]Sections 100 & 101 of the POPI Act.
[72]Section 109 of the POPI Act.
[73]Section 61 of the POPI Act.
[74]Section 65 of the POPI Act.

hoeren@uni-muenster.de

Another area where self-regulation seems to be relevant under the POPI Act is in its provision on the exclusion of the application of the Act to journalistic, literary and artistic purposes.[75] It is provided that where personal information is processed *solely* for any of the above listed purposes, then the Act does not apply. However, this is not a blanket provision as the Act is inapplicable only where such information is processed "subject to a code of ethics that provides adequate safeguards for the protection of personal information".[76] Furthermore, it is provided that in the event of a dispute regarding the adequacy of such a code, regards may be had *inter alia* to "the nature and ambit of self-regulatory forms of supervision provided by the profession."[77]

Be that as it may, an approved self-regulatory instrument in the form of a code of conduct is very relevant in South Africa in that failure to comply with its provisions is dealt with as a failure to comply with certain principal provisions of the Act and is punishable as such.[78]

4 The Regulation of Data Processing in Specific Contexts

4.1 Data Processing by Electronic Means

The processing of personal information electronically is usually taken to mean the same as automated processing of personal information and as shown earlier, the POPI Act is applicable to both automated and manual processing.[79] This means the POPI Act, in its provisions, does not discriminate between processing of personal information electronically and manually. Information being processed by internet service providers, social networks providers, and online retail services are processing by electronic/automated means and are all within the scope of the Act.

The Electronic Communications and Transactions Act also has particular provision on protection of personal data in the context of services provided electronically. This will be discussed below.

4.1.1 Specific Protection in the Context of Electronic Data Processing

There are certain protections which are provided in some specific context of electronic processing. For example, the POPI Act makes extensive provision on the protection of persons with regard direct marketing by electronic means.

[75] Section 7 of the POPI Act.

[76] Section 7(2) of the POPI Act.

[77] Section 7(3)(e) of the POPI Act.

[78] Section 68 of the POPI Act.

[79] Section 3(1) of the POPI Act.

hoeren@uni-muenster.de

Specific protection is provided for electronic processing in the ECT Act which has provisions protecting consumers in the context of e-commerce generally. Section 50 of the Act provides that it "applies to personal information that has been obtained through electronic transactions". Section 51 of the Act outlines principles that are specifically applicable for electronic collection of personal information and a data controller must subscribe to all the principles as a whole.[80]

The ECT Act also has provisions, like the POPI Act, on unsolicited electronic communications for direct marketing purposes and also protection of personal information in the context of e-commerce.[81] The major snag of this legislation is its voluntary nature making its provisions non-binding.[82]

4.1.2 The Requirement of Consent in the Electronic Processing of Personal Data

Under the POPI Act, personal data may only be processed if the data subject consents.[83] This means that previous consent is paramount for the electronic processing (since the Act does not discriminate as noted in 4.1 above). Furthermore, the responsible party bears the burden of proof of consent.[84] I have argued elsewhere that the kind of consent required under the Act is 'explicit' or 'opt-in' consent.[85] Similarly, there are specific instances consent is crucial under the other conditions for processing of personal information contained in Chapter 3 of the Act.

There is no specific provision under the Act specifying circumstances in which electronic processing may be carried out without consent. However, there are provisions on exemption from conditions for processing of personal information generally.[86] It is my view that since consent is among the conditions for lawful processing, this exemption also specifically applies to consent. In terms of the Act, processing is not in breach of a condition for processing if the Regulator grants exemption (in terms of section 37) or if processing is in accordance with section 38.[87] Instances listed under section 37 are where Regulator is satisfied that such processing is: in the public interest[88] and for the benefit of the data subject or a third-

[80]Section 51 of the ECT Act.

[81]See. 45 of the ECT Act.

[82]See Roos (2016a), p. 428.

[83]Section 11 of the POPI Act.

[84]Section 11(2) of the POPI Act.

[85]See Abdulrauf (2016), p. 344.

[86]Chapter 4 of the POPI Act.

[87]Section 36 of the POPI Act.

[88]Public interest includes items that are usually contained under this head which includes national security, prevention and detection of crimes etc. see section 37(2) of the POPI Act generally.

hoeren@uni-muenster.de

party. In both mentioned cases, these interests must outweigh any interference with privacy.[89]

Section 38 on the other hand lists instances where the conditions may be exempted for the purpose of discharging a relevant function which includes function: of a public body or conferred on any person in terms of the law which is performed with the view to protecting members of the public against fraudulent activities generally.[90]

4.1.3 Protection of Minors in the Context of Electronic Processing

The POPI Act, like the European Union (EU) Data Protection Regulation, makes a special provision for the protection of children/minors. Section 34 as a general rule provides that personal information concerning a child should not be processed. However, section 35 gives conditions under which information of children may be processed. The conditions are that processing of a child's information can be carried out: with the prior consent of a competent person; when necessary for the establishment of a right or obligation in law; when necessary to comply with an obligation in public international law and for historical, statistical or research purposes.[91] The last condition is where a child, with the consent of a competent person, has deliberately made public his/her personal information.[92] According to the Act, a competent person is "any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child".[93]

4.1.4 The Right to Erasure/Be Forgotten in Electronic Processing of Personal Data

Unlike the EU Regulation, the POPI Act does not have an explicit right to be forgotten. However, Section 24 of the Act grants a data subject a right to correct or delete personal information in its possession or under its control if such information is, *inter alia,* inaccurate, irrelevant, excessive or out of date. A data subject may also request to destroy or delete a record of personal data that a responsible party is no longer authorized to retain in terms of section 14.[94] The request by the data subject must be made in a prescribed form.[95]

[89]Section 37 of the POPI Act.

[90]Section 38(2)(b) of the POPI Act.

[91]Section 35(1) of the POPI Act.

[92]Section 35(1) of the POPI Act.

[93]Section 1 of the POPI Act.

[94]Section 24 of the POPI Act.

[95]Section 24(2) of the POPI Act. More on the prescribed format is also contained in Section 3 of the Regulation Relating to the Protection of Personal Information Act 2017 made by the Information

hoeren@uni-muenster.de

4.1.5 Electronic Processing for Direct Marketing and the Nature of Consent

Both the POPI Act and the ECT Act make copious provisions for protection of personal data in the context of electronic communications for marketing purposes.

With regard to the nature of consent required, it is my view that with respect to electronic communication for direct marketing purposes, the POPI Act strangely establishes both the opt-out and the opt-in system. This is because section 69 (2) provides that the processing of personal information of a data subject for the purpose of direct marketing by means of electronic communication is prohibited unless a data subject has given his (prior) consent. Consent according to the Act is "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information".[96] This clearly shows an 'opt-in' system is envisaged. However, subsection 2 of section 69 provides that processing of personal data electronically for direct marketing purpose may be lawful if the data subject is a customer of the responsible party. The Act provides for some other conditions.[97] In this case, it is arguable that the responsible party can process by default and it is left for the data subject to object. This, in my view, shows an 'opt-out' system.

Unlike the POP I Act, the ECT Act unequivocally provides for an 'opt-out' system. In terms of the latter Act, "Any person who sends unsolicited commercial communications to consumers, must provide the consumer with an option to cancel his or her subscription to the mailing list of that person".[98] But then, it must be stated that all of the provisions of the ECT Act relating to data protection will be repealed when the POPI Act fully comes into force.[99]

4.1.6 Protection of Employees' Personal Data in the Context of Electronic Processing

The POPI Act has a broad scope to cover personal information processing of employees through electronic means provided it "forms part of personal information entered in a record by or for a responsible party making use of automated or non-automated means".[100] It does not discriminate in terms of personal information of employees.

Regulator. This can be found in http://www.justice.gov.za/inforeg/docs/InfoRegSA-RegulationsDraft-Aug2017.pdf.

[96]Section 1 of the POPI Act.

[97]See Section 69(3) of the POPI Act.

[98]Section 45 of the ECT Act. See also Roos (2016a), p. 425.

[99]See the Schedule to the POPI Act.

[100]See Section 3(1)(a) of the POPI Act.

hoeren@uni-muenster.de

There are no specific legislation with regard to data protection in employment relations in South Africa. Similarly, the South African courts have made little or no significant contribution in this regard.[101]

4.1.7 Security Obligations and Data Breach Notifications in the Context of Electronic Processing

A responsible party, under the POPI Act, has a strict duty of security safeguard of personal information in his possession by ensuring that he takes "appropriate, reasonable technical and organisation measure to prevent information for loss, damage or unlawful access".[102] Where there is a security compromise or there are reasonable grounds to believe so, there is an obligation to notify the Regulator and the data subject (in as much as the identity of the data subject can be ascertained).[103]

4.2 Data Protection in the Electronic Communication Sector

The Primary law regulating the electronic communications sector in South Africa is Electronic Communications Act 2005.[104] It does not make any serious provision on personal data protection. It merely provides that the Independent Communications Authority of South Africa may prescribe or impose through licence conditions in respect of directories and directory enquiry services, regarding, *inter alia,* the protection of personal data and the protection of privacy.[105]

It is therefore arguable that both POPI Act and the ECT Act are applicable in the context of processing of personal information in the electronic communication sector. In any case, the POPI Act has already provided that in the context of data protection, its provisions supersedes where it has more extensive provisions on the conditions for lawful processing.[106] With regard to the POPI Act specifically, there is a provision for protection of a data subject who is a subscriber to electronic directory of subscribers.[107] A subscriber within the context of the provision is defined as "any person who is party to a contract with the provider of publicly available electronic communication services for the supply of such services".[108]

[101] See generally Gondwe (2011).
[102] Section 19 of the POPI Act.
[103] Section 22 of the POPI Act.
[104] Act 36 of 2005. Also available at http://www.wipo.int/edocs/lexdocs/laws/en/za/za082en.pdf.
[105] Section 75 of the Electronic Communications Act.
[106] Section 3(2)(b) of the POPI Act.
[107] Section 70 of the POPI Act.
[108] Section 70(5) of the POPI Act.

hoeren@uni-muenster.de

4.3 Data Protection and Digital Forensics

The POPI Act permits the Regulator to exempt a processing of personal information from its provisions in the public interest.[109] The Act further specifies that public interest includes "the prevention, detection and prosecution of offences"[110] There are instances also in which certain requirement of the Act is relaxed for the purpose of investigation and detection of crimes. For example, it is among the principles of data processing that information must only be collected directly from the data subject.[111] However, there is no need to comply with this principle if it is necessary for prevention, detection, investigation, prosecution and punishment of offences.[112]

4.3.1 Interception of Communication Data: The Permitted Scope

There are a number of laws regarding interception of communication in South Africa. The primary legislation in this respect is the Regulation of Interception of Communications and Provision of Communications Related Act (RICA).[113] In as much as the communication involves personal information however, it is the POPI Act that will.

Intentional interception of communications is, as a general rule, prohibited under the RICA.[114] However, the Act provides instances where such interception may be lawful among which is for the purpose of investigation, detection and prosecution of crimes. Section 47 of the RICA provides that information regarding the commission of any criminal offence, obtained by means of any interception, or the provision of any real-time communication related information, under this Act may be admissible in evidence in any criminal or civil proceedings as specified under the Act. It does not appear that the Act restricts the scope of information that can be intercepted in so far as it is either a direct or indirection communication.[115]

The RICA also provides that telecommunication service providers must provide services which can intercepted.[116]

The RICA provides for requirements for interception depending on the context and the purpose of the interception. For example, it provides that interception may take place when a person has an interception direction. An interception direction is a direction authorizing interception based on the provisions of the RICA. The

[109]Section 37(1) of the POPI Act.

[110]Section 37(2)(b) of the POPI Act.

[111]Section 12 of the POPI Act.

[112]Section 30(2)(d) of the POPI Act.

[113]Act 70 of 2002. Also available at http://www.saflii.org/za/legis/num_act/roiocapocia2002943.pdf.

[114]Section 2 of RICA.

[115]Section 1 (2) of RICA.

[116]Section 30 (1)(a) of RICA.

hoeren@uni-muenster.de

interception direction is usually issued by a designated judge upon an application if he is satisfied, *inter alia*, that "a serious offence has been or is being or will probably be committed".[117] Similarly, the designated judge must be satisfied that there are reasonable grounds to believe such relevant information will be obtained by the interception and most importantly, that "Other Investigative procedures have been applied and have failed to produce the required evidence".[118]

4.3.2 Data Retention

The POPI Act, ECT Act and RICA Act all have provisions on data retention with different scopes. It is pertinent to note that in all these legislation, it is not explicit that the purpose of retention is for the investigation and prosecution of crime but one can safely infer that objective.

The ECT Act, in its section 16, provides for retention of information which may include personal data.

The RICA places an obligation on telecommunication service provides (and retailers of telecoms facilities) to obtain and keep copies of certain personal information of consumers like information on his or her full names, identity number, residential and business address or postal address.[119]

The POPI Act also allows for the retention of personal data by a responsible party in circumstances authorized by law.[120] This circumstance may be interpreted to include national security interests.

4.4 Data Protection and Electronic Surveillance for Security and Defence Purposes

The POPI Act, arguably, has the most succinct provision on data protection and electronic surveillance for security and defence purposes. The RICA also has provisions authorizing electronic surveillance/interception of communications for national security and defence purposes.

4.4.1 The Scope

With regard to national security matters, the POPI Act provides that it does not apply to the processing of personal information by or on behalf of a public body "which

[117] S16 (5)(a) of RICA.

[118] S16 (5)(b), (c) of RICA.

[119] Secs. 39(1) and 40(1) of RICA.

[120] Section 14(1)(d) of the POPI Act.

hoeren@uni-muenster.de

involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety".[121] Also on national security, the POPI Act is inapplicable when the processing is for prevention and detection or assistance to locate proceeds of unlawful activates and the combating of money laundering activities.[122] Some of the conditions for lawful processing are also suspended on the grounds of national security. For example, the principle of collection directly from the data subject may be excluded in the interest of national security in terms of the Act.[123] The Regulator may also exempt certain processing if it is satisfied that national security interest outweighs the interest of privacy and data protection.[124]

With regard to the RICA, section 16(5) permits a judge to grant an interception direction when he is satisfied, on the facts alleged, that there are reasonable grounds to believe that the gathering of information (which may include personal information) concerning an actual or potential threat to national security is necessary.[125] Furthermore, the judge must be satisfied that only relevant information will be obtained by such interception and other investigative procedures have been applied and failed.[126]

Under the RICA, the designated judge may also grant a real-time or archived communication-related direction for national security purposes.[127]

In respect of the POPI Act, its exclusion from national security matters only applies "to the extent that adequate safeguards have been established in legislation for the protection of such personal information".[128]

Under the RICA, interception of communication, as stated in 23.1 above, can only be carried out for national security purposes with an interception direction from a designated judge under well-defined circumstances.

4.5 Remedies and Sanctions

Various remedies are available in the POPI Act for a breach of data protection in the context electronic processing. As mentioned earlier, the Act does not discriminate regarding electronic processing or if it is in a context of services provided at a distance. The general data protection rules are applicable in all processing which

[121] Section 6(1)(c) of the POPI Act.
[122] Section 6(1)(c) of the POPI Act.
[123] Section 12(2)(d) of the POPI Act.
[124] Section 37(2) of the POPI Act.
[125] Section 16 (5)(a) (ii) and (iii) of RICA.
[126] Section 16(5)(c) of RICA.
[127] Section 17(4) of RICA.
[128] Section 6(1)(c) of the POPI Act.

hoeren@uni-muenster.de

falls within the scope of the Act and as such, the remedies are general to all kinds of violations of protection of personal data.

A complaint on interference with protection of personal information by a data subject may cause the Regulator to conduct a pre-investigation or a full investigation.[129] The Regulator may refer the complaint to the enforcement committee.[130] At the end of the investigation, the Regulator may decide to take no action.[131] The Regulator may refer such complaint to the regulatory body to handle if such is within the jurisdiction of another regulatory body.[132] The Regulator could also cause a settlement between the parties if it appears that it is possible to do so.[133] The Regulator can approach the court for a warrant to enter, search and seize property.[134] The Regulator can finally issue an enforcement notice requiring an infringer or a responsible party to take or refrain from taking specific steps or to stop processing based on the notice.[135] Other remedies especially civil and criminal are discussed below. However, these remedies can only be carried out with the assistance of the courts.

Section 73 of the POPI Act considers non-compliance with the rules on electronic communications for direct marketing purposes as an interference with the protection of personal information and could be a ground for civil action for damages based on section 99. Details are provided below.

As mentioned below, a breach of the rules on security of personal data processed electronically (which is among the conditions for lawful processing) is considered as an interference with the protection of personal information[136] and this could be a ground for action in court for damages.[137] The Regulator may also impose an administrative fine.[138]

As mentioned earlier, the general data protection legislation in South Africa is yet to fully come into force. Hence, although the main supervisory body (Information Regulator) has been set up, it is yet to be fully functioning. The penalty for the breach of the provision of the POPI Act, if considered criminal, may be up to 12 months to 10 years with or without fine.[139] Furthermore, it is provided that the Information Regulator has the power to impose, in lieu of a criminal action, an administrative fine of up to R10 million (10 Million South African Rands).[140] Some commentators

[129] See Section 76(1) of the POPI Act.
[130] Section 76(1) of the POPI Act.
[131] Section 77 of the POPI Act.
[132] Section 78(1) of the POPI Act.
[133] Section 80 of the POPI Act.
[134] Section 82 of the POPI Act.
[135] Section 95 of the POPI Act.
[136] Section 73 of the POPI Act.
[137] Section 99 of the POPI Act.
[138] Section 109 of the POPI Act.
[139] Section 107 of the POPI Act.
[140] Section 109(2) (c) of the POPI Act.

hoeren@uni-muenster.de

contend that this fine is even higher than what is obtainable in UK and most of Europe.[141] So far, the Regulator has not exercised any of its enforcement powers.

It is not explicit whether it is possible to appeal to the court but it must be stated that the penalties are usually imposed with the support of the courts.[142]

5 The Extra-Territorial Reach of South Africa's Data Protection Framework

5.1 The Territorial Scope of Rules on Data Protection

The territorial scope of application of data protection rules is clearly defined under the POPI Act. Section 2 provides that the Act applies to processing of personal information (including electronic processing) by a responsible party where he is domiciled in the Republic (Republic of South Africa).

It goes without saying that the ECT Act and all the other legislation cited in this chapter are only applicable in South Africa.

Section 2 of the POPI Act further provides that the Act is also applicable where the responsible party is "not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic".[143]

5.2 Transfer of Personal Data to a Foreign Jurisdiction

The general rule under the POPI Act is that transfer of personal data to a third party in a foreign jurisdiction is prohibited.[144] However this rule, like Article 25 of the EU Directive and the Article 44 of the EU Regulation, is subject to some exceptions according to the Act, which are:

Firstly, where the third party recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that upholds the general principles of data processing which are substantially similar to the conditions for lawful processing under the Act.[145]

Secondly, where the data subject consents to such transfer.

---

[141] See Protection of Personal Information Act (POPI) - Ten things to know http://www.nortonrosefulbright.com/knowledge/publications/119575/protection-of-personal-information-act-popi-br-ten-things-to-know.

[142] See Secs. 99 and 107 of the POPI Act.

[143] Section 2(1)(b) of the POPI Act.

[144] Section 72(1) of the POPI Act.

[145] See Section 72(1) (a) of the POPI Act generally.

hoeren@uni-muenster.de

Thirdly, where the transfer is necessary for the performance of a contract between the data subject and the responsible party.

Fourthly, where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party and finally, where the transfer is beneficial to the data subject to some conditions.[146]

5.3 *Liability for Unlawful Processing of Personal Data in South Africa*

There is liability for unlawful processing of personal data in South Africa whether or not there is a resultant damage. Unlawful processing in this circumstance is a processing which infringes on any of the stipulated conditions for lawful processing under the Act.[147] The POPI Act lists instances of interference/violation with the provisions of the Act in section 73 and provides in section 99 that a data subject or the Regulator, may institute a civil action for damages against an infringer for the breach of any of the provision of the Act. Indeed, the POPI Act shows the uniqueness of data protection law by explicitly stating that liability attracts a penalty whether or not there is intent or negligence on the part of the responsible party.[148]

After hearing the matter as above, the court may award an amount which is just an equitable.[149] This amount could include "payment of damages as compensation for patrimonial; and non-patrimonial loss suffered by a data subject as a result of a breach of the provisions of the Act".[150] Similarly, the court may award an amount as aggravated damages based on its discretion.[151]

The POPI Act also creates offences as liabilities for unlawful for unlawful processing in South Africa. A person may be imprisoned, fined or both depending on if such offence falls into the category of serious or less serious offence.[152] For example, failure of a responsible party to comply with an enforcement notice is considered a serious offence.[153] Less serious offences include failure of a responsible party to notify the Regulator or the data subject for processing that needs prior

[146]Sec 72(1)(a) of the POPI Act.

[147]Except of course such processing falls within exceptions or exempted category under the Act.

[148]Section 99 of the POPI Act.

[149]Section 99(3) of the POPI Act.

[150]Section 99(3) of the POPI Act.

[151]Section 99(3) of the POPI Act.

[152]Section 107 of the POPI Act. See also Roos (2016a), p. 475.

[153]Section 103(1) of the POPI Act.

hoeren@uni-muenster.de

authorization.[154] Imprisonment period could range from 12 months to 10 years with or without fine.[155]

In lieu of a criminal proceeding, the Regulator may also impose an administrative fine.[156]

The ECT Act on its part does not impose legally binding obligations which means a breach of a principle will be treated like a breach of contract with the data subject.[157] However, as earlier mentioned, the provisions of the ECT relating to data protection will seize to be applicable when the POPI Act fully comes into force.

6 Conclusion

The protection of personal data in the internet in South Africa is to be achieved through a host of legislation and other legal instruments which have specific or general application. However, what seems to be like a 'patchwork quilt' has now been consolidated and harmonized with the recently enacted POPI Act. This law is the omnibus data protection instrument for South Africa and comprises sweeping provisions which is applicable to a broad range of sectors. Unfortunately, more than five years since the law was enacted, it is yet to fully come into force. Although the office of the supervisory agency has now been established, it is also yet to be fully effective since the law is yet to be enforceable. All this has, unfortunately, slowed down the process of development of the jurisprudence on data protection in South Africa. For now, just sectorial laws are however applicable. This is asides the well-developed jurisprudence on the constitutional and common law protection of privacy in South Africa. Be that as it may, this cannot be a potent substitute for a fully enforceable data protection law. It is hoped that the South African government will do the needful and make the POPI Act fully operational as soon as possible.

References

Abdulrauf LA (2016) The legal protection of data privacy in Nigeria: lessons from Canada and South Africa. Unpublished LL.D thesis, University of Pretoria

Abdulrauf LA, Fombad CM (2016) The African Union's Data Protection Convention 2014: a possible cause for celebration of human rights in Africa. J Media Law 8(1):67

Bygrave LA (2013) Data privacy law: an international perspective. Oxford

Currie I, de Waal J (2013) The bill of rights handbook. Claremont

[154]Section 59 of the POPI Act.

[155]Section 107 of the POPI Act.

[156]Section 109 of the POPI Act. See also Roos (2016a), p. 476.

[157]Roos (2016a), p. 428.

hoeren@uni-muenster.de

Gondwe M (2011) The protection of privacy in the workplace: a comparative study. Unpublished PhD thesis, Stellenbosch University
Greenleaf G, Georges M (2014) The African Union's Data Privacy Convention: a major step toward global consistency. Priv Laws Bus Int Rep 131:18
Makulilo AB (2015) Myth and reality of harmonization of data privacy policies in Africa. Comput Law Secur Rev 31:78
McQuoid-Mason DJ (2000) Invasion of privacy: common law v constitutional delict – does it make a difference? Acta Juridica 227:248
Neethling J, Potgieter JM, Visser PJ (2005) Law of personality. LexisNexis, Durban
Roos A (2012) Privacy in the Facebook era: a South African legal perspective. South Afr Law J 129:395
Roos A (2016a) Data privacy law. In: Van der Merwe DP et al (eds) Information and communication technology law, 2nd edn. Durban, p 368
Roos A (2016b) Data protection in South Africa. In: Makulilo AB (ed) African data privacy law, p 223
SALRC (2009) Privacy and data protection report. Available at http://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf

hoeren@uni-muenster.de

Data Protection in the Internet: National Report Spain

Felisa María Corvo López

1 General Data Protection Framework

1.1 Spanish Legal Framework

The framework regarding data protection in Spain is laid out by Organic Law (hereafter, OL) 15/1999 of 13 December on the Protection of Personal Data (hereafter, OLPPD), developed in the Regulation approved by Royal Decree 1720/2007 of 21 December (hereafter, ROLPPD).[1] However, there is currently an OL project being worked upon, which was presented on November 17, 2017[2]; although the essential content of the fundamental right to data protection must be regulated by way of an organic law, Royal Decree-Law 5/2018 of 27 July has recently adopted some urgent measures in order to adapt our regulations to the requirements of the General Data Protection Regulation (hereafter, GDPR).

1.2 The Notion of Personal Data

Art. 18 of the Spanish Constitution (hereafter, SC) establishes: "The right to honour, to personal and family privacy, and to the own image is guaranteed." Art. 18.4 SC

This report was finalised and sent forward for publication on 17th October 2018.

[1]For more information about this topic, see Martínez Martínez (2009).

[2]It's interesting to take into account this work: López Álvarez (2016).

F. M. Corvo López (✉)
University of Salamanca, Salamanca, Spain
e-mail: marcorvo@usal.es

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_15

hoeren@uni-muenster.de

adds: "The law shall restrict the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights." According to the doctrine of the Constitutional Court of Spain (hereafter, CC), the protection of personal data is a fundamental right, which is closely related to the right to privacy but independent of it, and it is characterised by the fact that it guarantees people the control of the use of their personal data (especially their use and destination), in order to prevent its trafficking, which may be illicit or harmful to the dignity or the rights of those affected.[3]

The OLPPD gives special protection to personal data related to ideology, trade union membership, religion, beliefs, racial origin, health, or sex life. Personal data which reveal the ideology, trade union membership, religion and beliefs may be processed only with the explicit and written consent of the data subject, who must be warned of their right not to declare their ideology, religion or beliefs. Personal data which refer to racial origin, health, or sex life may only be collected, processed or transferred when, for reasons of general interest, this is so provided for by law, or when the person affected has given explicit consent. These data may be processed when necessary for medical purposes of prevention or diagnosis, the provision of medical care or treatment, or the management of health-care services, provided such data processing is effected by a health professional subject to professional secrecy or by another person also subject to an equivalent obligation of secrecy; and also when it is necessary to safeguard the vital interests of the data subject or another person in the event that the data subject is physically or legally incapable of giving consent.

The current OLPPD is applied to personal data recorded on a physical support which makes them capable of being processed and to any type of subsequent use of such data by the public and private sectors. But data processing by the public administrations (hereafter, PA) features some peculiarities: *i.e.*, files of PA may only be created, modified or deleted by means of a general provision published in the Official State Gazette or in the corresponding regional official gazette; consent is not required when the personal data are collected by PA to exercise their functions within the scope of their responsibilities; personal data on criminal or administrative offences may be included in files of the competent PA only under the circumstances laid down in the respective regulations; personal data collected or drawn up by PA in the exercise of their tasks shall not be communicated to other PA for the exercise of different powers or powers relating to other matters unless the communication is for the purpose of subsequent processing for historical, statistical or scientific purposes; personal data obtained or drawn up by a PA on behalf of another administration may be communicated; the right of information about data collection is transferred whenever it would affect national defence, public safety or the prosecution of criminal offences.

[3]See CC judgement 254/1993 of 20 July; 290/2000 of 30 November; and 292/2000 of 30 November. For more information on this, see, *inter alia*, Conde Ortiz (2005).

hoeren@uni-muenster.de

1.3 The Supervision Authorities

In Spain, the role of ensuring compliance with the rules on data protection is attributed to the Spanish Data Protection Agency (hereafter, SDPA). It is a publicly constituted legal body with legal personality, an independent body with its own budget and full functional autonomy that acts in accordance with the provisions of the OLPPD and its own statute.[4] It is subject to administrative law both in the exercise of its powers and with regard to its property and recruitment regimes.

Art. 28.1 of Directive 95/46 establishes that "Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by them." That is the reason why, in Spain, different autonomous agencies have been created: in Madrid (2001), in Catalonia (2003), in the Basque Country (2004) and in Andalusia (2014). The Data Protection Agency of the Community of Madrid was abolished in 2013 and its functions were assumed by the SDPA.

The SDPA is responsible for ensuring compliance with legislation on data protection and monitoring its implementation, especially with regard to the rights of information, access, rectification, opposition and cancellation of data (ARCO rights). Its functions are contained in Art. 37 of the OLPPD and can be succinctly described as follows:

A. In connection with those affected

- Complying with their requests and complaints.
- Reporting about the rights recognized in the law.
- Promoting campaigns through the media.
- Ensuring the publicity of data files of a personal nature.

B. In relation to those processing data

- Issuing authorisations provided for in the law.
- Demanding corrective action.
- Ordering, in case of illegality, termination of the treatment and cancellation of data.
- Exercising the power of sanction under title VII of the OLPPD.
- Asking those responsible for processing files for assistance and information necessary for the exercise of its functions.
- Authorizing international transfers of data.

C. In relation to the development of standards

- Compulsorily report on the draft standards that develop the OLPPD.
- Reporting on draft regulations that involve data protection.
- Issuing precise instructions and recommendations to adapt automatic processing to the principles of the OLPPD.

[4]Royal Decree 428/1993 of 26 March, which approves the statute of the SDPA.

hoeren@uni-muenster.de

- Making recommendations for the implementation of the laws and regulations in the field of data security and control of access to the files.

D. Telecommunications

- Protecting the rights and guarantees of subscribers to and users in the field of electronic communications, including the sending of unsolicited commercial communications conducted via e-mail or equivalent electronic media (spam).
- Receiving notifications of any security breaches that may occur in the systems of service providers of electronic communications, and which may affect personal data.

E. Other functions

- Cooperating with various international agencies and with bodies of the European Union in the area of data protection.
- Representing Spain in international forums.
- Controlling and enforcing the provisions established in the Government Statistics Function Act.
- Drafting an annual report, presented the Director of the SDPA before the Parliament.

1.4 The Self-Regulation Instruments on Data Protection

Ethical codes or codes of conduct are an instrument of what we call self-regulation, *i.e.*, the ability of organizations and entities them to regulate themselves. These codes are described in Art. 32 of the OLPPD. They adapt the regulations included in OLPPD and ROLPPD to the specific characteristics of the operations carried out by those who adhere to them voluntarily, and they may or may not contain detailed operational rules for each particular system or technical standard. The SDPA publishes in its website the codes included in its General Registry and in the local registries.[5] We can highlight, for example, their use in the fields of health or insurance.

[5]Currently registered codes are available at https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index-ides-idphp.php. (Last accessed date 12 Feb 2018).

hoeren@uni-muenster.de

2 Specific Problems Concerning Data Protection in the Internet

2.1 Personal Data Processed by Electronic Means

2.1.1 Regulatory Framework

The current framework regarding personal data processed by electronic means in Spain is laid out by Law 34/2002 of 11 July on Information Society Services and Electronic Commerce. This regulation includes a broad concept of "services of Information Society" which, apart from the procurement of goods and services through electronic means, also applies to the supply of information through those means, the mediation activities related to the provision of access to the network, data transmission through telecommunication networks, the creation of temporary copies of internet pages requested by users, hosting information services or applications supplied by third parties on those servers, or the provision of tools to search or link other internet sites, as well as any other service requested individually by the users, providing that it represents an economic activity for those offering these services. Regulations in this law regarding data protection do not rule out the application of the OLPPD. Both laws can be applied to social networks.

Law 34/2002 does not exclude the implementation of regulations that protect the interests of consumers. We have to remember, then, Art. 98 of Royal Legislative Decree 1/2007 of 16 November that approves the recast text of the General Law on the Defence of Consumers and Users and other complementary laws (hereafter, RTGLDCU). As referring to distance contracts, the provider must give the consumer and user the information required by Art. 97.1 in the language used in the contract proposal or in the language chosen to sign the contract, as well as in Spanish. Alternatively, the provider may make this information available with the distance communication techniques used, in clear and understandable terms, and they must follow, specifically, the principles of good faith in commercial transactions, as well as the principles governing the protection of those who are unable to give their consent. The regulation also states that whenever that information is transmitted in a lasting medium, it must be legible. When a distance contract is signed, the employer must give the consumer and user confirmation of the contract that has been signed in a lasting medium and within a reasonable time (at the latest, before the goods are delivered or before the service starts to be provided).

2.1.2 Requirement of Prior and Informed Consent

According to Art. 6 of the OLPPD, processing of personal data requires the unambiguous consent of the data subject, except when:

a) the law states otherwise;
b) personal data

hoeren@uni-muenster.de

- are collected for the exercise of the functions of PA within the scope of their responsibilities;
- refer to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and are necessary for its maintenance or fulfilment;
- are contained in sources accessible to the public and their processing is necessary to satisfy the legitimate interest pursued by the controller or the third party to whom the data are communicated, unless the fundamental rights and freedoms of the data subject are jeopardised;

c) the purpose of processing the data is to protect a vital interest of the data subject.

This aspect is mentioned in Art. 22 of the Law 34/2002 with regard to the use by service providers of devices to store and retrieve data in terminal equipment owned by the users. In its ninth additional provision, Law 34/2002 establishes that service providers in the Society of Information, domain name registries and registry agents operating in Spain must cooperate with the competent CERT to solve any cyber security incidents that may affect the internet, and they must follow the security guidelines established in the codes of conduct that derive from this law. This cooperation includes submitting all the technical evidence necessary to prosecute crimes derived from said cyber security incidents: maintaining the secrecy of communications, they will supply all necessary information, including IP addresses that may be compromised by or involved in the crimes.

Furthermore, we must take into account that personal data may only be collected for the specified, explicit and legitimate purposes of the data controller. Data controllers must previously inform data holders about the purposes of collecting the data requested. The processing has to be restricted to personal data which are adequate, relevant and not excessive in relation to the purposes for which they were obtained (Art. 5 and 6 OLPPD, 8 ROLPPD).

2.1.3 Protection of Minors' Personal Data Processed by Electronic Means

According to Art. 13 of the ROLPPD, "Data pertaining to data subjects over fourteen years of age may be processed with their consent, except in those cases where the law requires the assistance of parents or guardians in the provision of such data." The consent of parents or guardians shall be required for children under 14 years old. The precept adds that data regarding information about any other member of the minor's family unit, or about their characteristics, cannot be collected from the minor (*e.g.* data relating to the professional activity of the parents, financial information, sociological data or any other kind), without the consent of the persons to whom such data refer. Nevertheless, data regarding the identity and address of the father, mother or guardian may be collected for the sole purpose of obtaining the authorisation set out above. The law underlines the idea that information regarding data processing aimed at minors shall be expressed in easily understandable language, with express

hoeren@uni-muenster.de

indication of the provisions of this Article; and emphasises the duty of the data controller to set up the procedures that guarantee that the age of the minor and authenticity of the consent given by the parents, guardians or legal representatives have been effectively checked. The draft of the OL reduces the age when the minor may give his consent to 13 years.

OL 1/1996 of 15 January, on the Legal Protection of Minors, for its part, allows the collection and processing of all necessary data without consent of the minor concerned (including data related to the minor, their social or family environment) in order to adopt appropriate protection measures to safeguard the best interests of the minor. In this regard, the general regulations on data protection must be followed, and high security measures must be adopted (Art. 22d).[6]

2.1.4 The Right to Be Forgotten

Spanish law does not regulate the "right to be forgotten" but establishes the rights of rectification, cancellation and opposition (Art. 16 and 17 OLPPD). In order to exercise the rights of cancellation and opposition, the citizen must address primarily the entity that has the data. If the entity does not answer the request made or the citizen thinks that the answer is wrong, the citizen may ask the SDPA to supervise that the entity responsible fulfils its obligations. Depending on the circumstances of each particular case, the Agency shall determine whether the request for cancellation or opposition is applicable or not. This decision of the Agency, in turn, may be appealed to the courts.[7]

2.1.5 The Protection of Personal Data in the Context of Electronic Communications for Marketing Purposes

Law 34/2002, OLPPD and its secondary legislation (particularly those regulations related to the collection of personal data, information to interested parties, creation and maintenance of personal data files), RTGLDCU, Law 9/2014, of 9 May, the General Telecommunications Act (hereafter, GTA) and the regulations on advertising, cover the protection of personal data in the context of electronic communications for marketing purposes.

In accordance with the provisions of Art. 21 of Law 34/2002, it is forbidden to send marketing or promotional communications through electronic mail or any equivalent electronic communication medium which has not been previously requested or expressly authorized by the recipients of the messages. This prohibition

[6]For information on this subject, see Andreu Martínez (2013).

[7]The application of the doctrine of the European Court of Justice in its judgement of 13 May 2014 (CJEU 2014\85) by Spanish courts is particularly relevant. See, *inter alia.* Corvo López (2017), pp. 175–245.

hoeren@uni-muenster.de

is not applicable when there is a prior contractual relationship, or if the service provider obtained the contact information of the client legally and used it to send commercial messages related to products of services of their own company which are similar to those that were initially contracted by the client. In any case, the provider must offer the client the possibility to oppose to the processing of their data with promotional purposes through a simple and free procedure, both at the moment of collecting the data and in each commercial message sent to them. If communications are sent through electronic mail, the message must include a valid electronic address where the client can exercise that right.

It is possible to restrict spam by registering our data for free and voluntarily in an opt-out list (Robinson List, run by the Spanish Digital Economy Association).

Art. 48.3 c) of Law 9/2014 recognizes the right not to be listed in the telephone directory.

The Advertising Self-Regulation Association has designed a system of voluntary mediation that makes it possible to receive a swift answer regarding complaints which may affect the processing of personal data, such as unwanted advertising.

2.1.6 Protection of Employees' Personal Data Processed by Electronic Means[8]

There are no specific regulations in this field, but our case law has admitted this processing based on the following arguments:

- The regulation on data protection is not applicable to data processing for legal entities or companies, or to files that just collect data from individuals who work for those entities or companies, which contain their name and surname, the job or the task they perform there, as well as the postal or electronic address and work telephone or fax numbers (Art. 2.2 ROLPPD). Data processing containing additional data is subject to OLPPD.
- Processing of personal data does not require the unambiguous consent of the data subject when the law states otherwise or when the data processing refers to the different parties in a contract or preliminary contract for a business, employment or administrative relationship, and are necessary for its maintenance or fulfilment (Art. 6 OLPPD). Art 20.3 of the Statute of Workers Rights (hereafter, SWR) authorizes the employer to adopt the necessary monitoring and control measures to verify that the worker fulfils their obligations and duties at work, with due observance of human dignity in this process (. . .). These measures may include the capture and/or processing of images or the installation of a GPS device in the work mobile phone of the worker or in a vehicle used by the worker without the worker's consent, because this processing is carried out to manage the working relationship. Notwithstanding, those practices are completely subject to the

[8] Another topic that may be of interest is Data protection in the area of job search processes. On this subject see García Coca (2016).

hoeren@uni-muenster.de

OLPPD and to Instruction 1/2006 of 8 November of the SDPA on the processing of personal data with monitoring purposes through cameras or video cameras,[9] and they must meet a series of specific requirements: (1) the worker must be informed (the worker must be aware that the measure will be adopted and that the data collected, for example, with the GPS device, may be used to sanction and dismiss them); (2) the proportionality principle must be applied: the measure will only be adopted if more appropriate measures cannot be adopted[10]; (3) the data must be adequate, pertinent and not excessive with regard to its sphere of action and the purposes for which they were collected (purposes established in the SWR and legal purposes allowed by the existing regulations); (4) the right to privacy,[11] the fundamental right to data protection and the right to self-image must be respected. In the case of the processing of personal data for monitoring purposes through cameras or video cameras, the data will be cancelled—according to Instruction 1/2006—within a maximum of 1 month, and only those images that record an infraction of working obligations or a breach of contract may be stored.

In the field of video surveillance, the CC judgements 29/2013 of 11 February and 39/2016 of 3 March and the Supreme Court judgement of 13 May 2014 (RJ 2014, 3307) are particularly relevant, and they reveal that: (1) the use of these measures to prove an infraction at work requires that the worker has been previously informed; (2) failure to warn the worker about the purposes of the working surveillance associated to the capture of images of the workers could invalidate the evidence in case of dismissal or any other sanction, because it affects the fundamental rights of the individual. See also ECHR judgement (third section) of 9 January 2018, in the *case of López Ribalda v. Spain*, in which the employer had informed the workers about the visible cameras, but not about the hidden ones.

Similar conclusions can be reached with regard to geolocation data: the judgements from the Madrid High Court of Justice (hereafter, HCJ) of 21 May, 2014 (AS 2014\823), Madrid HCJ of 29 September, 2014 (AS 2014\2981), Andalusia HCJ of 19 October, 2017 (JUR 2018\12280),[12] state that if the employer wants to use GPS devices, they must inform the workers beforehand and warn them about the purposes of said surveillance, and this control must be strictly limited to the duration of the working hours.

[9]With regard to Instruction 1/2006, the Legal Report 0019/2007 and Legal Report 0212/2007 of the SDPA specify that the reproduction of images in real time, even if they are not recorded, constitutes an act of data processing which lies within the scope of application of Instruction 1/2006 and the OLPPD.

[10]The proportionality principle is observed if: (a) the measure is susceptible of achieving its purpose (judgement of suitability); (b) there is no other more moderate measure that may achieve its purpose with the same effectiveness (judgement of necessity); (c) the measure is balanced (judgement of strict proportionality) [*e.g.* CC judgements 10/2000 of 10 July and 39/2016 of 3 March].

[11]Right recognized in Art. 4.2 e) of the SWR.

[12]The SDPA had previously issued its Report 193/2008 on the possibility of using GPS systems to control the activity of workers. The report insists that the file generated must be included in the General Registry of Data Protection of the SDPA.

hoeren@uni-muenster.de

With regard to the use of internet and corporate electronic mail, the Report from the SDPA 0464/2013 reminds us that the jurisprudence in those cases admits that the employer can control those media, provided that they have previously informed or warned the worker about the conditions of use and control [*e.g.* Supreme Court judgement of 26 September 2007, and CC judgement 170/2013 of 7 October].

The employer must respect the dignity of the worker when carrying out surveillance and control activities (Art. 20 SWR). According to the judgement from the Supreme Court of 6 October 2011 (RJ 2011, 7699), the right to the worker's dignity is not violated when instructions have specifically been given or when the employer has specifically stated that the computer may not be used for personal activities and can only be used for strictly professional purposes. In those cases, company records and surveillance of the computer without previous warning to the worker are completely legitimate. However, if the employer did not give specific instructions about the use of internet and the worker used the computer for private activities, it is possible to interpret that there are certain "expectations of confidentiality" and, therefore, the records and surveillance must respect the dignity of the worker. Consequently, a disciplinary dismissal has been considered lawful when the use of social networks during working hours has been interpreted as excessive [Judgement from the HCJ of the Community of Valencia of 12 February 2013 (JUR 2013 \1923299)], and it has been deemed unlawful when the behaviour of the worker was not of such serious nature and the employer had not issued a previous warning about possible restrictions in this regard or about surveillance activities related to it [Judgement of the Madrid HCJ of 28 April 2011 (AS 2011\1148)].

Comments posted by workers on social networks may also justify dismissal. This was the case, for example, in the judgement from the Castilla-La Mancha HCJ of 8 April 2016 (JUR 2016\97676), Galicia HCJ of 8 October 2014 (AS 2014\2738) or Castile and León HCJ of 21 April 2010 (AS 2010\1854). The judgements from the Murcia HCJ of 14 May 2012 (JUR 2012\229141) and the HCJ of the Community of Valencia of 18 February 2016 (JUR 2016\141128), on the other hand, have declared the nullity of the dismissal because they interpreted that the comments were protected by the right to free speech.

Employers also use the public sphere of life shared by the worker on social networks to justify a dismissal, particularly when the worker is in a situation of temporary inability. Our jurisprudence has deemed that these were lawful dismissals because there was a transgression of contractual good faith, and they have argued that the workers' right to privacy and their own image is not violated when the images (for example) submitted as evidence were obtained from a public Facebook account that did not require any kind of password [*e.g.* judgements from the Andalusia HCJ of 29 October 2015 (AS 2016\655), Asturias HCJ of 14 June 2013 (JUR 2013\245751), Madrid HCJ of 28 May 2012 (JUR 2012\226324)].

hoeren@uni-muenster.de

2.1.7 Other Obligations in Order to Protect Personal Data Conveyed and Stored Through Electronic Means

Art. 4.5 of the OLPPD stipulates that personal data shall be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which they are processed. Art. 8.6 of the ROLPPD admits that the data may be stored for as long as some kind of liability may be imposed, derived from a legal obligation, the performance of a contract or the implementation of pre-contractual measures requested by the data subject. In this case, the cancellation must be carried out by blocking the data, which will only be available to the PA, judges and courts, for the fulfilment of the abovementioned responsibilities (Art. 16.3 OLPPD). After this period, the data must be destroyed. By way of exception, Art. 4.5 also contemplates the possibility of preserving certain data in their entirety if their historical, statistical or scientific value is addressed by specific legislation (particularly, the provisions of act 12/1989 of 9 May on the Public Statistical Function, Law 16/1985 of 25 June, on the Spanish Historical Heritage, and Law 14/2011 of 1 June, on Science, Technology and Innovation, as well as their respective implementing provisions and the autonomous legislation on these matters).

2.1.8 Security Obligations and Data Breach Notifications Concerning Data Processed by Electronic Means

When regulating the basic and medium security measures applicable to electronic files and processing, Art. 90 and 100 of the ROLPPD provide for a register of incidents. However, this is a record obligation of an internal nature within the entity or the organization.

In the field of telecommunications, providers of electronic communication services to the public are obliged to notify about security breaches to the SDPA and, in some cases, also to their subscribers or clients (Art. 41.3 LGT). In this area, we must also bear in mind the newly approved Royal Decree-Law 12/2018 of 7 September, which transpose into Spanish law Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union.

2.1.9 Specific Legislation on Sectorial Areas

In the banking area in general, Law 44/2002 of 22 November, on measures to reform the financial system, is particularly relevant. It often refers to the OLPPD, but it includes some specific provisions related, for example, to the contents of the information coming from reporting entities, the rights of access, rectification and cancellation, as well as use and transfer of data by the Bank of Spain and the retention of data. Law 10/2014 of 26 June on the regulation, supervision and

hoeren@uni-muenster.de

solvency of credit institutions merely points out the following: when marketing loans or credits, the Ministry of Economy and Competitiveness may establish rules that promote compliance with the regulation on data protection; the Bank of Spain has the possibility to access the information and data it requires (a possibility covered by the OLPPD); all other entities and individuals who are subject to these regulations are obliged to maintain confidentiality with regard to all information related to account balances, items, transactions and any other operations of their clients, except in some specific cases (*e.g.* money laundering), without prejudice to the provisions of the rules on data protection. Law 22/2007 of 11 July on distance marketing of consumer financial services does not contain specific provisions regarding the processing of personal data.

a) Unmanned aerial vehicles

   Royal Decree 1036/2017 of 15 December regulating the civil use of unmanned aircraft systems does not contain specific rules on the processing of data; in this regard, it refers to the OLPPD. Therefore, if the use of drones involves the recording of images of identified or identifiable individuals, it will be necessary to have a valid reason to process personal data, to inform the data subjects (Art. 5 OLPPD) and to inform the SDPA about the characteristics of said data processing (Art. 26 OLPPD). The rules insist on the need to adopt all necessary measures to respect the privacy of individuals.

b) Mobile health

   The following regulations refer to the general rules on data protection:

   – The General Health Act 14/1986 of 25 April, and the Basic Law 41/2002 of 14 November, on the autonomy of the patient and the rights and obligations with regard to clinical information and documentation (data processed in the context of a healthcare activity carried out by health centres, services and professionals who are connected in a specific health information system or become part of the Electronic Health Record).
   – Royal Decree 1591/2009 of 16 October, that regulates medical devices (apps intended by the manufacturer to be used "specifically for diagnostic or therapeutic purposes and involved in their proper functioning".)
   – Law 39/2015 of 1 October, on the Common Administrative Procedure of PA (apps that allow users to access information and to initiate a procedure with a PA, such as the request of doctors' appointments).

c) IoT

   At this point, we need to mention the Royal Decree 188/2016 of 6 May, which approves the regulation laying down the requirements for marketing, placing in service and use of radioelectric equipment; and which regulates the procedure for compliance assessment, market surveillance and regime of sanctions of telecommunications equipment, transposes Directive 2014/53/EU. And also the OL 1/2015 of 30 March, amending the Criminal Code, transposes Directive 2013/40/EU.

hoeren@uni-muenster.de

Currently, a draft for a new OLPPD adapted to the requirements of the General Data Protection Regulation (GDPR) is being prepared.[13]

2.2 Data Protection in the Electronic Communications Sector

As far as the regulatory framework is concerned, we must say that, as a general rule, the OLPPD is applied, and the GTA is applied specifically in the electronic communications sector (particularly Art. 34 and 38). This act is developed in Royal Decree 424/2005 of 15 April, which approves the regulations on conditions for the provision of services of electronic communications, universal service and the protection of users (Title V). In addition, we must take into account Law 25/2007 of October 18, on the retention of data related to electronic communications[14] and public communication networks, and Royal Decree 899/2009 of 22 May, which approves the rights of users of electronic communication services (Art. 31).[15]

The entities subject to these legal rules are:

- Operators of public electronic communications networks or operators providing publicly available electronic communications services, including publicly available communications networks that provide support to devices for the identification and collection of data (Art. 41.1 GTA).
- Providers of publicly available electronic communications services or providers that operate public communications networks (Art. 2 of Law 25/2007).[16]

In the field of electronic communications, we talk about communication data to refer to the process in which information is shared among two or more entities. It requires four basic elements: sender, message, channel and receiver. Law 25/2007 refers to the data subject to retention, and it establishes a difference based on whether it is fixed network telephony and mobile telephony or internet access, internet-based electronic mail and internet telephony: (a) data necessary to trace and identify the source of a communication; (b) data necessary to identify the destination of a

[13]For commentary on this provision, see, Piñar Mañas (2016) and Aragonés Salvat (2016).

[14]This law has not been repealed, in spite of the fact that the judgement from the Court of Justice of the European Union of 8 April 2014 (CJEU 2014\104), Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, with case no. C-293/12 and C-594/12, declared Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services to be invalid, because it considered that it represented "a wide-ranging and particularly serious interference" with the fundamental rights to respect for privacy and the protection of personal data.

[15]See Dávara Rodríguez (2000), and, more recently, the study of comparative law carried out by Quesada Rodríguez (2015).

[16]This law does not apply to the provision of instant messaging services, according to Report 0343/2013 of the SDPA.

hoeren@uni-muenster.de

communication; (c) data necessary to identify the date, time and duration of a communication; (d) data necessary to identify the type of communication; (e) data necessary to identify the communication device or what purports to be the communication device; (f) data necessary to identify the location of mobile communication equipment.[17]

Art. 3i of the OLPPD, in contrast, defines the "Assignment or communication of data" as "any disclosure of data to a person other than the data subject". The OLPPD establishes a difference between data communication as such—which must take place to fulfil the purposes directly related to the legitimate functions of the transferor and the transferee and which requires, except in the cases specifically provided for in the Law, the consent of the data subject. This consent may be revoked and shall be null and void if the information provided to the data subject does not allow them to understand unequivocally the purpose for which the relevant data shall be used[18]—and the access to data by third parties when said access is necessary to provide a service to the person responsible for the processing of data, in which case the access is not classified as data communication.[19] Art. 21 of the OLPPD establishes specific regulations for the communication of data between PA, which must be connected to Art. 155 of the Law 40/2015 of 1 October on the legal regime of the public sector.

Operators of public electronic communications networks or operators providing publicly available electronic communications services must guarantee the confidentiality of communications (Art. 18.3 and 55.2 SC) and adopt all necessary technical measures to ensure it. However, they are obliged to execute the interceptions authorized in accordance with Art. 579 of the Criminal Procedure Act (hereafter, CPA); with OL 2/2002 of 6 May, regulating preliminary judicial control of the National Intelligence Centre; and with other regulations having the force of organic laws (Art. 39 GTA).

Art. 41.1 GTA establishes that operators of public electronic communications networks or operators providing publicly available electronic communications services, including publicly available communications networks that provide support to devices for the identification and collection of data, must adopt all necessary technical and management techniques to maintain the security of use of their network or the provision of services, in order to guarantee the protection of personal data. These measures may be examined by the SDPA—which may issue recommendations—and they will include, at least: (a) the guarantee that only authorized personnel will have access to the personal data and for the purposes authorized by the Law; (b) the protection of the personal data stored or communicated from accidental or unlawful destruction, accidental loss or alteration, or unauthorized or

[17]The transfer of these data is referred to in Art. 7 of Law 25/2007.

[18]Art. 11.2 of the OLPPD specifies the cases in which consent from the data subject is not necessary.

[19]See Art. 12 of the OLPPD.

hoeren@uni-muenster.de

unlawful storage, processing, access or disclosure; (c) the guarantee of an effective implementation of a security policy regarding the processing of personal data.

Art. 41.2 envisages the eventuality of a specific risk for the violation of the security of a public network or the service of electronic communications, and establishes that operators must inform their clients about the risks and the measures that may be adopted.

In the case of a personal data breach,[20] the operator must notify the SDPA of the breach without delay (Art. 41.3). The operator must also inform without undue delay the client or the individual if this breach may have a negative impact on their privacy or personal data, unless the operator can prove, to the satisfaction of the SDPA, that the necessary technological protection measures have been applied and that said measures have been applied to the data affected by the security breach (*e.g.* measures that render the data incomprehensible to any person without an authorization to access them). The notification to the client or the individual must describe, at least, the nature of the personal data breach and the contact points in which they can obtain more information, as well as recommended measures to mitigate the possible adverse effects of said breach. The notification to the SDPA must also describe the consequences of the breach and the measures that have been proposed or implemented by the provider to manage the breach.

The law obliges the providers to have a record of the personal data breaches that allows the SDPA to verify that the notification requirements have been fulfilled. In addition, the law empowers the SDPA to adopt guidelines or even issue instructions about the circumstances in which the provider must inform about the personal data breach, the format of the notification and the way in which this notification has to be managed.

At this point, we must remember that the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union, has been recently, transposed into Spanish law by Royal Decree-Law 12/2018 of 7 September.

The supervising body in charge of the control of the processing of personal data in the context of electronic communications is the SDPA, according to the provisions of Art. 41 of the GTA.[21] However, the National Commission on Markets and Competition has the power to sanction, for example, the unauthorized interception of telecommunications not addressed to the general public as well as the publication of those contents; and the non-compliance of providers with their obligations regarding the legal interception of communications laid down in the implementation of Art. 39 of the GTA (Art. 72.3 GTA).

[20] A personal data breach is interpreted as a security breach that leads to the accidental or unlawful destruction, loss, alteration, revelation of or unauthorized access to personal data transmitted, stored or processed in any other way with regard to the provision of publicly available electronic communications services.

[21] This provision ultimately specifies that the OLPPD and ROLPPD are applicable. Therefore, the penalty regime established in it is also applicable.

hoeren@uni-muenster.de

2.3 Data Protection and Digital Forensics

In the rules of criminal procedure (Art. 588 onwards of CPA, modified by OL 13/2015 of 5 October), we can find some special rules with regard to the interception of telephonic and online communications; the capture and recording of oral communications with the use of electronic devices; the use of technical devices for image monitoring, localization and capture; and the register of devices for massive information storage and remote register of computing equipment. Until said reform, the legislative shortcomings revealed by the investigative needs required to fight technological crimes had been overcome thanks to the commendable efforts carried out by the Supreme Court and the CC.[22]

2.3.1 Preservation and Access to Computer Data Hosted on a Computer System

Art. 588e a) to 588e c) of the CPA regulate the handling of and access to the contents of computers, telephonic or online communication devices or devices for massive storage of digital information or access to online data repositories. This regulation is applicable to the access to any kind of electronic device with the ability to store information, even if they do it temporarily and secondarily to the functions that represent their primary purpose (*e.g.* mobile telephones, tablets, etc.).

This legislation provides for the seizure of and access to devices when a house search is performed [Art. 588e a.1)] and the seizure of devices outside the context of a search of the individual being investigated[23] [Art. 588e b)] and requires, as a condition to authorize the access to the data contained in said devices, a judicial authorization that motivates the access.[24] This authorization must establish the terms and the extent of the data register; it may authorize the making of copies of digital data; and it must establish the necessary conditions to guarantee the integrity and preservation of data that make it possible, if necessary, to procure expert advice (Art. 588e c.1). The provisions included in this text must be complemented with the provisions of Art. 588b c), in which the examining judge must take the decision to authorize or refuse the requested measures, after hearing the Public Prosecutor's Office, within a period of no more than 24 h since the request is submitted. This period may be interrupted if the judge requires extension or clarification of the terms

[22]CC judgement 145/2014 of 22 September is particularly significant here.

[23]This includes files stored outside the device in the cloud, or through any other system that provides services to the user, such as a bank, a medical centre, etc., and which must be accessed from the seized device that was used by the subject under investigation.

[24]The Supreme Court judgement of 10 March 2016, for example, highlights this aspect very clearly (RJ 2016\1114).

While assessing the proportionality of the measure of confiscation and exam of the computing devices, the special nature of technological crimes must be taken under consideration. [Supreme Court judgement of 9 December 2015 (RJ 2015\5420)].

hoeren@uni-muenster.de

in the request. The rule establishes the minimum contents of the decision, which must include, for example, the duration and purposes of the measures.

A judicial authorization will not be necessary when the individual under investigation gives consent and in cases of urgency (Art. 588e c.3 and 4 CPA).

In addition, in its Art. 588f, the law provides for the possibility that the competent judge authorizes the use of identification data and codes, as well as the installation of software that makes it possible to carry out a remote and online analysis of the contents of a computer, electronic device, computing system, device for the massive storage of digital data or database without the knowledge of its owner or user, provided that it is pursuant to the investigation of one of the following crimes: (a) crimes committed within criminal organizations; (b) terrorist offences; (c) crimes against minors or individuals with their capacities modified by a court order; (d) crimes against the Constitution, treasonable offences or offences against national defence; (e) offences committed through computing devices or any other information and communications technology or communications service. After mentioning the questions that must be specified in the court's decision that authorizes the register, the law specifies that this measure shall have a maximum duration of 1 month, renewable in 1-month periods up to a maximum of 3 months.

2.3.2 Interception of Communication Data

The interception of communications is mentioned in Art. 40 GTA and Art. 83-101 of Royal Decree 424/2005.The only interceptions that the subjects who are required to carry them out are obliged to perform are provided for in CPA, OL 2/2002 and other regulations having the force of organic laws.

According to Art. 588c a) of the CPA, the authorization for the interception of telephonic and online communications may only be granted when the investigation has to do with: (1) intentional crimes carrying a punishment of no more than 3 years of imprisonment; (2) crimes committed within criminal groups or organizations; (3) terrorist offences; (4) offences committed through computing devices or any other information and communications technology or communications service.

The communication devices or terminals under investigation must be those generally used by the person under investigation, but those belonging to or used by the victim may also be intercepted if their life or integrity could be at serious risk [Art. 588c b) CPA].

The interception granted by a judge may authorize access to the contents of the communications and the electronic data related to the traffic or associated to the communication process, as well as to the data that are independent from the establishment of a specific communication, in which the subject under investigation participates (either as sender or as receiver), and it may involve the communication devices or terminals owned or used by the person under investigation [Art. 588c b) CPA].

The judge may even grant the interception of communications issued from online communication devices or terminals belonging to a third party if it is established that

hoeren@uni-muenster.de

the subject under investigation uses said devices to transmit or receive information, or when the owner or user of the device collaborates with the person under investigation for their illegal purposes, or when they benefit from their activity; and also when the device under investigation is used maliciously by third parties remotely without the knowledge of its owner [Art. 588c c) CPA].

In its Art. 588c d), which refers to Art. 588b b), the CPA specifies the data that must be included in the request for a judicial authorization, including the duration of the measures, for example. The law also specifies the purposes it may have: (a) the register and recording of the contents of the communication, with explicit mention to the form or the type of communications involved; (b) data regarding the source or the destination of the communication in the moment in which it takes place; (c) the geographical location of the source or destination of the communication; (d) other traffic data associated or not associated with the communication but which provide an added value to the communication. In this case, the request shall specify the data that must be obtained.

This regulation contains a particular rule for cases of urgency, in which the investigations pursue crimes related to the activity of armed groups or terrorist units and there are legitimate grounds that make it indispensable to adopt these measures. In this case, the measure may be authorized by the Minister of the Interior or, failing this, by the Secretary of State for Security. The competent judge shall be informed immediately, and they will issue an informed decision in which they confirm or reject this measure.

All the providers of telecommunications services, of access to a telecommunications network, or of services from the information society, as well as any individual who in any way contributes to facilitate communications through the telephone or through any other means of online, logical or virtual communication, are obliged to give their specific assistance and cooperation to the judge, the Public Prosecutor's Office and the judicial police officers in charge of implementing the measures, in order to facilitate the fulfilment of the authorizations to intercept the communications [Art. 588c e)].

The maximum initial duration of the intervention is 3 months from the date of the judicial authorization. This period may be renewed for consecutive 3-month periods up to a maximum of 18 months, provided that this extension is duly justified [Art. 588c g) and h) CPA]. OL 2/2002 does not establish a maximum duration.

Finally, the CPA establishes, in Art. 588c i), the access of the different parties to the recordings when the secrecy order is lifted and the validity period of the intervention has expired.

In the case of OL 2/2002, the Secretary of State and Director of the National Intelligence Centre must ask the competent judge of the Supreme Court to adopt this measure, and the judge must issue the decision within a maximum of 72 h (24 h in case of urgency).

hoeren@uni-muenster.de

2.3.3 Data Retention

With regard to the retention of data, we must highlight Law 25/2007, in which Art. 6 mentions that all data retained according to this Law can only be transferred according to what is provided for in the Law, for the purposes established in it and with prior authorization of a judicial authority. This transfer will be carried out in electronic format and only to the authorized agents (that is, members of the State security forces and public officials of the Deputy Office of Customs Surveillance when working in the capacity of Judicial Police, and personnel of the National Intelligence Centre within their security investigations of individuals or entities). The court's decision will specify the data that must be transferred (Art. 7).[25]

In the field of criminal proceedings, we must take into account Art. 588g of the CPA, which allows the Public Prosecutor's Office or the Judicial Police to request that any individual or legal entity retains and protects specific data or information included in a digital storage system under their control until a judicial authorization for the transfer of said data is obtained, according to the provisions laid down in the previous articles of the Law. These data will be retained for a maximum period of 90 days, renewable only once until the transfer is authorized or up to a maximum of 180 days. According to the provisions laid down in the law, the individual or legal entity that receives the request is obliged to cooperate and to keep the confidentiality regarding the development of these measures, and may be charged for a crime of disobedience in case of non-compliance (Art. 588c e 3 CPA).

2.4 Data Protection and Electronic Surveillance for Security and Defence Purposes

According to Art. 2 of the OLPPD: (1) the provisions of this law shall not apply to "files established for the investigation of terrorism and serious forms of organised crime. However, in such cases, the person responsible for the file shall previously inform the SDPA of its existence, its general characteristics and its purpose"; (2) the processing of personal data contained in the Civil Register and the Central Criminal Register, and those that derive from images and sound recorded with video cameras by the security forces in accordance with the relevant legislation—that is, OL 4/1997 of 4 August, regulating the use of video cameras by security forces and units in public open and closed spaces—among others, shall be governed by the specific provisions, and by any special provisions, of this Law.[26]

[25]For more information, see De Miguel Asensio (2015), pp. 355–359.

[26]The installation of cameras must be authorized by the corresponding administrative authorities. The public must be informed about the installation of fixed cameras, and the image and sound captured by any of the devices established by the law must be destroyed within a month after they were obtained, except in the case in which they are related to serious or very serious criminal or

hoeren@uni-muenster.de

The files created by the security forces and containing personal data which, because they were collected for administrative purposes, must be recorded permanently, are subject to the OLPPD (Art. 22 OLPPD). This Law enables the collection and processing, for police purposes, of personal data by the security forces without the consent of the data subjects, but limits that possibility to those cases and categories of data necessary for the prevention of a genuine threat to public security or for the suppression of a crime; it also allows the collection and processing of especially protected personal data by the security forces, but only if it is absolutely essential for the purposes of a specific investigation. It considers the possibility of denying access, rectification or cancellation in the light of the risks which might arise for the defence of the state or public safety, the protection of the rights and liberties of third parties, or for the needs of investigations under way (Art. 23.1 OLPPD). Nevertheless, personal data stored for police purposes must be cancelled when they are not necessary for the investigations which motivated their storage; to this end, special consideration is given to "the age of the data subject and the nature of the data stored, the need to maintain the data until the conclusion of a specific investigation or procedure, a final judgement, and in particular an acquittal, a pardon, rehabilitation and the expiry of liability" (Art. 22.4 OLPPD). Furthermore, the right of the data subject to be informed when their data were collected is excluded when it could affect national defence, public safety or the prosecution of criminal offences (Art. 24.1 OLPPD); and the law provides for the possibility that the rights of access, rectification and cancellation of the data subject are waived for reasons of public interest or because the interests of third parties need more protection, after considering all the interests at stake (Art. 24.2 OLPPD).

At this stage, Art. 6 and 7 of Law 25/2007, which have already been discussed, are relevant here.

Art. 42 of Law 5/2014 of 4 April, on private security, provides for the submission, either voluntarily or at the request of the security forces, of the recordings captured by video surveillance systems that may be related with criminal acts or that may affect public safety.

Access to the data stored in a computer requires judicial authorization.

Regarding the drones, we must point out that the Royal Decree 1036/2017 of 15 December, regulating the civil use of unmanned aircraft systems excludes from its scope military remotely piloted aircraft systems (RPAS) and aircraft (Art. 2.2). However, the provisions laid down in chapters I and II will be applicable to the police operations attributed to security forces by OL 2/1986 of March 13, to customs operations, to traffic surveillance carried out by the Directorate-General for Traffic, and to operations carried out by the National Intelligence Centre. These rules only contain a general reference to the competencies of the SDPA.

---

administrative infractions against public security, to an ongoing police investigation or to ongoing legal proceedings. Recordings that captured the commission of acts that could represent criminal offences must be brought under judicial control immediately.

hoeren@uni-muenster.de

2.5 Remedies and Sanctions

The infringement of Spanish data protection rules may result in administrative, civil or criminal liability. Find below the penalties imposed by some of our rules on data protection.

2.5.1 General Personal Data Protection Rules

Administrative penalty: A fine of an amount that varies depending on the type of sanction: minor (€900–40,000), serious (€40,001–300,000) or very serious (€300,001–600,000), which may be graded according to the criteria established in Art. 45.4 of the OLPPD. The SDPA has imposed fines of up to €1,200,000 (specifically to Facebook, in September 2017).[27]

Civil penalty: compensation for the infringement of the right to honour, privacy and self-image (OL 1/1982).

Criminal penalty: Crimes of illegal interference with information or data systems (Art. 264 to 264d); crimes of discovery and revelation of secrets (Art. 197 to 197e of the Criminal Code).

2.5.2 Rules Regarding the Protection of Personal Data in the Context of Services Provided at a Distance, by Electronic Means, at the Individual Request of a Recipient of Services

Administrative penalty: A fine of an amount that varies depending on the type of sanction: minor (up to €30,000), serious (€30,001–150,000) or very serious (€150,001–600,000), which may be graded according to the criteria established in Art. 39b and 40 of Law 34/2002.

Civil penalty (consumer protection): Cancellation of the distance contract at the request of the consumer (Art. 100 RTGLDCU).

Criminal penalty: fraud (Art. 248 onwards of the Criminal Code).

2.5.3 Rules Regarding the Protection of Personal Data in the Context of Electronic Communications for Marketing Purposes

Administrative penalty: According to Art. 43.1 of Law 34/2002, the SDPA is responsible for imposing sanctions for infractions classified as "serious" in Art. 38.3 c), d) and i) and infractions classified as "minor" in Art. 38.4 d), g) and h) of

[27] "The Spanish DPA fines Facebook for violating data protection regulations", available on http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_11-ides-idphp.php.

hoeren@uni-muenster.de

this Law. The sanction for serious infractions is a fine ranging from €30,001 to €150,000, and in the case of minor infractions, the sanction is a fine of up to €30,000 (Art. 39 of Law 34/2002).

Civil penalty (consumer protection): If the requirements provided for in Art. 97.1 e) and j) of RTGLDCU are not met, the consumer and user shall not pay for the costs or expenses. If the other requirements are not met and the information is particularly relevant, the contract will be cancelled due to absence of valid consent.

Criminal penalty: Electronic harassment (Art. 172c).

2.5.4 Rules Regarding the Electronic Processing of Personal Data of Employees

Administrative penalty: The processing of personal data of data subjects (in this case, employees), without providing them with the information established in Art. 5 of the OLPPD is a minor infraction that involves a sanction of €900–40,000. Failure to block data referring, for example, to withholding taxes, could represent a serious infraction that violates the principles and guarantees established in the OLPPD (sanction of €40,001–300,000).

Criminal penalty: Discovery and revelation of secrets (Art. 197 to 197e).

2.5.5 Rules Regarding the Security of Personal Data Processed by Electronic Means

Administrative penalty: Severe infraction that involves a fine of €40,001–300,000, which may be graded according to the criteria established in Art. 45.4 OLPPD.

Criminal penalty: Illegal interference with information or data systems (Art. 264 to 264d of the Criminal Code).

2.5.6 Rules Regarding the Processing of Personal Data in the Electronic Communications Sector

Administrative penalty: Failure to meet the obligations of public service provided for in Art. 41 of the GTA on data protection is considered a serious infraction, which may be sanctioned with a fine of up to €2,000,000 (Art. 77 and 79 GTA).

Criminal penalty: Discovery and revelation of secrets (Art. 197 to 197e of the Criminal Code).

hoeren@uni-muenster.de

2.5.7 Rules Applicable to the Protection of Personal Data for the Purpose of the Investigation, Detection and Prosecution of Crimes Through Electronic

Criminal penalty: Crime of disobedience (Art. 410, 556 of the Criminal Code). Penalties vary significantly depending on whether the subject is an authority or public servant or an individual.

2.5.8 Rules Applicable to the Electronic Processing of Personal Data for Security and National Defence Purposes

Criminal penalty and, if it is not possible to establish criminal responsibilities, according to Art. 10 of OL 4/1997, sanctions may be imposed according to the corresponding disciplinary regime applicable to the offenders or, failing that, according to the penalty regime regarding the automatic processing of personal data.

3 Private International Law Rules

3.1 The Scope of Application of Data Protection Rules

Processing of personal data will be governed by the OLPPD: (a) when the processing is carried out in Spanish territory as part of the activities of an establishment pertaining to the data controller; (b) when the data controller is not established on Spanish territory but is subject to Spanish Law pursuant to the norms of Public International Law; (c) when the data controller is not established on European Union territory and uses means located on Spanish territory for the processing of data, unless such means are only uses for transit purposes (Art. 2 LOPD).[28]

3.2 Conditions, Under Which the Transfer of Personal Data to a Foreign Jurisdiction Is Allowed

In accordance with the provisions of Art. 33 of the OLPPD, there may be no temporary or permanent transfers of personal data which have been processed or which were collected for the purpose of such processing to countries which do not provide a level of protection comparable to that provided by this Law, except where, in addition to complying with this Law, prior authorisation is obtained from the Director of the SDPA, who may grant it only if adequate guarantees are obtained. In

[28]For more information, see De Miguel Asensio (2015), pp. 359 and following.

hoeren@uni-muenster.de

order to assess the adequacy of the level of protection afforded by the country of destination, the SDPA will take into consideration particularly the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectorial, in force in the third country in question, the content of the reports by the Commission of the European Union, and the professional rules and security measures in force in those countries.

Art. 34 of the OLPPD indicates the circumstances under which prior authorization of the director of the SDPA is not required:

a) When the international transfer of personal data obtained by the application of treaties or conventions to which Spain is a party.
b) When the transfer is made to deliver or seek international judicial assistance.
c) When the transfer is necessary for medical purposes of prevention or diagnosis, the provision of medical care or treatment, or the management of health-care services.
d) When it relates to cash transfers in accordance with their specific legislation.
e) When the person concerned has given unambiguous consent to the proposed transfer.
f) When the transfer is necessary for the performance of a contract between the individual concerned and the individual responsible for the file for the adoption of pre-contractual measures taken at the request of the individual concerned.
g) When the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual concerned, the individual responsible for the file and a third party.
h) Where the transfer is necessary or legally required to safeguard a public interest.
i) When the transfer is required for the establishment, exercise or defence of a right in a legal process.
j) When the transfer is effected at the request of any person with a legitimate interest from a public register and the request is consistent with the purpose of the register.
k) When the destination of the transfer is a Member State of the EU or a State declared to have an adequate level of protection by the Commission of the European Communities.

According to the first Provisional Regulation of the OLPPD, the SDPA is competent to protect the processing of personal data established in any international convention in which Spain participates that confers said competence to a national authority until a different authority is created for that purpose in the framework of the convention.

hoeren@uni-muenster.de

3.3 The Law Applicable to Liability for Damages Caused by the Unlawful Processing of Personal Data

The applicable law is the law of the country where the damage is sustained (non-contractual obligations, Art. 10.9 of the Criminal Code). The Rome II Regulation exempts from its application damages derived from rights relating to the personality.

References

Andreu Martínez MB (2013) La protección de datos personales de los menores de edad, 1st edn. Aranzadi, Cizur Menor

Aragonés Salvat J (2016) GDPR (General Data Protection Regulation): el nuevo Reglamento Europeo de Protección de Datos, 1st edn. Ateneu Privacy Consulting, Tortosa (Tarragona)

Conde Ortiz C (2005) La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad. Dykinson, Madrid

Corvo López FM (2017) El «derecho al olvido»: de la STJCE de 13 de mayo de 2014 al Reglamento general de protección de datos (Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016). Revista de Direito Intelectual 2017(1):175–245

Dávara Rodríguez MÁ (2000) La protección de datos personales en el sector de las telecomunicaciones. Universidad Pontificia de Comillas, Fundación Airtel, Madrid

De Miguel Asensio PA (2015) Derecho Privado de Internet, 5th edn, Civitas. Thomson Reuters, Cizur Menor

García Coca O (2016) La protección de datos de carácter personal en los procesos de búsqueda de empleo, 1st edn. Laborum, Murcia

López Álvarez LF (2016) Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo. Francis Lefebvre, Madrid

Martínez Martínez R (coord) (2009) Proteccion de datos: comentarios a la LOPD y su Reglamento de Desarrollo. Tirant lo Blanch, Valencia

Piñar Mañas JL (dir) (2016) Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad. Reus, Madrid

Quesada Rodríguez A (2015) Protección de datos y telecomunicaciones convergentes. Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, Madrid

hoeren@uni-muenster.de

Swiss Data Protection Law

Dominic N. Staiger

1 Introduction to Data Protection in Switzerland

The data protection framework in Switzerland is based on both laws and regulations of the individual Cantons as well as the Swiss Confederation. The processing of personal data by private entities such as corporations is based on the Federal Data Protection Act (FDPA) ("Datenschutzgesetz"). This Act also governs the processing of personal data by federal agencies. Since its enactment in 1993 the law has undergone several minor revisions. However, a new fundamental revision of the FDPA has been introduced into parliament in 2016 in order to bring the Swiss data protection law in line with the requirements of the new EU General Data Protection Regulation (GDPR).[1] This adjustment is necessary for Switzerland to maintain its status as a country with an equivalent data protection level to that of the EU. Currently Switzerland retains this status allowing for a free flow of personal data between EU Member States and Switzerland. Thus, for the Swiss economy with its many innovative service providers and export industry, the ability to offer cross boarder personal data processing plays an important role in the increasingly digitised and interconnected markets.

In some respect the new draft FDPA (dFDPA) falls short of the GDPR standard and seeks to limit certain areas. For example, the dFDPA provides in particular no right to data portability, no extra-territorial scope, lower requirements with respect to

[1]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119 4.5.2016, p. 1.

D. N. Staiger (✉)
University of Zurich, Zurich, Switzerland
e-mail: dominic.staiger@sidd.swiss

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_16

hoeren@uni-muenster.de

consent, certification mechanisms and codes of conduct and limited sanctions. However, it has taken on the risk-based approach of the GDPR and aims to strengthen the oversight by the Federal Data Protection and Information Commissioner (FDPIC). This is necessary as currently enforcement of data protection is fairy limited based on the lack of resources and competencies of the various data protection authorities.

To complicate matters the current reform process has been split in two parts. The first part now is prioritized and deals with the mandatory implementation of EU law elements based on the Schengen Agreement/Bilaterals II.[2] These are mainly cooperation in criminal matters and the connected data exchange. The second part will then address the necessary revisions in light of the technological changes since 1993 and the changes that must be carried out with a view to the GDPR. Such an approach aims at reducing the time pressure and achieving a balanced result for the Swiss economy. However, it significantly slows down the legislative process for enacting the new dFDPA for personal data processing by the private sector. The information provided in this chapter is based on the proposal as it stands in June 2018. However, possibilities for change remains as the final version will only be available during 2019.

In addition to the FDPA, the right to privacy is also derived from Article 13 of the Swiss Constitution which protects private and family live and misuse of personal data. As a signature party to the European Convention on Human Rights Switzerland is also bound by its protection with regard to private and family life.[3] However, these courses of action are only used in cases where all other means have failed as they are costly and time consuming and generally do not produce an immediate effect with regard to the processing of personal data by a private entity. Rather all other local court procedures must be exhausted before an application to the European Court of Human Rights can be submitted. This procedure has been shown to be very effective as it highlights non-compliant action and often leads to adjustments in local laws based on international pressure.

1.1 Protection of Personal Data

The Swiss interpretation of personal data has closely followed the approach on the EU level which is evidenced in the judgements on the classification of IP addresses

[2]For more details on the Swiss Bilateral Agreements with the EU see: Federal Department of Foreign Affairs https://www.eda.admin.ch/dam/dea/en/documents/folien/Folien-Abkommen_en.pdf.

[3]For more information on the Protocols signed by Switzerland see: Federal Department of Foreign Affairs, European Convention on Human Rights, https://www.eda.admin.ch/eda/en/home/foreign-policy/international-organizations/council-europe/european-convention-human-rights.html.

hoeren@uni-muenster.de

as personal data.[4] The question in these cases is always one of degree to which the personal data relates to an identifiable individual and the ability of one party to identify that individual or its power to affect identification. These questions will also remain under the GDPR as well as the revised Swiss FDPA. Most likely the EU Data Protection Board (EDPB) will issue some guidance on this matter with regard to specific and common processing scenarios so as to limit the legal ambiguity especially for smaller enterprises that cannot afford vast legal assessments and rely on any guidance that they may be able to receive from data protection authorities and the EDPB.[5]

Once personal data is present in any business operation, it must be processed in accordance with the principles set out in Article 5 of the draft revised FDPA. These principles include data minimization, purpose limitation and transparent data processing. In cases where enforcement under FDPA fails, the Swiss Civil Code provides catch-all elements ensuring the civil protection of personality rights.[6] This allows for an independent course of action that is currently already present today. However, these remain in addition to the power of the Federal Data Protection and Information Commissioner to impose fines and penalties and are often of much more limited scope.

In addition to the general scope of personal data there is also a category of sensitive data which requires further protection going beyond the standard protections. This category includes data relating to the religious, political and union member views, health care data, data relating to race or ethnicity, biometric data which allows for the identification of an individual, data on any prosecution or administrative procedure concerning an individual, as well as information on social welfare issues.[7] Such sensitive data also triggers the necessity of a Data Protection Impact Assessment as there is generally a high risk involved in the processing of such data that needs to be accounted for and were possible mitigated. In such a case the FDPIC must also be contacted for an opinion unless a Data Protection Officer has been consulted by the private entity.[8]

The revised dFDPA is applicable both to private entities and persons, as well as all federal agencies. However, the courts as well as the agencies involved in the legislative process are excluded from the scope of the law. In contrast to the old version the dFDPA does not classify data of companies (legal entities) as personal data anymore.

---

[4] *Logistep BGE 136 II 508* and *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

[5] For more information on the European Data Protection Board see: https://edpb.europa.eu.

[6] Swiss Civil Code, Art, 28 *et seq*. https://www.admin.ch/opc/en/classified-compilation/19070042/201801010000/210.pdf.

[7] Draft Federal Data Protection Act, Art. 3(c), https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf.

[8] *Ibid*., Art. 21.

hoeren@uni-muenster.de

1.2 Data Protection Supervisor

Under the previous as well as the revised dFDPA the supervision of data protection matter lies with the Federal Data Protection and Information Commissioner. Section 7 (Articles 37–49) contains the rights and responsibilities of the Federal Data Protection and Information Commissioner who is tasked with ensuring data protection compliance in accordance with the law. The Commissioner's powers include the right to investigate matters and conduct on premise inspections. However, currently any fines that may be imposed under the FDPA are not issued by the Commissioner but by the court system. The revision of the FDPA aims at allowing the Commissioner to impose such fines and not only to investigate the matters. This would also enable him to address complaints that are brought to his or her attention by the public, and to take remedial action. Section 8 of the dFDPA contains specific penal provisions. Sanctions are imposed on the individual who is responsible for the processing operation and include personal fines of up to 500,000 CHF (Article 50 *et seq*). As the revised dFDPA is still a draft, there is no relevant case law under the new data protection code yet. It will remain to be seen to what extent the power to issue fines will be used or if alternative administrative measures will be chosen.

As Switzerland has a federal system, the Commissioner is responsible for the compliance with data protection law on the federal level; however, there are authorities on the Cantonal level (Data Protection Commissioners) supervising strictly cantonal issues of data protection compliance.

In addition to the powers of the Commissioner the new dFDPA eliminates the duty to notify data files to the Federal Data Protection and Information Commissioner, which applied to all private parties who regularly disclosed personal data to third parties or processed sensitive personal data.[9]

2 Key Data Protection Provisions in Switzerland

Swiss data protection law does not distinguish by the specific method of data handling as it aims at being technology neutral. Cases of data handling by the electronic means fall under the FDPA in the same way as any other method does. The law generally regulates how the data controller must act. For example, social media companies are classed as data controllers within the meaning of the FDPA.[10]

Article 4 paragraph 6 of the dFDPA requires the data controller to provide the data subject with clear information about whether data is collected or not, as well as information about what kind of data is collected. This is in line with the GDPR requirements to ensure transparent data processing and allows the affected individual

[9]Federal Data Protection Act, Art. 11a (5).

[10]Draft Federal Data Protection Act, Art. 3 (h).

hoeren@uni-muenster.de

to understand and make informed decisions if she or he wishes to be subject to a particular data processing.

2.1 Scope

Neither the FDPA nor the proposed draft contains any remarks as to the territorial scope of the data protection law. Nonetheless, the FDPA is a national law and therefore the territorial principle is applied limiting the scope to conduct in Switzerland. This means in fact, that the law is applicable to any data handling occurring within Switzerland. This has also been firmly established in a decision of the Swiss Federal Administrative Tribunal against Google in 2011 (A-7040/2009).[11]

The transfer of personal data to another country is regulated in Articles 5 and 6 of the FDPA. Namely, personal data can be transferred if the Swiss Federal Government has determined that the foreign jurisdiction provides an equivalent level of protection for the data handled. If there is no determination available as to the data protection level of a foreign jurisdiction, exceptions under Article 5 paragraph 3 FDPA may apply. Under no circumstances can data be transmitted if personality and privacy rights of the data subject are severely threatened.

Damages as well as compensation for pain and suffering are subject to civil actions governed by the Swiss Civil Code. However, this process is costly and is seldom used by individuals. The most likely result of a breach will be a complaint to the local data protection authority. However, their powers and remedies are currently limited.

The following four specific situations are not subject to the FDPA. These involve the data collection for the purposes of personal use, consultation of federal councils and commissions, handling by a neutral judicial authority as well as data handling by institutions as determined by "host state" legislation.

2.2 Legal Basis for Processing

In order to process personal data a legal basis must be available to the private entity. However, in comparison to the EU General Data Protection Regulation the current FDPA allows for much more leeway as many of the processing activities can be carried out as long as they are not infringing the privacy rights of the individual. For this to apply, however, the context of the data collection, the expectations of the individual, the information provided and the limitation of the processing are key factors. If sensitive personal data is involved either the consent of the individual is required, or alternatively a public or private interest is applicable that outweighs the

[11]Google Street View decision A-7040/2009, https://www.bvger.ch/bvger/de/home/medien/medienmitteilungen-archiv-2002%2D%2D-2016/2011.html.

hoeren@uni-muenster.de

privacy interest of the individual.[12] However, in practice as soon as sensitive data is involved the informed consent of the affected individual should be sought.

2.3 Purpose Limitation

The current FDPA also contains a purposes limitation similar to the former EU Data Protection Directive as well as the new GDPR. This requires the processing that is being conducted by a private entity to be in conformity with the expectations of the affected individual present at the time of the data collection and based on the context of the collection.[13]

2.4 Data Subject Rights

The rights of the data subject are set out in section 4 of the FDPA. As described above, the Swiss legislator does not distinguish between the legal basis of data collection, hence section 4 provides the general rules and rights that apply to the data subject. These include mainly access rights in order to provide better transparency for the data subject. However, the current FDPA does not contain any of the wide-ranging information and transparency provisions that are present in the GDPR. Rather an internal check is imposed whether the data processing meets the expectations of the individual concerned. With the draft FDPA the information requirements will be expanded to fulfil those of the GDPR. However, it is currently debated whether the draft FDPA will fall short of the current GDPR with regard to the rights of individuals.

No court fees are charged in disputes relating to data protection. Further, no fee shall be charged to data subjects for exercising their right of access, subject to any exceptions that may be provided for by way of ordinance.

2.5 Automated Decision Making

Controllers must upon request inform the data subject of automated decisions that are carried out on their personal data (i.e. decisions taken solely on the basis of automated data processing) which result in legal consequences or significant impairment and give the data subject the opportunity to comment on such decisions. Controllers are exempt from such information duties in particular if the data subject

[12]Federal Data Protection Act, Art. 12 and 13.

[13]Federal Data Protection Act, Art 4(3).

hoeren@uni-muenster.de

has expressly consented to such processing or if the decision relates directly to the execution or performance of a contract. This stands in stark contrast to the GDPR which requires prior notice through for example the data protection policy in order to allow the individual to understand and assess the data processing that will be undertaken.

2.6 Protection of Minors

The FDPA does not contain any clauses with regard to minors. However, the view in the legislative process is that the current protections under Swiss civil law are sufficient and the revised FDPA does not require specific protections such as the ones that are contained in the GDPR. This may present a point of controversy for enterprises that operate in various EU jurisdictions as well as Switzerland as they are required to undergo legal assessments in every country and to adjust their service offering according to origin of the user. Such as situation hinders business and should be addressed through a universal standard.

2.7 Right to Be Forgotten

Currently Switzerland does not have a right to be forgotten similar to the EU. However, the new draft FDPA contains a conclusive list of legal claims against data handling by any natural person and is to be understood as an extension of the protection of personality rights. The list includes the right to be forgotten, right to rectification, and the right to forbid data handling. As Switzerland is debating the extent to which it wants to follow EU law and the GDPR it remains to be seen what the effect of such a right to be forgotten will be and the extent to which it will be applicable in light of vast legal data retention requirements that cover nearly all business communication.[14]

2.8 Data Protection Impact Assessment

Controllers must conduct an impact assessment if processing may lead to a high risk for the data subject's privacy or fundamental rights (e.g. in case of extensive

[14]For more details on the current state see the draft Federal Data Protection Act https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf and the parliamentary discussion https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=43570.

hoeren@uni-muenster.de

processing of sensitive personal data or profiling).[15] If such risk is present, the Federal Data Protection and Information Commissioner must be consulted prior to the processing. No impact assessment is required if the Controller is certified by a recognized certification body or complies with a code of conduct. In case of multiple similar processing activities, the Controller may conduct a general impact assessment which applies across all processing activities. This is in line with the EU approach which will facilitate the development and usability of standards with regard to high risk personal data processing. However, it has been criticized as hindering the common use of profiling which forms the backbone of most of today's online business. Some profiling does not necessary involve any high risk for the individual and thus profiling should not generally require a DPIA without further factors that substantiate the claim of a high risk.

2.9 Data Breach Obligations

The Swiss FDPA does not contain a requirement to notify a data protection authority of a data breach. However, in light of the risk-based approach taken by the EU, clear notification requirements also seem warranted for Switzerland. As small data protection breaches occur on a daily basis, notification requirements should be practicable thus only require notification to the authorities when there is a real and substantial risk for the affected individuals. Nevertheless, in order to cope with the higher workload and added responsibility additional funds must be provided to the Federal Data Protection Supervisor.

2.10 Employee Data

Section 5 of the FDPA regulates data collection and handling by private individuals, including corporate bodies. Most importantly it governs personality rights and the legal consequences of violations. This affects employers as well as other data collectors, as personality rights may only be limited with strict justification under Article 24 of the data protection code. Although personal data of employees are not considered as sensitive data in the sense of the legal definition in Article 4, the Swiss legislator did provide further protection for employee data in the Code of Obligations (Article 328b OR) according to which an employer may only collect and handle data for which he can provide a legitimate interest for. Such data would typically include information such as home addresses, banking connections (in order to pay salary), emergency contacts, and personal information as provided in a CV or by an employee directly. However, the scope of this provision and its application

[15]Draft Federal Data Protection Act, Art. 20.

hoeren@uni-muenster.de

have come under scrutiny by the courts and have resulted in conflicting judgements. Thus, it remains to be seen what effect this section will have in light of the new dFDPA.

Use of electronic means by employees is not regulated by law, though; many companies regulate the use internally, as they need to comply with other regulations. For example, the banking sector must comply with financial market law, professional secrecy laws and client confidentiality. In order to do so, the way in which employees may use electronic means and to what extent may be strictly governed by corporate regulations and compliance procedures within the company.

2.11 Enforcement

The FDPA—like many statutes—has in addition to the Swiss Penal Code, its own penal provisions at the end in Section 8 (so called "Nebenstrafrecht"). Therein, sanctions are provided for the violation of the duty of disclosure, reporting obligations, duty to collaborate, due diligence as well as the violation of non-disclosure obligations. The non-disclosure obligations are the only obligations sanctioned by a potential prison sentence of up to 3 years or financial penalty within the data protection code. All other violations are sanctioned by fines of up to 500,000 CHF and a reduced amount of up to 250,000 CHF in case of negligence. Fines are issued by the Federal Data Protection and Information Commissioner's Office and may be imposed on the company as well as the responsible person.

3 Special Processing Situations

The draft FDPA provides a central regulatory framework. However, Swiss legislators have decided not to include issues such as Big Data at this time (at least not in a structured way). The FDPA merely touches topics including access rights, privacy by design and default and data protection impact assessments. This creates a degree of legal uncertainty for the online marketing sector, as much leeway in the interpretation of certain provisions is available similar to the GDPR.

The framework formulates basic data protection principles that are now common standard across the EU. The principle of data protection by default is now also a part of the draft FDPA, which requires companies to apply by default the highest data protection setting to their services and only to reduce these settings if the customer or user wishes to do so.[16] Furthermore, consent must be given voluntarily and freely.

[16]See for example the European Data Protection Board, Preliminary Opinion on privacy by design, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

hoeren@uni-muenster.de

Therefore, the opt-out system (which so far has been popular in Switzerland) will not be accepted anymore since a voluntary consent can only be given by actively checking a box.

3.1 Utilizing a Sub-Processor

Under the draft FDPA the prior consent of the controller is required. How whether this position will be maintained remains to be seen in the final version of the law. For efficiency purposes a general authorization such as the one allowed under the GDPR should be made possible. Currently there is no such requirement for any form of authorization for sub-processing under the FDPA. In light of the complexities of cloud businesses and other multi-layered business arrangements in which the identity of the business partners is a key asset not requiring the disclosure is a key advantage. Nevertheless, in order to meet the data protection requirements enforceable rights should be granted and the liability should rest on the processor subcontracting with the other party as this is the case under the GDPR.

3.2 Marketing, Television and Radio

Generally, any entity handling data is subject to the FDPA, however, institutions such as the Swiss public television and radio network might also be subject to further laws due to the public service they offer. Swiss public radio and TV for example, are also subject to the federal law on radio and television "RTVG" (Bundesgesetz über das Radio und Fernsehen) as this special code governs public radio and TV stations in general. Importantly, this law currently does address some topics related to data protection, but mostly refers to the Data Protection Code.

Democratic values and thus, the Swiss Constitution regard any means of telecommunication and digital communication as private and therefore the data as worthy of protection. This is set out in the Constitution under Article 13, the right to privacy. However, in Switzerland the law on marketing cookies is much less stringent as this is the case in the EU with the E-Privacy Directive.[17]

[17]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJL 201, 31/07/2002 pp. 37–47, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

hoeren@uni-muenster.de

3.3 Government Access to Data

The access to private data transmitted by a communication services provider is also subject to the FDPA. However, there is a civil law, the "Bundesgesetzüber den Post- und Fernmeldeverkehr" (BÜPF), which governs the power authorities have regarding surveillance of telecommunication and digital communication. The Swiss Constitution generally prohibits systematic surveillance of communication. Nevertheless, the government has an obvious interest in the surveillance of some communication in case of impending crimes, in order to carry out its duties in enforcing the law and ensuring security of the general population. The specific permission of surveillance measures is a fought over aspect in politics, since the surveillance is neither noticeable to the surveillance subject, nor is the subject aware if the surveillance is legitimate. Therefore, the BÜPF introduces high requirements for a legitimate surveillance measure.

Article 3 BÜPF provides a conclusive list of criminal offences, for which strong suspicion must be presumed by authorities in order for a legitimate act of surveillance to be carried out. Furthermore, other means of investigation must have been carried out, failed and a criminal procedure must have been initiated against the individual subject to the surveillance. Such surveillance includes the collection and analysis of communication metadata that is being collected by telecommunication providers. Moreover, the power to conduct surveillance is limited to a specific public authority that forms part of the executive branch. Most noticeably, Swiss Intelligence Agencies are not permitted to do this. Surveillance is ordered by a Judge working presiding over the relevant case, which formally opens a request with the Swiss Service for Special Tasks (Dienst für besondere Aufgaben). The Service then works together with involved authorities (such as the Police) and telecommunications companies acting as technical specialists in the proceeding.[18] The scope and duration of the measure is set by the judge and mostly limited to a maximum of 6 months. The affected individual must be informed of the measure once it has been concluded in order to be able to seek legal counsel and challenge the order and ultimately the use of the collected information.

The statute has recently undergone revision, providing authorities with further capabilities in the area of GovWare use and other surveillance technology. The revised law includes obligations on communications and internet access providers to retain information such as IP addresses for a duration of 12 months. The scope of the order is adjusted to the needs of the case taking into account the alleged offence as well as the effects on the individual and the possibility of gathering the evidence through less invasive means.

[18]For more details ee: Datenschutzbeauftragter des Kantons Luzern, Merkblatt Telefonüberwachung, https://datenschutz.lu.ch/-/media/Datenschutz/Dokumente/Publikationen/dsb_lu_merkblatt_telefonueberwachung.pdf?la=de-CH.

hoeren@uni-muenster.de

Information about calls is stored for accounting purposes for 10 years. The investigating authority must seek a court to obtain this information which costs about 770 CHF per request. These costs act also a deterrent to use surveillance or metadata collection on a greater scale.

hoeren@uni-muenster.de

Data Protection in the United States: U.S. National Report

Shawn Marie Boyne

1 General Data Protection Framework

1.1 Introduction

The United States follows a sectoral approach to data privacy protection. There is no all-encompassing federal legislation that ensures the privacy and protection of personal data. Instead, legislation at the federal level primarily protects data within sector-specific contexts. In contrast to Europe's comprehensive Data Protection Directive, the United States relies on a combination of legislation at the federal and state levels, administrative regulations, as well as industry specific self-regulation guidelines. Privacy protection guarantees are sector specific and are located in a myriad of legislative instruments and case law. These statutes apply only to specific sectors such as "healthcare, education, communications, and financial services or, in the case of online data collection, to children".[1] Although, at first glance, comparative legal scholars are likely to dismiss America's privacy protection framework as less robust than the European approach, in some respects, the American framework provides greater protection than in Europe.[2]

[1] Terry (2017), pp. 19–27 at 21.

[2] Swire and Kennedy-Mayo (2017), pp. 617 and 642. Swire and Kennedy-Mayo argue that U.S. protections are stricter in seven ways:

> 1) oversight of searches by independent judicial officers; (2) probable cause of a crime as a relatively strict requirement for both physical and digital searches; (3) even stricter requirements for government use of telephone wiretaps and other real-time interception; (4) the exclusionary rule, preventing prosecutors' use of evidence that was illegally obtained, is

S. M. Boyne (✉)
Indiana University, Robert H. McKinney School of Law, Indianapolis, IN, USA
e-mail: smboyne@iupui.edu

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_17

hoeren@uni-muenster.de

1.2 Evolution of Personal Data Protection

The first data privacy legislation in the United States,[3] the Fair Credit Reporting Act (FCRA), was enacted in 1970.[4] The FCRA aimed to impose limits on data sharing in the consumer credit reporting industry and, in particular, to make it easier for individuals to correct reporting errors.[5] The FCRA established a tripartite model for subsequent data protection legislation that (1) provided notice to consumers of a specific type of data record, (2) established an administrative redress procedure administered by a government agency, and (3) defined the conditions under which law enforcement could access the data by meeting various standards of proof.[6]

In 1973, the U.S. Department of Health, Education, and Welfare (HEW) published a report entitled "Computers and the Rights of Citizens" which recommended that the government enact a Code of Fair Information Practices (FIPs).[7] Those practices would bind all organizations to comply with a code that would seek to protect personally identifiable information.[8] Practices that did not meet the standards of the code would be subject to government sanction.[9] In 1974, in the aftermath of the Watergate scandal, Congress ratified the Privacy Act.[10] Despite the fact that the HEW report called for legislation that would apply to "all automated personal data systems",[11] the final legislation applied only to federal agency databases.[12] The Act declared that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States".[13] The Privacy Act protects personal information that the U.S. General Services Administration maintains in systems of records (SORs).[14]

Despite the fact that Congress declared its commitment to the right to data privacy in 1974, the U.S. continues to lack a comprehensive data protection framework. The

supplemented by civil suits; (5) other legal standards that are relatively strict for government access in many non-search situations, such as the judge-supervised "reasonable and articulable suspicion" standard under ECPA; (6) transparency requirements, such as notice to the service provider of the legal basis for a request; (7) lack of data retention requirements for internet communications; and (8) lack of limits on use of strong encryption.

[3] Although European states commonly use the term "data protection", the phrase "data privacy" is more common in the United States. Swire and Ahmad (2012), p. 4.

[4] Title VI of Pub.L. 91-508, 84 Stat. 1114, enacted October 26, 1970.

[5] 15 U.S.C. § 1681 et seq.

[6] Cobb (2016), p. 2.

[7] *Id.* at 3.

[8] *Id.*

[9] *Id.*

[10] 5 U.S.C. § 552.

[11] Ware (1973), p. 5.

[12] 5 U.S.C. § 551(a).

[13] Raul et al. (2014), pp. 268–294 at 269.

[14] 5 U.S.C. § 552a(a)(5).

hoeren@uni-muenster.de

American lattice work of narrowly-tailored laws, and regulations at the federal and state levels enable government authorities, and, in some cases, private individuals, to bring lawsuits against organizations that are violating the law. However, in contrast to the European Union's data protection approach, which in many ways represents the gold standard of privacy protections, the dominant approach in the U.S. is grounded in consumer protection regulations.[15] Accordingly, in the United States, it is the Federal Trade Commission (FTC), an independent U.S. law enforcement agency charged with protecting consumers, which has become the primary privacy enforcement agency. However, because the FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act,[16] the FTC's jurisdiction is limited to challenging privacy violations by organizations whose information practices have been deemed "deceptive" or "unfair".[17] In that sense, the Privacy Act is not specifically a data privacy law, but rather a system of broad consumer protection laws that have "been used to prohibit unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information".[18]

In addition to its authority to take action against deceptive or unfair trade practices, Congress has granted the FTC authority to enforce several sector specific laws which include: "the Truth in Lending Act,[19] the CAN-SPAM Act,[20] the Children's Online Privacy Protection Act,[21] the Equal Credit Opportunity Act,[22] the Fair Credit Reporting Act,[23] the Fair Debt Collection Practices Act,[24] and the Telemarketing and Consumer Fraud and Abuse Prevention Act".[25] In addition, the Identity Theft Assumption and Deterrence Act charges the FTC which establishing a centralized complaint and consumer education service for victims of identity theft and strengthens the criminal laws concerning identity theft.[26]

[15]McGeveran (2016), pp. 959 and 961.

[16]The Federal Trade Commission Act (15 U.S.C. §§41–58) (FTC Act).

[17]Sotto and Simpson (2014), p. 191.

[18]Jolly (2016).

[19]15 U.S.C §1601.

[20]15 U.S.C. §7704.

[21]15 U.S.C. §§6501–6506 (restricts the online collection of personal information from children under the age of 13).

[22]15 U.S.C. § 1691.

[23]15 U.S.C. § 1681 (regulates the use and disclosure of "consumer reports" by consumer reporting agencies).

[24]15 U.S.C. § 1692.

[25]15 U.S.C. § 6101–6108 (protects consumers from invasive and fraudulent telemarketing practices).

[26]18 U.S.C. § 1028.

hoeren@uni-muenster.de

1.3 Major Sector-Specific Legislation and the Classification of Data

In addition to the legislation that comes within the FTC's jurisdiction, there are several other major pieces of federal sector-specific legislation:

1. Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U. S.C. §§6801–6827).
2. Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.)
3. Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S.C. §§7701–7713 and 18 U.S.C. §1037)
4. The Fair Credit Reporting Act (15 U.S.C. §1681).
5. Electronic Communications Privacy Act (18 U.S.C. §2510) regulates the interception of electronic communications
6. The Computer Fraud and Abuse Act (18 U.S.C. §1030) which criminalizes computer tampering.

Legislation title	Definition personal data[27]	Data classifications	Processing of information
Financial Services Modernization Act: (Gramm-Leach-Bliley Act) Protects consumers' *"nonpublic" personal information* when used by financial institutions	"Nonpublic personal information" means personally identifiable financial information that is provided by a consumer to a financial institution; resulting from a transaction with the consumer or from a service provided to the consumer; or otherwise obtained by the financial institution[28]	Nonpublic personal information is protected. Publicly available personal information is not protected	Financial institutions may transfer personal information to other companies if it is necessary to the performed financial services. Information may be shared with credit reporting agencies or financial regulatory agencies[29]
Health Insurance Portability and Accountability Act (HIPPA)	'Protected health information' means individually identifiable health information: (1) Except as	Under the Act there is protected health information (PHI) and "electronic Protected Health Information".	The Security Rule establishes the minimum requirements for all health care entities and

(continued)

[27]The legislative enactments in this chart are not based on sector specific protections rather than on broad rights to personal data protection as exist in the European Union.

[28]15 U.S. Code §6809(4).

[29]https://epic.org/privacy/glba/.

hoeren@uni-muenster.de

Legislation title	Definition personal data	Data classifications	Processing of information
	provided in paragraph (2) of this definition,[30] that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium[31]	(e-PHI) While HIPPA protects PHI, there are additional requirements that apply to e-PHI[32]	contractors which require all data processors to (1) adopt administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the information; and (2) report security incidents[33]
Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)	Regulates the collection and use of e-mail addresses. Covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service", including email that promotes content on commercial websites	Regulates "commercial" and "transactional or relationship" emails. Commercial email must include non-deceptive sender and subject information; opt-out provisions; sender's address; and clear and conspicuous identification that the e-mail is an advertisement or solicitation[34]	The Act imposes criminal penalties on individuals who: harvest email addresses or generate them through a dictionary attack[35]

(continued)

[30]"(2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g (a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer." See §160.103.

[31]Individually identifiable health information includes demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. See 45 CFR 160.103.

[32]Specifically, covered entities must: "Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; Identify and protect against reasonably anticipated threats to the security or integrity of the information; Protect against reasonably anticipated, impermissible uses or disclosures; and ensure compliance by their workforce." See https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[33]Eisenhauer (2007), p. 2.

[34]15 U.S.C. §§7701–7713.

[35]"CAN-SPAM Act: A Compliance Guide for Business", Federal Trade Commission. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

hoeren@uni-muenster.de

Legislation title	Definition personal data	Data classifications	Processing of information
The Fair Credit Reporting Act (15 U.S.C. §1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108–159) which amended the Fair Credit Reporting Act)	Applies to consumer reporting agencies, those who use consumer reports (such as a lender) and those who provide consumer-reporting information (such as a credit card company)	"Consumer reports" are any communication issued by a consumer reporting agency (CRA) regarding a consumer's creditworthiness, credit history, credit capacity, character, and general reputation that is used to evaluate a consumer's eligibility for credit or insurance[36]	A CRA must, "follow reasonable procedures to assure accuracy of the information."[37] Where data are "inaccurate or incomplete or cannot be verified", a CRA must immediately correct the data[38]
Electronic Communications Privacy Act (18 U.S.C. §2510)	Prohibits wiretaps of communications of others without court approval without a party's prior consent. Prohibits the use or disclose any information acquired by illegal wiretapping or electronic eavesdropping[39]	Interception "means the aural or other acquisition of the contents" of various kinds of communications by means of "electronic, mechanical or other devices"[40]	"Content" means "information concerning [its] substance, purport, or meaning"[41]
Computer Fraud and Abuse Act (18 U.S.C. §1030)	Seeks to prevent and punish hacking-related activities which the Act defines as "unauthorized access" to protected computers.[42] In addition, the Act bars individuals or entities from exceeding the scope of their "authorized access"[43]	"Protected computers" includes: those used by financial institutions, the U.S. government, and computers used in or affecting interstate or foreign commerce or communication[44]	The Act defines "damage" as any impairment to the integrity or availability of data, a program, a system, or information[45]

[36] 15 U.S.C. § 1681(d)(1).
[37] 15 U.S.C. § 1681e (2013).
[38] 15 U.S.C. § 1681i (a)(5)(A) (2013).
[39] Doyle (2012), p. i.
[40] *Id.* at. 9.
[41] 18 U.S.C. 2510(8).
[42] 18 U.S.C. § 1030.
[43] 18 U.S.C. § 1030(e)(6).
[44] 18 U.S.C. § 1030(e)(2).
[45] 18 U.S.C. §1030(a)(5).

hoeren@uni-muenster.de

1.4 Supervisory Agencies

As stated above, the FTC has become the leading privacy enforcement agency in the United States.[46] Today, the agency has even extended its jurisdiction to include undertaking consumer protection enforcement actions against foreign companies that do business in the U.S.[47] Using its authority arising out of Section 5 of the Federal Trade Commission Act, the FTC has taken a leading role in bringing privacy deception and unfair trade practices cases and enforcement actions.[48] Illustrating the breadth of the agency's expanded reach, as of November 2013, the agency had brought "134 spam and spyware cases, 108 Do Not Call cases against telemarketers, 97 Fair Credit Reporting Act lawsuits involving credit-reporting problems, 47 data security cases, 44 general privacy lawsuits, and 21 actions under the Children's Online Privacy Protection Act ("COPPA")".[49]

As Congress has continued to pass sector-specific privacy legislation, it has continued to enhance the FTC's enforcement role. The agency also reports to Congress and recommends the enactment of additional privacy-related legislation.[50] Perhaps more importantly, the broadening reach of the FTC's enforcement actions and consent decrees have fueled the growth of a "new common law of privacy".[51] Professors Daniel Solove and Woodrow Hartzog have argued that, because the FTC's enforcement actions nearly always result in settlement agreements, the content of those agreements have, in effect, become a new common law of privacy that companies look for guidance in developing privacy practices.[52]

Although the FTC also enforces the GLB Act, federal banking agencies as well as state level insurance agencies may also bring actions under the Act.[53] HIPPA is enforced by the Office of Civil Rights within the U.S. Department of Health and Human Services.[54] In addition to the enforcement powers of federal agencies, state consumer protection regulators (usually the state Attorney General) also exercise privacy regulatory authority.[55]

---

[46] See Sect. I(B).

[47] Brill (2012).

[48] Raul et al. (2014), p. 284.

[49] Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework (November 12, 2013). Available online at: https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf.

[50] Jolly (2016), Sect. 25.

[51] Solove and Hartzog (2014), p. 583.

[52] *Id.* at pp. 611–627.

[53] Jolly (2016), Sect. 25.

[54] *Id.*

[55] Raul et al. (2014), p. 284.

hoeren@uni-muenster.de

Although the FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace, the agency also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[56] The Commission is empowered to bring enforcement actions to stop violations of the law and to force companies to take affirmative steps to remediate their unlawful behavior. These steps include: "implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust transparency and choice mechanisms to consumers".[57] In addition, FTC has the power to seek civil monetary penalties against organizations or individuals who violate the FTC Act, as well as against entities that violate the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule.[58] The forms of relief for privacy violations that the FTC has secured include injunctive relief, damages, and consent decrees which require companies to submit to the FTC's ongoing oversight and to implement controls, audits, and other privacy enhancing processes during a period of time that can span decades.[59]

1.5 Self-Regulation Instruments and Data Protection

The Network Advertising Initiative, formed in 1999, is a robust self-regulation framework that is comprised exclusively of third-party digital advertising companies. The NAI relies on a thorough new member review process, technical monitoring tools, and investigation of consumer concerns to encourage compliance with the organizations Self-Regulatory Code of Conduct.[60] According to NAI's 2015 Update to the Code of Conduct, the organization may impose sanctions, including suspension or revocation of membership and may refer the matter to the Federal Trade Commission for non-compliance.[61] In addition, the NAI may publicly name a company or the violation in its annual compliance report, and in the press, when

[56]Federal Trade Commission, Privacy & Data Security Update (2016). Available online at: https://www.ftc.gov/reports/privacy-data-security-update-2016.
[57]*Id.*
[58]*Id.*
[59]*Id.*
[60]"Enforcement", Network Advertising Initiative (April 2016). Available at https: www.networkadvertising.org/code-enforcement/enforcement.
[61]*Id.*

hoeren@uni-muenster.de

NAI determines that a member has engaged in a material violation of the 2015 Code of Conduct.[62]

In addition, another industry organization comprised of marketing and advertising industry associations was established in 2009. Its membership includes the Association of National Advertisers, The American Advertising Federation, the American Association of Advertising Agencies, the Network Advertising Initiative, Direct Marketing Association (DMA), and Interactive Advertising Bureau.[63] The Network Advertising Initiative (NAI) has adopted a self-regulatory code that requires transparency, an opt-in choice before sensitive information may be used for behavioral advertising, and reasonable security provisions.[64] However, the FTC has criticized the NAI's definition of "sensitive information" as being too narrow.[65] A relatively new organization, the Digital Advertising Alliance (DAA) requires companies to "inform consumers of data practices, allow consumers to opt out of behavioral advertising, maintain reasonable security for the data collected, and refrain from using sensitive information for behavioral advertising without consumers' opt-in consent".[66] Starting in 2011, the DAA expanded its efforts to include social networks and non-advertising firms. Enforcement is handled by the DMA and the Council of Better Business Bureau.[67]

Despite the fact that the FTC issued guidelines and best practices for self-regulation of consumer privacy in both 2009 and 2012, self-regulation covering the use of digital information has obtained only mixed results.[68] Critics contend point to the growing use of online behavioral advertising (OBA) and other forms of personalization in the advertising field as evidence that self-regulation does not preserve consumer privacy.[69]

[62] *Id.*

[63] Listokin (2017), pp. 92–95 at 94.

[64] Digital Advert. All., Self-Regulatory Principles for Online Behavioral Advertising 12, 14–15, 17 (2009), http://digitaladvertisingalliance.org/sites/digital.daaoperations.org/files/DAA_files/seven-principles-07-01-09.pdf.

[65] Rich (2015), p. 2.

[66] Federal Trade Commission, "Cross-Device Tracking an FTC Staff Report", January 2017 at 1, *citing* Digital Advert. All., Self-Regulatory Principles For Online Behavioral Advertising 12, 14–15, 17 (2009), http://digitaladvertisingalliance.org/sites/digital.daaoperations.org/files/DAA_files/seven-principles-07-01-09.pdf.

[67] Listokin (2017), p. 94.

[68] *Id.*

[69] Castro (2011), p. 8.

hoeren@uni-muenster.de

2 Personal Data Processed by Electronic Means

2.1 Services Provided at a Distance

The primary piece of legislation that is designed to protect personal data related to services provided at a distance is the Fair and Accurate Credit Transactions Act (FACTA) enacted in 2003.[70] FACTA was specifically designed to protect consumers from identify theft and to ensure that consumers' credit information is accurate. The Act requires the three main credit reporting agencies in the U.S. to provide consumers with one free credit report per year. In an effort to improve the security of card-related data, the Act requires retail systems that print payment card receipts to use PAN truncation (personal account number truncation) so that transaction receipts do not contain a consumer's complete account number.[71] The Act also contains a provision that allows consumer to place fraud alerts in their credit files so that they may monitor certain types of purchases to protect against fraud. The Act creates a private cause of action for consumers who can show a "concrete harm".[72]

With respect to the privacy of entertainment services, there are two federal statutes on the books: the Cable Communications Policy Act of 1984 (CCPA)[73] and the Video Privacy Protection Act of 1988 (VPPA).[74] Under the terms of the CCPA, cable companies are prohibited from collecting personally identifiable information concerning subscribers without the prior consent of the subscriber.[75] Cable companies must also destroy personal data when that data is no longer necessary for the purpose for which it was collected.[76] The VPPA contains provisions similar to the CCPA and prevents providers from knowingly disclosing personal information without the subscriber's written consent.[77] Courts have denied the claims of a number of parties seeking damages under VPPA in cases where the court has held that the shared data did not qualify as personally identifiable information. These denials have included cases involving a consumer's Roku serial number[78] as well as an encrypted serial number on a digital streaming device.[79]

Although the FTC proposed a "Do Not Track" mechanism in 2010 that would allow consumers to choose whether to allow websites to collect information about

[70] Pub. L. No. 108–159, 117 Stat. 1952, codified to 15 U.S.C. §§ 1681–1681x.

[71] Braverman (2013).

[72] Spokeo, Inc. v. Robins, 136 S.Ct. 1540 (2016).

[73] 47 U.S.C. §551.

[74] 18 U.S.C. §§2710–2711.

[75] 47 U.S.C. §551(b)(1).

[76] 47 U.S.C. §551(e).

[77] 18 U.S.C. §§2710(2)(B). Pursuant to the Amendments Act of 2012, a videotape service provider may obtain a consumer's consent through the internet. 18 U.S.C. §2710.

[78] Eichenberger v. ESPN, Inc., No. C14-463 TSZ, 2015 WL 7252985 (W.D. Wash. May 7, 2015).

[79] Robinson v. Disney Online, 152 F.Supp.3d 176 (S.D.N.Y. 2015).

hoeren@uni-muenster.de

their internet activity, at the present time, it is up to internet search engines to voluntarily implement changes to their browsers to block annoying ad formats.[80] Many states, most notably California, have enacted online privacy protection legislation. Many of these identity-theft protection measures impose an obligation on business entities to protect social security numbers and similar person data against unauthorized use.[81] California's Online Privacy Protection Act requires any person or entity that collects personally identifiable information from California residents through an internet Web site or online service for commercial purposes, to identify the categories of information that it collects about individual consumers as well as to post a conspicuous privacy policy on its Web site or online service.[82] At least four states have enacted legislation that protects the personal information of users of digital book services and technologies.[83]

2.2 *Electronic Communications for Marketing Purposes*

The small number of laws that regulate electronic marketing target specific marketing channels.[84] At the federal level, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) regulates all commercial email.[85] The Act applies to any business entity or individual that initiates or sends commercial messages via email. Critically, it gives recipients of commercial emails the right to prohibit marketers from continuing to email them.[86] It covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service". This includes all email that promotes content on commercial websites.[87] The law makes no exception for business-to-business email as even messages to former customers announcing new products must comply with

[80]Toner (2017).

[81]See, *e.g.*, "State Laws Related to Internet Privacy", National Conference of State Legislatures. Available online at: http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

[82]Calif. Bus. & Prof. Code § 22575–22578 (CalOPPA).

[83]These states include: Arizona, California, Delaware, and Missouri.

[84]Sotto and Simpson (2014) (Gideon Roberton (2014)). P. 192. Pp. 191–198. Available online at: https://www.hunton.com/files/Publication/1f767bed-fe08-42bf-94e0-0bd03bf8b74b/Presentation/PublicationAttachment/b167028d-1065-4899-87a9-125700da0133/United_States_GTDT_Data_Protection_and_Privacy_2014.pdf.

[85]15 U.S.C. §§ 7701–7713.

[86]"CAN-SPAM Act: A Compliance Guide for Business", Federal Trade Commission Website. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business. Last accessed on 17 July 2017.

[87]See 15 U.S.C. § 7702(2)(A).

hoeren@uni-muenster.de

the law.[88] It is important to note that the CAN-SPAM Act does not create a private right of action for consumers; instead the primary responsibility for enforcement of the Act falls within the FTC's jurisdiction.[89] A host of federal and state agencies, along with internet service providers (ISPs) also possess the ability to enforce provisions of the Act.[90]

From the perspective of privacy rights advocates, the FTC has failed to adequately protect consumers' privacy rights with respect to the collection of consumer information and the use of Big Data.[91] Rather than draft rules to would govern how corporations collect consumer data, the agency has chosen a less adversarial strategy that seeks to raise awareness about the issues that companies should consider when collecting data.[92] In stark contrast to the rights enjoyed by European consumers, American consumers do not possess "a right to be forgotten.[93] Nor is there a single federal notification law that mandates notification in case of a data breach.[94] While U.S. officials and industry representatives maintain that America's sector-specific approach to data regulation is more nimble than Europe's blanket protections of privacy, some European legislators charge that the U.S. approach protects commerce at the expense of consumers.[95] Rather than impose strong regulations with respect to the collection of consumer data, the FTC has drafted Behavioral Advertising Principles.[96] These principles suggest that website operators that collect and/or store consumer data for behavioral advertising should provide reasonable data security.[97]

2.3 *Children's Online Privacy Protection Act of 1998 (COPPA)*

COPPA regulates the collection and use of information collected from children under the age of 13 by internet websites and mobile apps. Congress has assigned the principle enforcement responsibility to the FTC and has given the agency the power to promulgate rules to guide the interpretation and enforcement of the Act. In 2000, the FTC first promulgated the Children's Online Privacy Protection Rule. That Rule detailed regulations governing the collection and use of personal information

[88] *Id.*
[89] Brennan (2016).
[90] Brennan (2016).
[91] Lazarus (2016).
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] Singer (2013).
[96] See, *infra*, Sect. 1.5.
[97] Jolly (2016), Sect. 7.

hoeren@uni-muenster.de

from and about children online. While the FTC's original rule prohibited operators of websites or online services directed at children from collecting personal information from a child, as technology has evolved to expand the ways in which advertisers can potentially target children, the FTC has updated and expanded the focus of the COPPA regulations. Specifically, in 2013, the FTC amended the COPPA rule to expand the definition of "personal information" to include persistent identifiers that recognize users over time and across different online services, all behavioral advertising on online services directed at children now require parental notice and consent. Specifically, COPPA requires that children's websites post privacy policies that describe "what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information". It applies to operators of online websites or services directed to children, including makers of mobile apps, and "any operator that has actual knowledge that it is collecting personal information from a child". The legislation also requires internet website operators to obtain a more reliable method of consent if an operator seeks to disclose a child's personal information to third parties or to make it publicly available.

Under the amended rules promulgated by the FTC, which went into effect in 2013, "communications data" includes the following types of information:

A. A child's first and last name;
B. A home or other physical address including street name and name of a city or town;
C. Online contact information;
D. A screen or user name that functions as online contact information;
E. A telephone number;
F. A social security number;
G. A persistent identifier that can be used to recognize a user over time and across different websites or online services;
H. A photograph, video, or audio file, where such file contains a child's image or voice;
I. Geolocation information sufficient to identify street name and name of a city or town; or information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above.

Since the FTC promulgated the 2013 policy changes, the agency has issued additional guidance stating that internet connected toys and other devices intended for children fall under the provisions of the Act. With respect to COPPA's data protection and retention policies, the new changes require that covered website operators adopt reasonable procedures for data retention and deletion. The legislation also requires that parents have the ability to review personal information collected about their children and request that it be deleted. COPPA requires that site operators protection the confidentiality and security of any information that is collected from children online. Although the FTC has suggested that site operators require the use of passwords to access personal information on the website, install of

hoeren@uni-muenster.de

intrusion-detection software to monitor unauthorized access, and use of secure web servers and firewalls to ensure confidentiality, data breaches have occurred.

The FTC is the primary agency entrusted with prosecuting COPPA violations on the federal level. Because COPPA violations are considered to be unfair or deceptive trade practices under § 5 of the Federal Trade Commission Act, the FTC can impose civil penalties for its violation. State-level attorneys general are authorized to bring compliance actions in federal district court. Although the COPPA Act itself does not establish dollar penalty figures, courts determine damages based on Section 5 of the FTC Act. While the maximum penalty figure for Section 5 violations was originally set at $16,000 per violation, as of August 1, 2016, the maximum civil penalty nearly doubled to $40,654 per violation. Because a violation is defined as each incident in which a website or app collects personal information falling under the Act, the size of potential civil penalties is extremely large.

The 2003 case, *United States v. Boston Scientific Corp*., 253 F. Supp. 2d 85, 98 (D. Mass. 2003), developed a six-step process for determining damages pursuant to 15 U.S.C. §45(a)(1). Those factors include: the level of harm to the public; the benefits gained by the defendant; the good or bad faith of the violator [willful versus negligent conduct]; the defendant's ability to pay; the deterrence value of the penalty for this defendant and other operators; and an amount needed to vindicate the FTC's authority. Although there is no private cause of action for COPPA violations, states may file civil actions to obtain injunctions and damages in the interest of their citizens.

2.4 Mandated Opt-Out Systems

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, covers all commercial messages,[98] which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service", including email that promotes content on commercial websites. Pursuant to this Act, the sender of the message must clearly and conspicuously disclose that the message is an advertisement.[99] The message must explain how recipients may opt out of receiving future email using clear and conspicuous language that an ordinary person can recognize, read, and understand.[100] Although senders of marketing based

[98]Under the Act commercial messages are defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an internet web site operated for a commercial purpose)." 15 U.S.C. 7702(2)(A).

[99]15 U.S.C. § 7704.

[100]"CAN-SPAM Act: A Compliance Guide for Business", Federal Trade Commission Website. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business. Last accessed on 17 July 2017 [hereinafter Compliance Guide].

hoeren@uni-muenster.de

emails may create menu options that allow the recipient to opt out of some messages, the choices must also contain the option to stop all commercial communications.[101] Marketers must honor recipients' opt-out request within 10 business days.[102] The potential penalties that may be imposed for each separate email sent in violation of the law include a fine of up to $40,654.[103] In addition, after the consumer has submitted an opt-out request, neither the sender nor any person who knows of the opt-out request may "sell, exchange, or otherwise transfer the recipient's e-mail address without the recipient's affirmative consent, except as required by law".[104]

2.5 Processing of Personal Data of Employees

2.5.1 Email & Computer Storage

As a general rule, employees in the United States enjoy few privacy rights in the workplace. The Electronic Communications Privacy Act of 1986 (ECPA) is the primary federal law that governs the monitoring of electronic communications in the workplace.[105] The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act Of 1968 which originally addressed the interception of "wire communications". While the ECPA in general prohibits individuals and companies from intercepting oral, wire, and electronic communications,[106] there are two exceptions to this prohibition that apply to the workplace. According to the business purpose exception, employers may monitor employees' electronic communications as long as the monitoring is done in the "ordinary course of business" and the employer uses certain limited types of equipment to monitor the communications.[107] Federal courts have held that any emails sent using company equipment are considered to be company property.[108] With respect to email activity, any emails sent using company equipment are considered to be company property.[109] Employers who have a valid business purpose for monitoring employee email may view employee email.[110] In

[101] *Id.*

[102] See 47 C.F.R. § 64.3100(b)(1), (6).

[103] Compliance Guide for Business, *supra* note 100.

[104] Brennan (2016).

[105] "Managing Workplace Monitoring and Surveillance", Society for Human Resource Management, 18 February 2016. Available online at: https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx.

[106] 18 U.S.C.S. § 2510(4).

[107] 18 U.S.C.S. § 2510(5)(a).

[108] See Williams v. Poulos, 11 F.3d 271, 280 (1st Cir. 1993).

[109] "Privacy in the Workplace: Overview", FINDLAW, Available online at: http://employment.findlaw.com/workplace-privacy/privacy-in-the-workplace-overview.html. Last accessed on 18 July 2017.

[110] *Id.*

hoeren@uni-muenster.de

fact many employers now use email systems that copy all email messages that pass through the system to check for issues related to employee productivity and illegal conduct.[111] In addition, employers have the right to track the websites visited by their employees, to block employees from visiting specific internet sites, or to limit the amount of time an employee may spend on a specific website.[112] Finally, it is important to recognize that because Title III's definition of "electronic communications", does not include communications held in electronic storage, courts have granted free reign to read the private email of employees stored in systems such as an electronic bulletin board.[113] As a result, although Title III prohibits the "interception" of electronic communications in real time, it does not prohibit the retrieval of that communication after it has been put into "electronic storage".[114]

Even if the employer's monitoring program does not explicitly further a business purpose, employers may lawfully monitor communications under the "consent exception" provided that they have an employee consents to monitoring.[115] Because the consent exception is not limited to business communications, a company may arguably monitor personal electronic communications if it can show employee consent. Some courts have held that consent may be implied in cases where employers have informed their employees: "1) of the manner in which the monitoring will be conducted; and 2) that he or she will be subjected to such monitoring."[116]

Employees who work for public employers such as Federal and State agencies also enjoy the protection of the Fourth Amendment to the U.S. Constitution. This Amendment and the case law surrounding it protect public employees from "unreasonable government searches".[117] Public employers who conduct searches that exceed the scope of a legitimate business purpose may put themselves at risk of violating the Constitution and exposing their agency to a suit brought pursuant to 42 U.S.C. §1983. However, the scope of Fourth Amendment protections in the workplace may be shrinking in the digital world. While the Supreme Court, in *O'Connor v. Ortega* (1983),[118] held that a government employee had a legitimate expectation of privacy in the contents of his desk and file cabinets,[119] the Court stated that in determining whether an employee's expectation of privacy is a

[111] *Id.*

[112] "Privacy in the Workplace: Overview", Findlaw, Available online at: http://employment.findlaw.com/workplace-privacy/privacy-in-the-workplace-overview.html Last accessed on 18 July 2017.

[113] Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994), aff'g 816 F. Supp. 432 (W.D. Tex. 1993).

[114] Caragozian and Warner Jr (2000).

[115] 18 U.S.C. § 2511(2)(d).

[116] Caterine (2009).

[117] Gray Plant Mooty & the Minnesota Department of Employment and Economic Development, A Legal Guide to Privacy and Data Security (2017). P. 68. Available online at: https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf.

[118] 480 US 709 (1987).

[119] 480 U. S. 714–719.

hoeren@uni-muenster.de

reasonable one, courts must balance the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace.[120] In addition, government employers may weaken employees' expectations of privacy by simply informing employees in advance that their desks, computers, and lockers may be searched for a legitimate business purpose.[121]

In addition to the ECPA, employees have tried to file claims against employers using the state level common law protections against invasion of privacy. However, those causes of action provide employees with only very limited protections against monitoring. Employees seeking to recover damages using the tort theories of intrusion upon seclusion and the publication of private facts must demonstrate that they have a reasonable expectation of privacy in the information which has been monitored.[122]

Some states, notably California and Massachusetts, have enacted privacy rights legislation.[123] Despite the statute's name, the Massachusetts Right of Privacy Act,[124] does not create significant new privacy rights for employees.[125] To begin, the language of the statute addresses individuals in general rather than employees: "A person shall have a right against unreasonable, substantial or serious interference with his privacy."[126] When courts have interpreted the statute in the workplace context, they have used a balancing test that seeks "to balance the employer's legitimate business interest in obtaining and publishing the information against the substantiality of the intrusion on the employee's privacy resulting from the disclosure".[127]

2.5.2 CCTV Cameras

There is no explicit protection in U.S. federal law that protects employees against the use of CCTV cameras for monitoring purposes unless employees are engaged in "protected concerted activity" such as union meetings. Section 7 of the National Labor Relations Act protects workers' "right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their

[120] 480 U.S. 719–726.

[121] "Workplace Privacy", Epic.Org, Electronic Privacy Information Center. Available online at: https://www.epic.org/privacy/workplace/.

[122] Gray Plant Mooty & the Minnesota Department of Employment and Economic Development, A Legal Guide to Privacy and Data Security (2017). p. 66. Available online at: https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf.

[123] See, *e.g.*, Minn. Stat. §626A.02 Subd. 1.

[124] G.L. 214 §1B.

[125] Litwin (2006).

[126] G.L. 214 §1B.

[127] Bratt v. Int'l Bus. Machs. Corp., 392 Mass. 508, 521 (1984).

hoeren@uni-muenster.de

own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection."[128] Employers who monitor union organizing activities may face complaints that they sought to intimidate or deter employees from exercising their federal rights.[129]

Employers who seek to monitor employee's performance through the use of hidden surveillance cameras must provide notice to labor unions before installing the cameras in the workplace. In addition, employers must provide the opportunity to negotiate and bargain over this action. There are key limits to workers' protections under the National Labor Relations Act. Notably, the Act does not apply to anyone employed by Federal, state, or local governments, agricultural laborers, anyone employed as a supervisor, employees of railroads and airlines, and employees of retailers whose gross annual volume is less than $500,000.[130]

2.5.3 Sharing of Employee Information Posted on Social Media in the Disciplinary Context

Employer monitoring of employee activity on social networks may run afoul of the Stored Communications Act (SCA),[131] state regulations, as well as trigger liability under a common law invasion of privacy claim.[132] Congress enacted the SCA to protect electronic communications that are configured to be private and are stored electronically.[133] However, it does not protect electronic communications that are readily available to the public or have been disclosed by an authorized user of the account.[134] Employees who share information about their employers on social media platforms like Facebook with other employees cannot recover damages if their fellow Facebook "friends" share that information with their supervisors. In *Ehling v. Monmouth-Ocean Hospital Service Corp*., the court denied relief to the plaintiff who was fired based on the content of her Facebook posts.[135] Although the court held that private Facebook posts fall within the protections of the SCA, the employer had lawfully gained access to the posts by another "authorized user"—a co-worker and Facebook "friend" of the plaintiff.[136] Because the plaintiff authorized her coworker to access her Facebook wall as her Facebook "friend", when the plaintiff's

[128] 29 U.S.C. § 151–169.

[129] Section 8(a)(1).

[130] "Jurisdictional Standards", National Labor Relations Board. Available online at: https://www.nlrb.gov/rights-we-protect/jurisdictional-standards.

[131] 18 U.S.C. § § 2701–11.

[132] Hamilton (2016).

[133] 18 U.S.C.S. § 2511(2)(g)(i).

[134] 18 U.S.C.S. § 2511(2)(g)(i).

[135] 961 F. Supp. 2d 659 (D. New Jersey 2013).

[136] 961 F. Supp. 2d 669–670.

hoeren@uni-muenster.de

coworker shared the information with their employer, the access gained by the employer fell under the "authorized access" exception to the ACA.[137]

Employers who gain unauthorized access to employee accounts and use that access to discipline or terminate employees risk civil liability under the SCA.[138] Even in cases where employer obtains material through authorized access to those accounts, employers must be careful not to "unnecessarily infringe on employees' Section 7 rights under the National Labor Relations Act to gripe about terms and conditions of employment".[139] However, Section 7 does not protect employees whose posts negatively affect a company's image as long as the employer lawfully obtained access to the posts.[140] As applied to blogging, several cases have ruled that an employer who gains unauthorized access to an employee's password-protected blog—and punishes or fires the employee for content appearing on that blog—may violate the SCA and, if found to be liable, could be required to pay damages to the aggrieved employee.[141]

Another key issue with respect to the privacy of employee social media accounts is whether employers may compel employees or prospective employees to disclose their passwords to permit the employer to monitor those accounts. Since 2012, 25 states have enacted legislation that prevents employers from forcing employees to disclose their passwords.[142] Sixteen states have passed legislation that bars educational institutions from requiring students to reveal their passwords.[143] One state, Wisconsin, bars landlords from requiring tenants to share their passwords.[144]

2.6 *Other Protections for Employees' Personal Data Conveyed or Stored Electronically*

In addition to the SCA's protection against the unauthorized access of employee social media posts, a number of federal statutes require that employers protect a variety of different types of data. These include the obligation to protect medical records under HIPPA, as well as the diverse requirements under the Family and Medical Leave Act (FMLA), the Genetic Information Nondiscrimination Act

[137] *Id.*, citing 18 U.S.C. § 2701(c)(2).

[138] Crane (2012), pp. 639 and 642 citing Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

[139] Grosdidier (2013).

[140] 29 U.S.C. §§ 157.

[141] Grosdidier (2013).

[142] "State Social Media Privacy Laws", National Conference of State Legislatures, 5 May 2017. Available online at: http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx.

[143] *Id.*

[144] Wis. Stat. § 995.55(4).

hoeren@uni-muenster.de

(GINA), the Americans with Disabilities Act (ADAAA), and other statutes that specifically protect personally identifiable information such as the Fair and Accurate Credit Transactions Act.[145] Pursuant to this legislation, employers must keep Information about an employee's medical condition, genetics, disability, reasonable accommodations, and positive drug test results in a separate, confidential, secure electronic or physical file, and disclosed only to those within the company who need to know the information.[146]

2.7 *Data Breach Notification Obligations*

Despite efforts to pass legislation on the federal level that would mandate notification procedures across industry sectors, the only applicable federal legislation to date is the sector specific legislation in the credit, financial services, health care, government, securities, and internet sectors.[147] The various sector-specific legislative enactments contain Information security provisions that are designed to protect personally identifiable information or sensitive personal information from unauthorized disclosure, acquisition, or access.[148] These notification provisions usually require covered entities to implement a notification policy and include provisions for incident reporting and handling as well as breach notification requirements.[149]

The major privacy rights laws that contain breach provisions are detailed in the Table below:

Name of legislation	Industry targeted	Breach provisions	Security provisions
Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 111-5) (2009). Section 13407	Health Care	Section 13410(d) of the HITECH Act	Requires web-based businesses to notify consumers when the security of their electronic health information is breached. Applies to both vendors of personal health records, which provide online record keeping systems that consumers may use to track their health records, and

(continued)

[145] McGinnis (2014).
[146] *Id.*
[147] Stevens (2010), p. 1.
[148] *Id.*
[149] *Id.*

hoeren@uni-muenster.de

Name of legislation	Industry targeted	Breach provisions	Security provisions
			entities that offer third-party applications for personal health records[150]
"Safeguarding Against and Responding to the Breach of Personally Identifiable Information". OMB Memorandum M-07-16	Federal Government Agencies	Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974	Requires federal agencies to implement a breach notification policy to safeguard "personally identifiable information". Agencies must report all incidents involving personally identifiable information within one hour of discovery/detection. Following the detection of a breach, agencies should notify affected parties without unreasonable delay unless law enforcement, national security, or agency needs permit a delay[151]
Veterans Affairs Information Security Act[152]	Department of Veterans Affairs	38 U.S.C. §§5724 and 5727	In the event of a "data breach" of sensitive personal information processed or maintained by the VA Secretary, the Secretary must ensure that either a non-VA entity or the VA's Inspector General conduct an independent risk analysis of the data breach to determine the level of risk associated with the data breach.[153] Based upon this analysis, if a reasonable risk of the potential misuse of sensitive personal

(continued)

[150]Health Breach Notification Rule, 16 C.F.R. 318.

[151]Stevens (2010), p. 8.

[152]The Veterans Benefits, Health Care, and Information Technology Act of 2006, P.L. 109–461 (December 22, 2006); 38 U.S.C. §§ 5722 et seq.

[153]38 U.S. C. § 5724(a)(1).

hoeren@uni-muenster.de

Name of legislation	Industry targeted	Breach provisions	Security provisions
			information exists, the Secretary must provide credit protection services in accordance with regulations issued by the VA Secretary.[154] The VA must notify individuals affected by the breach within 60 days of the breach[155]
Financial Services Modernization Act: (Gramm-Leach-Bliley Act)	Institutions engaged in the financial services industry	§ 501(b) of the Gramm-Leach-Bliley Act (GLBA)[156]	When a breach occurs, the institution must conduct an investigation to determine the likelihood that the information has been or will be misused. If misuse has occurred or is reasonably possible, the institution must notify the affected customer as soon as possible, except in cases where a law enforcement determination that notification will interfere with a criminal investigation[157]
Fair Credit Reporting Act	Retail businesses[158]	15 U.S.C. § 1681	When identity theft is suspected, the credit reporting agency must include a fraud alert in

(continued)

[154]38 U.S.C. § 5724(a)(2).

[155]VA Handbook 6500.2, Section 4(c), p. 48. July 28, 2016. Available online at: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=843&FType=2.

[156]See "Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice", Federal Deposit Insurance Program, 1 April 2005. Available online at: https://www.fdic.gov/news/news/financial/2005/fil2705.html.

[157]Saikali (2012).

[158]FACTA includes a "truncation" requirement that applies to anyone who accepts credit or debit cards as a form of payment. According to this requirement, the business entity may not print a receipt that contains more than the last five digits of the card number or print the card's expiration date on any receipt given the customer at the point of the transaction. Transactions where the consumer enters the account number by handwriting or the business uses an imprint of the card are not bound by this requirement. Under the provisions of the Act, any person who negligently violates the truncation requirement may be required to pay actual damages and attorneys' fees. See 15 U.S.C. §§ 1681o(a) and 1681n(a).

hoeren@uni-muenster.de

Name of legislation	Industry targeted	Breach provisions	Security provisions
			the file of that consumer, and also provide that alert along with any credit score generated.[159] Consumers are entitled to receive free annual credit reports from the top credit reporting agencies.[160] The Act also requires some banks and other financial institutions to disclose credit report information to their consumers and to develop programs to prevent and mitigate identity theft.[161] Finally, the Act aims to help victims of identity theft by requiring lending institutions to notify victims of their rights[162]

3 Data Protection in the Electronic Communications Sector

The primary federal legislation that regulates the privacy of electronic communications is the Electronic Communications Privacy Act of 1986.[163] The ECPA updated the Federal Wiretap Act of 1968, which "addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications".[164] The ECPA regulates the interception of

[159] 15 U.S. Code § 1681c–1.

[160] "The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report", Epic.org. Available online at: https://epic.org/privacy/fcra/.

[161] *Id.*

[162] *Id.*

[163] 18 U.S.C. § 2510-22. The ECPA also includes the Stored Wire Electronic Communications Act.

[164] "Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22", Justice Information Sharing, U.S. Dept. of Justice, Office of Justice Programs, Bureau of Justice Assistance, last updated on: 30 July 2013. Available online at: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 Last accessed on 13 August 2017 [hereinafter ECPA 1986].

hoeren@uni-muenster.de

three types of communications: wire communications,[165] oral communications,[166] and electronic communications.[167] As amended, the ECPA, not only protects wire, oral, and electronic communications while those communications are being made and are in transit, but also when they are stored on computers.[168] The ECPA creates a tiered system of protections based on the level of privacy interests in the data.[169] For example, the ECPA grants higher privacy protection to the content of stored emails than in basic subscriber information.[170] In some respects, these levels of protection track with established Fourth Amendment case law.[171] For example, a customer or subscriber has no reasonable expectation of privacy in her subscriber information or transactional records under the U.S. Supreme Court's Third Party doctrine.[172] The ECPA also blocks third parties and internet service providers (ISPs) from accessing these communications without legitimate authorization.[173]

Unfortunately, attempts to invoke the provisions of the ECPA under Title I (Wiretap Act) or Title II (Stored Communications Act) to curtail the use of personal information by commercial entities are typically unsuccessful because the ECPA does not apply in cases of user consent.[174] The one exception appears to apply to cases where website users do not explicitly consent to the scope of the interception. In *Campbell v. Facebook Inc*., 77 F.Supp.3d 836 (N.D. Cal. 2014), a Federal District

[165]Pursuant to 18 U.S.C. § 2510(1), a "'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce."

[166]"Oral communications" are typically intercepted through bugs or other recording and transmitting devices and consist of "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." See 18 U.S.C. § 2510(2).

[167]Pursuant to 18 U.S.C. § 2510(12), "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;
(B) any communication made through a tone-only paging device;
(C) any communication from a tracking device (as defined in section 3117 of this title); or
(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds."

[168]ECPA 1986, supra note 164.

[169]*Id.*

[170]*Id.*

[171]*Id.*

[172]See United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (holding that individuals retain no Fourth Amendment privacy interest in subscriber information and transactional records).

[173]ECPA 1986, *supra* note 164.

[174]Solove and Hartzog (2014), p. 178.

hoeren@uni-muenster.de

Court in California held that Facebook's notification to consumers that it might use information for data analysis was insufficient to allow the company to scan users' private messages to guide targeted advertising.[175]

4 Data Protection and Digital Forensics

4.1 Interception of Communication Data: Electronic Communications Privacy Act of 1986 (ECPA)[176]

Since the ECPA's original enactment, Congress has sought to keep pace with the rapid evolution of technology and the nation's security threats by clarifying and updating the ECPA. Some of these updates, most notably the USA Patriot Act, have eased restrictions on law enforcement's ability to access stored communications.[177] In some cases, courts have struck down Congress's attempts to liberalize privacy requirements. Most notably, in *Doe v. Ashcroft*, a federal district court held that Section 2709 of the Patriot Act violated the First Amendment as it permitted the FBI to use National Security Letters to obtain internet service providers' customer records without giving the ISP a vehicle to challenge the request.[178]

Unfortunately, despite the name of the Act, the ECPA allows the government to routinely request information collected by cell phone providers, search engines, social networking sites, and other websites every day with relative ease.[179] The Act consists of three parts. Title I, which applies to wire, oral, and electronic communications while in transit, affords the highest level of protections.[180] Title II or the Stored Communications Act (SCA), applies to communications stored by service providers and records about the subscriber such as the subscriber name, billing records and ISP addresses.[181] The privacy protections available under Title II are weaker than Title I protections as they allow state and federal prosecutors to obtain records without meeting the heightened protection standards of search warrants.[182]

---

[175] 77 F.Supp.3d 836, 848 (N.D. Cal. 2014).

[176] 18 U.S.C. §§2510–3127.

[177] The amendments include: Communications Assistance to Law Enforcement Act (CALEA) (1994), the USA Patriot Act (2001), the USA Patriot reauthorization acts (2006), and the FISA Amendments Act (2008).

[178] 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

[179] "Modernizing the Electronic Communications Privacy Act (ECPA)", ACLU, Available online at: https://www.aclu.org/feature/modernizing-electronic-communications-privacy-act-ecpa Last accessed on 13 August 2017.

[180] Title 1 includes "The Wiretap Act", 18 U.S.C. §§2510–2522.

[181] 18 U.S.C. §§2701–2711.

[182] "Electronic Communications Privacy Act", University of Cincinnati IT@UC Office of Information Security, Available online at: http://www.uc.edu/infosec/compliance/ecpa.html.

hoeren@uni-muenster.de

In addition to the ECPA's Title I, the Communications Assistance for Law Enforcement Act of 1994 (CALEA) also seeks to regulate the interception of electronic communications. This Act requires telecommunications carriers to redesign their network architectures to make it easier for the government to wiretap digital telephone calls.[183] In 2005, the Act was updated to include service providers (ISPs) and VoIP services. To comply with CALEA, communications providers must be "able to isolate all wire and electronic communications to and from any account targeted by law enforcement and identify the numbers or accounts with which the target has communicated".[184] While the legislation mandates that the carriers design their networks in a manner that protects "the privacy and security of communications and call-identifying information not authorized to be intercepted",[185] CALEA's critics argue that the Act, and its continuing expansion, is a massive infringement on user's rights.[186]

4.2 Preservation and Access to Computer Data Hosted on a Computer System

The Stored Communications Act sets forth the procedures that government actors must follow to obtain communications records and the content of electronic or wire communications. Pursuant to 18 U.S.C. §2703, the Act requires the government to obtain a court order or warrant to access customer data held by ISPs.[187] The SCA distinguishes between communications data stored for 180 days or less and data stored for longer than 180 days. In the case of the former, the government must obtain a warrant supported by probable cause to obtain the data. To obtain communications stored in excess of 180 days, the government need only provide prior notice to the subscriber and meet the standard mentioned above showing that there are "reasonable grounds" to believe that the communications are relevant to an ongoing criminal investigation. In the case in which the government elects not to provide prior notice to the subscriber, the government must obtain a warrant.

In addition, where a public electronic communication service (ECS) provider or a public remote computing service (RCS) provider inadvertently discovers information pertaining to the commission of a crime, the provider may disclose the information directly to the government in a situation where the provider believes in good

[183]"CALEA: The Communications Assistance for Law Enforcement Act (CALEA) of 1994", Electronic Frontier Foundation. Available online at: https://www.eff.org/issues/calea.

[184]Zetter (2014).

[185]47 U.S.C. § 1002(a)(4)(A).

[186]Zetter (2014).

[187]This includes customer data such as the name, address, length of service, and means of payment. See 18 U.S.C. §2703(c).

hoeren@uni-muenster.de

faith that an emergency "involving danger of death or serious physical injury to any person requires disclosure".

4.3 Pen Register and Trap and Trace Devices

Title III, which applies to the use of pen register and trap and trace devices that record dialing, routing, signaling, and signaling information used in the process of transmitting wire or electronic communications, requires law enforcement to secure an ex parte court order before installing a device to obtain that information.[188] To obtain a court order to install a pen register and trap and trace devices, the government must only demonstrate that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation".[189] Obviously, this standard offers a lowest level of privacy protection among all three titles of the ECPA.

Title III permits government officials to intercept the wire or electronic communications of individuals who "trespass" into protected computers if:

> (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer; (II) the person acting under color of law is lawfully engaged in an investigation; (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.[190]

Title III opens the door to criminal sanctions under three circumstances. First, pursuant to 18 U.S.C. 2511(1)(c), anyone who intentionally "discloses or endeavors to disclose to another person the contents of any wire, oral, or electronic communication having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication" may be punished. Second, it is a federal crime to disclose, "with an intent to obstruct criminal justice, any information derived from lawful police wiretapping or electronic eavesdropping".[191] Finally, the third proscription against disclosure applies to electronic communications service providers "who intentionally divulge the contents of the

[188] 18 U.S.C. §§3121–3127. "Electronic Communications Privacy Act", University of Cincinnati IT@UC Office of Information Security, Available online at: http://www.uc.edu/infosec/compliance/ecpa.html.

[189] 18 U.S.C. §3123(a)(1).

[190] 18 U.S.C. 2511(2)(i(I). Pursuant to 18 U.S.C. 2510(21), a computer trespasser is a person who: (A) "accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."

[191] Doyle (2012), p. 18.

hoeren@uni-muenster.de

communication while in transmission" to anyone other than sender and intended recipient.[192] Individuals or entities who violate these provisions may face criminal liability under the general disclosure proscription, 18 U.S.C. 2511(1)(c), and civil liability under 18 U.S.C. 2520.[193]

4.4 *Data Retention: Preservation of Digital Documents in the Litigation Context*

Lawyers and their clients have long had a legal duty to take reasonable steps to prevent the intentional or negligent destruction of evidence that might be used as evidence in future litigation.[194] Long before the dawn of the digital age and the creation of electronic evidence, American courts possessed the power to hold parties who were seen as interfering with the judicial process in contempt.[195] In the criminal law arena, prohibitions on the destruction of evidence have traditionally fallen under the rubric of obstruction of justice laws that generally prohibit any attempt to interfere with the administration of justice. Still, it was not until Congress passed the Sarbanes-Oxley Act, that there was a specific federal statute in place that prohibited the destruction of documents. Specifically, 18 U.S.C. § 1519, criminalizes any "knowing" destruction of documents with the intent to impede a "contemplated" investigation.[196] This prohibition against spoliation now extends to the preservation of electronic evidence.[197] Because violations of civil laws may sometimes lead to criminal prosecution, once a corporate client is on notice of a possible criminal investigation, they have a duty to preserve digital evidence.[198] Pursuant to 18 U.S. Code §1519, it is a crime to "knowingly alter, destroy, mutilate, conceal, cover up, falsify, in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter with administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under Title 11, or in relation to or contemplation of any such matter or case".[199] Although the language of the Act appears to be quite broad, in *United States v. Aguilar*, the U.S. Supreme Court held

[192] *Id.* at 19.

[193] *Id.*

[194] Gorelick et al. (1989), pp. 255–256.

[195] Stanger (2005), p. 13 citing United States v. Hudson, 11 U.S. (7 Cranch) 32, 34 (1812). Available online at: http://blj.ucdavis.edu/archives/vol-5-no-2/document-destruction-after-enron.html.

[196] 18 U.S.C. § 1519.

[197] Leahy and Gilchrist, 126 Am. Jur. Proof of Facts 3d 1, Sanctions for Spoliation of Electronic Evidence § 12, p. 13 (2012) (citing numerous cases).

[198] Young (2001).

[199] Pub. L. 107–204, title VIII, § 802(a), July 30, 2002, 116 Stat. 800).

hoeren@uni-muenster.de

that §1519 only applies to actions undertaken after a judicial proceeding has actually commenced.[200]

Section § 1512(b) of the Act seeks to punish those who command or induce others to destroy documents relevant to a proceeding.[201] To prove an offense under this section:

> [t]he government must prove that the defendant (1) knew or had notice of the likelihood of an "official proceeding"; (2) knowingly engaged in intimidation, threats, corrupt persuasion, or misleading conduct; (3) with the intent to cause or induce any person to alter or destroy documents relevant to the proceeding.[202]

Where the government holds digital evidence that exculpates the defendant, the government has an affirmative duty to disclose that information to the defense.[203] Defendants in some cases have unsuccessfully petitioned the court for a jury instruction, alleging that the government failed to preserve potential electronic evidence attempt to reverse a conviction or obtain a new trial.[204]

5 Data Protection and Electronic Surveillance for Security and Defense Purposes

Although the Fourth Amendment to the U.S. Constitution regulates the actions of law enforcement in criminal investigations, the Amendment's impact on foreign intelligence gathering is mediated by legislative instruments such as the Foreign Intelligence Surveillance Act (FISA).[205] FISA provisions govern when an investigation's significant purpose is to conduct foreign intelligence gathering.[206] The Act aims to empower law enforcement to monitor national security threats while maintaining the secrecy of those investigations.[207] While American courts have developed an extensive Fourth Amendment jurisprudence that seeks to balance privacy interests with law enforcement's interest in investigating crime, when national security interests are at stake, Congress has sought to balance those interests through FISA and subsequent legislation. Given the subsequent expansion of FISA's

[200] 515 U.S. 593, 598–599 (1995).

[201] Stanger (2005).

[202] *Id.*

[203] See, *e.g.*, *U.S. v. Wise*, 221 F.3d 140 (5th Cir. 2000).

[204] See, *e.g.*, *U.S. v. Wise*, 221 F.3d 140 (5th Cir. 2000).

[205] 50 U.S.C. §§ 1801–11, 1821–29, 1841–46, 1861–62, 1871.

[206] 50 U.S.C. § 1804(a)(6)(B) &§1823 (a)(6)(B).

[207] "Privacy & Civil Liberties: The Foreign Intelligence Surveillance Act of 1978", U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Information Sharing. Available online at: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286.

hoeren@uni-muenster.de

reach, it now seems ironic, that FISA was born in the aftermath of Church Committee's exposure of uncontrolled domestic spying by the FBI and the CIA.[208]

As amended, FISA sets forth a framework of standards and procedures for the government's use of electronic surveillance,[209] physical searches, business records, as well as pen registers and trap and trace devices.[210] FISA established a special court that consists of eleven federal district court judges. The court meets in secret and primarily conducts ex parte proceedings to review applications to authorize surveillance applications.[211] While the government must establish that probable cause exists that the party to be monitored is a "foreign power" or an "agent of a foreign power", the government need not show that the agent is engaged in criminal activity.[212] Government agents must also demonstrate that "a significant purpose" of the surveillance is to obtain "foreign intelligence information", and that appropriate "minimization procedures" are in place.[213] However, if the targeted individual is a U.S. citizen, the government must establish probable case that the individual's activities "may" or "are about to" involve a criminal violation.[214] Because the government is the only side represented in the majority of hearings before the court, critics have alleged that the court is a rubber stamp for the executive branch.[215]

In cases where the Attorney General certifies that there is "no substantial likelihood that the surveillance will acquire the contents of any communication to which a U.S. person is a party" and that the surveillance is directed solely at communications among or between foreign powers, or "the acquisition of technical intelligence . . . from property or premises under the open and exclusive control of a foreign power", the President may authorize electronic surveillance to acquire foreign intelligence information for periods of up to 1 year without a FISC court order.[216]

5.1 The USA Patriot Act

In the wake of the 9/11 attacks, the federal government's use of its FISA powers dramatically increased. Among the Act's provisions are a number which impacted or amended the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq. (FISA).

[208] Goitein and Patel (2015), p. 13.

[209] 50 U.S.C. § 1801(f)(2).

[210] Solove and Hartzog (2014), p. 86.

[211] *Id.*

[212] *Id.* citing 50 U.S.C. § 1801.

[213] 50 U.S.C. § 1804.

[214] Solove and Hartzog (2014), *citing* 50 U.S.C. § 1801(b)(2)(A)–(B).

[215] Perez (2013).

[216] "The Foreign Intelligence Surveillance Act of 1978 (FISA)", U.S. Dept. of Justice, Justice Information Sharing. Available online at: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286, citing 50 U.S.C. § 1802.

hoeren@uni-muenster.de

Most notably, Section 215 of the PATRIOT Act expanded the government's ability to obtain business records held by third parties. Before the 2001 Act, the FBI could petition the FISA Court to obtain an order to require third parties to turn over the business records of transport companies, hotels and motels, car and truck rental agencies, and storage rental facilities if the government certified that the records were sought for a foreign intelligence or international terrorism investigation being conducted by the FBI and that it had "specific and articulable facts giving reason to believe" that the subject of the records was a foreign power or agent of a foreign power.[217]

The Patriot Act's Section 215 amended Section 501 of the Foreign Intelligence Surveillance Act and greatly expanded the types of records the government could obtain while relaxing the requirement that the investigation be connected to a foreign power or its agent as long as the information did not concern U.S. persons. Critically, instead of obtaining individualized court orders, the government began obtaining FISA orders to permit the bulk collection of "telephony metadata" from telecommunications companies under the FISA pen register and trap and trace authority and the National Security Letter statutes.[218] Under provisions of several pieces of legislation, the FBI had right to demand that the relevant organizations produce telecommunications records,[219] financial records,[220] credit records,[221] as well as consumer reports[222] when that information was relevant to foreign intelligence gathering or for purposes of a terrorism investigation without a showing of probable cause.[223] In the years following the passage of the Patriot Act, the FBI's use of national security letters grew exponentially. For example, between 2003 and 2006, the Justice Department's Inspector General has reported that the FBI issued nearly 200,000 NSLs.[224] While the metadata collection program operated without much fanfare for years that changed when Edward Snowden blew the whistle on the program's existence in 2013.[225] One of the reasons why the program was able to operate under the radar for so long is that the law blocked anyone who had received an NSL from telling anyone about it for an indefinite period.[226] Two years after the Snowden disclosures Congress moved to prohibit the bulk collection of metadata by enacting the USA Freedom Act of 2015.[227]

[217] Goitein and Patel (2015), p. 21.

[218] Mann (2014).

[219] 18 U.S.C. §2709 [The Stored Communications Act].

[220] 12 U.S.C. §3414(a)(5)(A). [The Right to Financial Privacy Act of 1978].

[221] 15 U.S.C. §1681u. [The Fair Credit Reporting Act of 1970].

[222] *Id.*

[223] Solove and Hartzog (2014), p. 88.

[224] "National Security Letters", ACLU Website. Available online at: https://www.aclu.org/other/national-security-letters [hereinafter National Security Letters].

[225] Lynch and Flint (2017).

[226] "National Security Letters", *supra* note 224.

[227] H.R. 2048, Pub.L. 114–23.

hoeren@uni-muenster.de

5.2 *USA Freedom Act of 2015*

The USA Freedom Act banned NSA's bulk collection of U.S. call metadata and telephonic records previously permitted under Section 215 of the Patriot Act.[228] Instead of permitting the government's bulk collection of data, the Act requires that government applications for call records be based on a "specific selection term" (SST) that "specifically identifies a person, account, address, or personal device" in a way that "limit[s], to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things".[229] Notably, the Act removed the presumption of relevance for the production of information and precluded the production for mere threat assessments.[230]

In order to apply for records based on the first hop of a specific selection term, the government must have:

> (1)'reasonable grounds to believe that the call detail records sought to be produced based on [a] specific selection term . . . are relevant to [an authorized] investigation,' and (2) 'a reasonable, articulable suspicion' that the selection term is 'associated with a foreign power engaged in international terrorism or activities in preparation there for, or an agent of a foreign power engaged in international terrorism or activities in preparation there for.'[231]

Other provisions in the Act include minimization requirements on the use of technology by prohibiting the retention of information not pertaining to the target of the search.[232] The Act mandates the "the prompt destruction of all call detail records" determined not to be "foreign intelligence information".[233] In addition, the Act grants FISA court judges the authority to "impose additional, particularized minimization procedures" with respect to any "non publicly available information concerning unconsenting United States person[s]".[234] Finally, the Act also attempts to take steps to increase the transparency of government surveillance by requiring annual publication of the number of orders sought and granted as well as the number of U.S. persons who were targeted.[235]

[228] Solove and Hartzog (2014), p. 87.

[229] Liu (2015).

[230] H.R. 3361 § 101 (amending 50 U.S.C. § 1861(b)).

[231] *Id.*

[232] "USA Freedom Act Reinstates Expired USA PATRIOT Act Provisions but Limits Bulk Collection", CRS Legal Sidebar, 4 June 2015. Available online at: https://fas.org/sgp/crs/intel/usaf-rein.pdf.

[233] *Id.*

[234] *Id.*

[235] Ombres (2015), pp. 27–58 at 43–44.

hoeren@uni-muenster.de

5.3 *Forced Assistance to the Government to Bypass Password Security*

One interesting issue regarding password security is whether private companies like Apple must assist the government in bypassing a mobile phone's security system. Two recent cases electronic communications privacy cases involve the government's attempt to force Apple, Inc. to help investigators to bypass the iPhone's passcode security. In the first case, *In re Apple, Inc.,* a Federal District Court denied the government's request for a Court order that would have forced Apple to bypass the phone's password security. In that case, the government was trying to obtain data from a cellphone seized in a search related to a drug investigation.[236] The second case, *In Re the Search of an Apple iPhone*, the government sought to force Apple to disable the phone's encryption feature that automatically erases data on the phone after a user enters an incorrect password ten consecutive times.[237] This case received substantial publicity because the iPhone belonged to Syed Farook, a domestic terrorist who conspired with his wife to kill fourteen individuals at a government facility in San Bernardino, California in December 2015.[238] Although the Federal Magistrate Judge initially granted the government's ex parte request, Apple then filed a motion to vacate the order and oppose the government's motion to compel assistance.[239] Apple argued that creating a backdoor to devices like the iPhone would make the device vulnerable to breaches by other actors.[240] While Apple fought the court's order, the Justice Department hired a third party who successfully broke into the phone rendering the issue moot.[241]

6 Remedies and Sanctions

Because the United States lacks an overriding data protection law, the potential remedies and sanctions available are located within the sector-specific legislation described above. The primary enforcement agency is the Federal Trade Commission

[236] 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

[237] In Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, (2016 WL 618401) (2016 U.S. Dist. LEXIS 20543) (C.D. Cal. Feb. 16, 2016).

[238] "Everything We Know So Far About the San Bernardino Shooting", Los Angeles Times, 14 December 2015. Available online at: http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html.

[239] Apple Inc.'s Mot. to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance entered February 25, 2016, Case No. 5:16-cm-00010-SP.

[240] *Id.*

[241] Kang (2016).

hoeren@uni-muenster.de

which is empowered to bring enforcement actions under Section 5 of the FTC Act targeting unfair[242] or deceptive[243] data processing practices. In addition to the FTC, the Consumer Financial Protection Bureau, the Department of Health and Human Services ("HHS") and the 50 state Attorneys General all possess various levels of enforcement responsibility.

6.1 Gramm-Leach-Bliley Act

Penalties for violations under the *Gramm-Leach-Bliley Act* ("GLBA"),[244] vary depending upon the specific authority of the agency that brings the enforcement action. For example, if the Federal Trade Commission brings the action pursuant to Section 5(l) of the FTC Act, the penalties may run up to $40,000 per offense.[245] The FTC Act does not create a private cause of action. Nor can the FTC impose fines for violations of Section 5. Instead the Act authorizes injunctive remedies and issue fines for violations of Section 5 consent decrees.[246] The Federal Consumer Financial Protection Bureau ("CFPB") can bring administrative adjudication enforcement actions or actions in federal district court against individuals or entities that violate federal consumer financial laws pursuant to the provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

In a new development, the CFPB has begun to use its authority to regulate unfair, deceptive, or abusive acts or practices to bring data security related enforcement actions even in cases where consumers have not experienced a discernable harm.[247] In a recent case, the CFPB entered into a consent decree with Dwolla, Inc. ("Dwolla"), an online payment platform, for alleged misrepresentations regarding Dwolla's data security practices.[248] According to the CFPB, Dwolla, which collects and stores consumers' sensitive personal information and provides a platform for

[242]An act or practice is unfair where it (1) causes or is likely to cause substantial injury to consumers, (2) cannot be reasonably avoided by consumers; and (3) is not outweighed by countervailing benefits to consumers or to competition. See "Consumer Compliance Handbook: Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices", Federal Reserve Supervisor's Handbook, at 7. Available online at: https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

[243]"A representation, omission, or practice is deceptive if it is likely to mislead a consumer acting reasonably under the circumstances and is likely to affect a consumer's conduct or decision regarding a product or service" *Id.* at 7.

[244]Title V, 15 U.S.C. §§6801–6809.

[245]Fair (2016). The Federal Trade Commission ("FTC") may bring an administrative hearing against an individual or entity, suspected of unfair or deceptive trade practices and subsequently issue an order to cease and desist. If the individual or entity subject to the order violates that order, the FTC may impose an administrative fine.

[246]Solove and Hartzog (2014), p. 159.

[247]*Id.*

[248]Tosi et al. (2016).

hoeren@uni-muenster.de

financial transactions, falsely claimed that its data security practices "exceeded" or "surpassed" industry security standards as well as falsely claimed that its information was securely encrypted and stored.[249] Under the terms of the consent decree, Dwolla must (1) pay a $100,000 civil penalty to CFPB's Civil Penalty Fund, (2) stop misrepresenting its data security practices, and (3) train its' employees properly and fix any security weaknesses found in its web and mobile applications.[250]

In the realm of criminal actions, individuals who violate the GLBA by fraudulently obtaining financial information belonging to another person may face up to a 5 year term of imprisonment.[251] If the individual is convicted of this offense while violating another U.S. law or as a pattern of illegal activity involving more than $100,000 per year, may also face criminal penalties of up to 10 years in prison and fines of up to $500,000 (individual) or $1,000,000 (company).[252]

6.2 *Federal Trade Commission Act & Enforcement Authority*

In addition to actions brought under the Gramm-Leach-Bliley Act, the FTC may bring a broad range of actions under Section 5(a) of the FTC Act to protect consumers' privacy and personal information. The Federal Trade Commission has the authority to bring claims under the Federal Trade Commission Act (FTC), 15 U.S.C.A. § 45(a), in the data-breach context.[253] At first glance, it may seem like a stretch to fit claims related to data breaches and safety under the FTC's broad mandate to protect consumers against unfair trade practices. However, in *F.T.C. v. Wyndham Worldwide Corp.*,[254] Third Circuit Court of Appeals upheld a lower court decision which held that the FTC possessed power to regulate data security practices under the unfairness prong of 15 U.S.C. § 45(a).[255] Notably, the Third Circuit rejected Wyndham's argument that subsequent Congressional legislation, including legislation such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act could be read to exclude cyber security from the FTC's authority.[256] The FTC may also obtain civil monetary

[249]"CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices", Consumer Financial Protection Bureau, 2 March 2016. Available online at: https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[250]In the Matter of Dwolla, Inc. Consent Order, United States of America Consumer Financial Protection Bureau, Administrative Proceeding File No. 2016-CFPB-0007, 03/02/2016. Available online at: http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.

[251]15 USC §6823(A).

[252]15 USC §6823(B).

[253]Surette n.d..

[254]799 F.3d 236, 2015 U.S. App. LEXIS 14839 (3rd Cir. 2015).

[255]799 F.3d At 245–46.

[256]799 F.3d At 247.

hoeren@uni-muenster.de

penalties for violations of the Children's Online Privacy Protection Act,[257] the Fair Credit Reporting Act,[258] and the Telemarketing Sales Rule.[259]

If the FTC believes that a person or company has violated the law, the agency's first step is often to obtain voluntary compliance by entering into a consent order with the company.[260] A company that signs a consent order needs not liability, but it must agree to stop the disputed practices, consent to the entry of a final order, and waive its rights to a judicial review.[261] Before an order is made final, the FTC will place an order on the record for 30 days of public comment.[262] Through its administrative powers, the FTC may require companies to implement comprehensive privacy and security programs, submit to biennial assessments by independent experts, provide monetary redress to consumers, return ill-gotten gains, delete illegally obtained consumer information, and implement robust transparency and choice mechanisms to consumers.[263]

In the absence of a consent order, the FTC may initiate an administrative complaint. Respondents may appeal decisions made by an administrative law judge to the Commission. A Commission's decision may be appealed to a U.S. Court of Appeals and ultimately to the Supreme Court. As an alternative to seeking administrative relief, the FTC may seek injunctive relief in the federal courts.[264] In addition, if the company violates an FTC order, the Commission also may seek civil penalties or an injunction.[265]

6.3 HIPPA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorizes the U.S. Department of Health and Human Services (HHS) to impose civil penalties on any person who violates the HIPAA Privacy Standards, at an amount of

[257] 15 USC § 6501 et. seq. COPPA also gives states and certain other federal agencies authority to enforce compliance. Because COPAA violations are considered to be unfair or deceptive trade practices and are therefore subject to the same administrative penalties as set forth under the FTC Act.

[258] 15 U.S.C. §1681.

[259] 16 U.S.C. §310.

[260] "The Enforcers", Federal Trade Commission Website. Available online at: https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/enforcers.

[261] "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority", Federal Trade Commission Website (July 2008). Available online at: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority#N_1_ [hereinafter "A Brief Overview"].

[262] *Id.*

[263] "Privacy & Data Security Update (2016)", FTC Website. Available online at: https://www.ftc.gov/reports/privacy-data-security-update-2016.

[264] 15 U.S.C. § 53(b).

[265] A Brief Overview, *supra* note 261.

hoeren@uni-muenster.de

between US$100 to 50,000 per violation, with a total of $25,000 to 1.5 million for all violations of a single requirement in one calendar year of up to $1.5 million on covered entities (CEs)[266] that are found to have violated HIPAA Rules.[267]

Like most U.S. data protection legislation, HIPAA is domain-specific. The rules protect "individually identifiable health information" held by health care entities.[268] Because HIPAA targets health care entities and a narrow class of businesses that contract with health care entities, rather than all individuals and businesses that handle health care data, "most healthcare data controlled or processed by those outside the traditional health care environment will not be subject to HIPPA rules".[269]

The penalties levied against HIPPA violators are based on the level of negligence involved. While the Office of Civil Rights (OCS) within HHS investigates civil infractions, the Department of Justice is responsible for pursuing criminal actions under the Act. Criminal penalties may range from a fine of up to $50,000 and imprisonment up to 1 year for entities and individuals who "knowingly" obtain or disclose individually identifiable health information.[270] At the top end of the punishment spectrum are offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm-convictions under those provisions may result in fines of up to $250,000 and imprisonment up to 10 years.[271]

6.4 Consumer Civil Litigation

Consumers who have been victims of data breach often find it difficult to bring civil claims in federal court in cases where they cannot identify any actual harm caused by the misappropriation and purported misuse of data.[272] In several recent data security breach class action cases, courts have held that the plaintiffs have failed to allege an actual, cognizable harm arising from a data security breach.[273] This harm is required to establish legal standing under U.S. Const. Article III to bring a lawsuit in federal court.[274]

[266]CEs include healthcare providers, health plans, healthcare clearinghouses and all other CEs—including Business Associates (BAs) of CEs.

[267]42 U.S. Code § 1320d–5.

[268]Terry (2017), p. 22.

[269]*Id.*

[270]Section 13410(D) of the HITECH Act.

[271]42 U.S.C. § 1320d-6.

[272]Tosi et al. (2016).

[273]See, *e.g.*, Whalen v. Michael Stores Inc., --- F. Supp. 3d ---, 2017 U.S. App. Lexis 7717; In re Zappos.com, Inc., 108 F. Supp. 3d 949 (D. Nev. 2016); and Schwartz v. HSBC Bank USA, N.A., --- F. Supp. 3d --, U.S. Dist. Lexis 94019 (2017).

[274]Tosi et al. (2016).

hoeren@uni-muenster.de

6.5 Other Criminal Enforcement Provisions

There are a number of other federal statutes, the violation of which may trigger criminal penalties. The most well-known statutes are summarized below:

Name	Code sections	Actions targeted	Criminal penalty
CAN-SPAM Act	15 U.S.C. §§7703–7704	(1) knowingly accessing a protected computer[275] (2) using a protected computer to transmit commercial e-mails with the intent to deceive or mislead recipients about their origin[276] (3) falsifying header information[277] (4) registering 5 or more email accounts or 2 or more domain names using false identity information and sending commercial email there from[278] (5) falsely representing oneself as being as being the legitimate registrant of 5 of more internet addresses and sending multiple commercial emails there from[279]	Punishable by fines and prison terms from one to 5 years incarceration and confiscation of any real or personal property purchased through spam earnings. The criminal penalties may be increased if the crime is perpetuated by fraudulent activity[280]
Computer Fraud and Abuse Act (CFFA)	18 U.S.C. §1030(C)	(1) computer trespassing a government computer[281] (2) computer trespassing resulting in exposure of governmental, credit, financial, or computer-housed	Penalties range from imprisonment for not more than a year for simple cyberspace trespassing to a maximum of life imprisonment when death results

(continued)

[275] 18 U.S.C. § 1037(a)(1).
[276] 18 U.S.C. § 1037(a)(2).
[277] 18 U.S.C. § 1037(a)(3).
[278] 18 U.S.C. § 1037(a)(4).
[279] 18 U.S.C. § 1037(a)(5).
[280] 18 U.S.C. § 1037.
[281] 18 U.S.C. 1030(a)(3).

hoeren@uni-muenster.de

Name	Code sections	Actions targeted	Criminal penalty
		information[282] (3) damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce[283] (4) committing fraud an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce[284] (5) threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce[285] (6) trafficking in passwords for a government computer, or when the trafficking affects interstate or foreign commerce[286] (7) accessing a computer to commit espionage[287]	from intentional computer damage[288]

(continued)

[282] 18 U.S.C. 1030(a)(2).
[283] 18 U.S.C. 1030(a)(5).
[284] 18 U.S.C. 1030(a)(4).
[285] 18 U.S.C. 1030(a)(7).
[286] 18 U.S.C. 1030(a)(6).
[287] 18 U.S.C. 1030(a)(1).
[288] Doyle (2014).

hoeren@uni-muenster.de

Name	Code sections	Actions targeted	Criminal penalty
Fair Credit Reporting Act	15 U.S.C. §1681q	Knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses[289]	Fined under title 18, imprisoned for not more than 2 years, or both[290]
Foreign Intelligence Surveillance Act	50 U.S.C. §1809	Officers or employees of the U.S. who (1) engage in unauthorized electronic surveillance under color of law; or (2) use or disclose information obtained under color of law through unauthorized electronic surveillance	A fine of not more than $10,000 or imprisonment for not more than 5 years, or both[291]
	50 U.S.C. §1827	Intentionally— (1) under color of law for the purpose of obtaining foreign intelligence information, executes a physical search within the United States except as authorized by statute; or (2) discloses or uses information obtained under color of law by physical search within the United States, knowing or having reason to know that the information was obtained through physical search not authorized by statute, for the purpose of obtaining intelligence information[292]	Punishable by a fine of not more than $10,000 or imprisonment for not more than 5 years, or both[293]

(continued)

[289] 15 U.S.C. §1681q.
[290] *Id.*
[291] 50 U.S.C. §1809(c).
[292] 50 U.S.C. §1827 (a).
[293] 50 U.S.C. §1827(c).

hoeren@uni-muenster.de

Name	Code sections	Actions targeted	Criminal penalty
Gramm-Leach-Bliley Act	15 U.S.C. §6821	Obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, customer information of a financial institution relating to another person— (1) by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution; (2) by making a false, fictitious, or fraudulent statement or representation to a customer of a financial institution; or (3) by providing any document to an officer, employee, or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation[294]	Fined in accordance with title 18 or imprisoned for not more than 5 years, or both[295] Whoever violates, or attempts to violate, section 6821 of this title while violating another law of the U.S. or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period shall be fined twice the amount provided in subsection (b)(3) or (c)(3) (as the case may be) of section 3571 of title 18, imprisoned for not more than 10 years, or both[296]
Pen Register Act	18 U.S.C. §3121	Knowingly install or use a pen register or a trap and trace device without first obtaining a court order[297]	A fine as provided by Title 18 and imprisonment of not more than 1 year[298]

(continued)

[294] 15 U.S.C. §6821(a).
[295] 15 U.S.C. §6823(a).
[296] 15 U.S.C. §6823(b).
[297] 18 U.S.C. §3121(a).
[298] 18 U.S.C. §3121(d).

hoeren@uni-muenster.de

Name	Code sections	Actions targeted	Criminal penalty
Privacy Act	5 U.S.C. §552a(i)	(1) Knowingly and willfully disclosing individually identifiable information which is prohibited from such disclosure by the Act or by agency regulations; or willfully maintaining a system of records without having published a notice in the Federal Register of the existence of that system of records (2) knowingly and willfully requesting or gaining access to a record about an individual under false pretenses[299]	Fines of up to $5000[300]
Stored Communications Act (SCA)	18 U.S.C. §2701	(1) intentionally accesses without authorization a facility through which an electronic communication service is provided[301]; (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system[302]	If the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State— (A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and (B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and (2) in any other case— (A) a fine under this title

(continued)

[299] 5 U.S.C. Sec. 552a(i).

[300] 5 U.S.C. §552a(i).

[301] 18 U.S.C. §2701(a)(1).

[302] 18 U.S.C. §2701(a)(2).

hoeren@uni-muenster.de

Name	Code sections	Actions targeted	Criminal penalty
			or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section[303]

7 Private International Law Rules

7.1 U.S. Legislation

Consistent with the U.S. national commitment to free and fair trade, the U.S. does not have many specific rules that govern the transfer of data outside of the county, beyond the "basic fair information principles for notice and prohibitions on deceptive or unfair business practices".[304] Nor does the United States have any forced localization requirements for data servers with the exception of the data used by certain government agencies.[305] As one example, in 2016, the Internal Revenue Service (IRS) issued security guidelines that require federal agencies to "restrict the location of information systems that receive, process, store, or transmit [federal tax information] to areas within the United States territories, embassies, or military installations".

Foreign organizations that operate in the United States are considered responsible parties under U.S. law provided that the organization satisfies American jurisdictional requirements. Foreign organizations may be subject to sector-specific laws, such as those enforced by the FTC and the Department of Health and Human Services.

The Safe Web Act[306] amended the jurisdiction of the FTC under Section 5(a) of the FTC Act to regulate "unfair or deceptive acts or practices" to include "such acts

[303] 18 U.S.C. §2701(b).

[304] Brown et al. (2017).

[305] Raul et al. (2014), p. 286.

[306] Pub. L. No. 109–455, 120 Stat. 3372, extended by Pub. L. No. 112–203, 126 Stat. 1484, codified at 15 U.S.C. §§ 41 *et seq*.

hoeren@uni-muenster.de

or practices involving foreign commerce that—"(i) cause or are likely to cause reasonably foreseeable injury within the United States"; or "(ii) involve material conduct occurring within the United States".[307] Thus, if a foreign organization engages in interstate commerce in the U.S., the FTC has jurisdiction.

The FTC and other U.S. regulators maintain that applicable U.S. laws and regulations still apply to the data after it leaves the US.[308] In particular, regulated entities remain liable for: "[d]ata exported out of the US, [t]he processing of data overseas by subcontractors, and [s]ubcontractors using the same protections (such as through the use of security safeguards, protocols, audits and contractual provisions) for the regulated data when it leaves the country".[309] In addition, the Department of Defense requires require all cloud-computing service providers that work for the department to store data domestically.[310] Under the Gramm-Bliley-Leach Act, a financial institution must disclose its privacy notice and provide the individual with the opportunity to opt out of certain non-affiliated third party sharing (whether the transfer is within or outside of the US).[311]

7.2 International Agreements

In 2016, the U.S. Department of Commerce, the European Commission, and the Swiss Administration adopted the "Privacy Shield" framework with the goal of strengthening enforceable rights regarding data transfers.[312] The goal of the Framework is to provide companies "with a mechanism to comply with data protection requirements when transferring personal data".[313] Pursuant to the Framework, organizations based in the U.S. must self-certify to the Department of Commerce and commit to comply with the Framework's requirements.[314] Those requirements include: data handling requirements, clear safeguards and transparency obligations on U.S. government access, effective protection of individual rights, and an annual joint review mechanism.[315] In addition, pursuant to the Judicial Redress Act citizens

[307] *Id.* at §3.

[308] Jolly (2016).

[309] *Id.*

[310] "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)" (Washington, DC: Defense Acquisition Regulations System, Department of Defense, August 26, 2015), https://www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reporting-and-contracting-for.

[311] Jolly (2016), p. 22.

[312] Jolly (2016), p. 22.

[313] "Privacy Shield Framework", U.S. Department of Commerce—International Trade Administration. Available online at: https://www.privacyshield.gov/Program-Overview.

[314] *Id.*

[315] *Id.*

hoeren@uni-muenster.de

of EU member states may bring civil actions under the Privacy Act against U.S. government agencies for unlawful disclosure of their personal records.[316]

8 Conclusion

Europe has adopted a broad approach data privacy rights, granting citizens strong privacy rights that sharply regulate corporate use of consumers' personal information. In many parts of Europe, privacy intrusions that Americans have come to take for granted are prohibited.[317] While European states rely on data protection agencies to monitor corporate behavior, the primary U.S. regulatory authority, the F.T.C., primarily relies on consent decrees and self-regulatory instruments to shape corporate behavior. This difference in part reflects a divergence in citizens' sources of distrust. As Bob Sullivan notes, "Europeans reserve their deepest distrust for corporations, while Americans are far more concerned about their government invading their privacy".[318] Reflecting Americans' distrust of governmental authority, Americans are far more concerned with limiting the government's attempts to invade individual privacy.

References

Braverman B (2013) Fear FACTA: beware the truncation requirement of the Fair and Accurate Credit Transactions Act. http://www.dwt.com/Fear-FACTA-Beware-the-Truncation-Requirement-of-the-Fair-and-Accurate-Credit-Transactions-Act-12-04-2013

Brennan W (2016) Complying with the CAN-SPAM Act. Lexis Pract Advis J. https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2016/11/08/complying-with-the-can-spam-act.aspx. Last accessed 18 July 2017

Brill J (2012) Privacy, consumer protection, and competition. Loyola University Chicago School of Law. www.ftc.gov/speeches/brill/120427loyolasymposium.pdf

Brown CT, Raul AC, Spencer AL, McNicholas ER (2017) Collection, storage and transfer of data in the United States. Lexology. https://www.lexology.com/library/detail.aspx?g=44b4db4a-6111-48a1-badf-87f8e2a73e67

[316] *Id.*

[317] For example, "[p]ersonal information cannot be collected without consumers' permission, and they have the right to review the data and correct inaccuracies; [c]ompanies that process data must register their activities with the government; [e]mployers cannot read workers' private e-mail;[and] personal information cannot be shared by companies or across borders without express permission from the data subject." See Bob Sullivan, "La difference is Stark in E.U., U.S. Privacy Laws", NBCNEWS.COM, 19 October 2006. Available online at: http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.WanIt7pFy00.

[318] *Id.*

hoeren@uni-muenster.de

Caragozian JS, Warner DE Jr (2000) Privacy rights of employees using workplace computers in California. Privacy Rights Clearinghouse. https://www.privacyrights.org/blog/privacy-rights-employees-using-workplace-computers-california
Castro D (2011) Benefits and limitations of industry self-regulation for online behavioral advertising. The Information Technology & Innovation Foundation. http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf
Caterine MJ (2009) Privacy of electronic communications. American Bar Association. https://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2009/2009_err_008.authcheckdam.pdf
Cobb S (2016) Data Privacy and Data Protection: U.S. Law and Legislation, ESET. https://www.welivesecurity.com/wp-content/uploads/2016/04/US-data-privacy-legislation-white-paper.pdf
Crane C (2012) Social networking v. the employment-at-will doctrine: a potential defense for employees fired for Facebooking, terminated for Twittering, booted for blogging, and sacked for social networking. Wash Univ Law Rev 89:639
Doyle C (2012) Privacy: an overview of the Electronic Communications Privacy Act. Congressional Research Service, p i. https://www.hsdl.org/?view&did=725508
Doyle C (2014) Cybercrime: an overview of the federal computer fraud and abuse statute and related federal criminal laws. Congressional Research Service, "Summary". https://fas.org/sgp/crs/misc/97-1025.pdf
Eisenhauer MP (2007) Managing your data processors: legal requirements and practical solutions. BNAI's World Data Protection Report. http://www.privacystudio.com/Links%20posted%20to%20web/BNAI%20-%20Managing%20Data%20Processors%20Aug%2007.pdf
Fair A (2016) Civil penalties undergo inflation recalculation. Federal Trade Commission. https://www.ftc.gov/news-events/blogs/business-blog/2016/06/civil-penalties-undergo-inflation-recalculation
Goitein E, Patel F (2015) What went wrong with the FISA Court. Brennan Center for Justice 13. https://www.scribd.com/document/259083922/What-Went-Wrong-With-the-FISA-Court
Gorelick JS, Marzen S, Solum LB (1989) Destruction of evidence. Aspen Law and Business, Aspen, Co. 255
Grosdidier P (2013) Choose your friends — and privacy settings — wisely. LAW 360. https://www.law360.com/articles/477202/choose-your-friends-and-privacy-settings-wisely
Hamilton MD (2016) Social media privacy issues in workplace investigations. LAW 360. https://www.law360.com/articles/812907/social-media-privacy-issues-in-workplace-investigations
Jolly I (2016) Data protection in the United States: overview. Thompson Reuters Practical Law. https://content.next.westlaw.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&__lrTS=20170522004900131&firstPage=true&bhcp=1
Kang YP (2016) DOJ Hacks Shooter's iPhone, Drops Apple Suit. Law 360. http://www.law360.com/articles/777150
Lazarus D (2016) Column: FTC is falling short in protecting consumers' data used by big business. Los Angeles Times. http://www.latimes.com/business/la-fi-lazarus-20160112-column.html
Listokin S (2017) Does industry self-regulation of consumer data privacy work? IEEE Security & Privacy, 92
Litwin S (2006) Employees' right to privacy in the workplace. Massachusetts Continuing Education Program. http://www.kcslegal.com/assets/MCLE_Right_to_Privacy_Article_Dec_2006.pdf
Liu J (2015) So what does the USA Freedom Act do anyway? Lawfare. https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway
Lynch C, Flint L (2017) The USA Freedom Act turns two. Lawfare. https://www.lawfareblog.com/usa-freedom-act-turns-two
Mann SF (2014) Fact sheet: Section 215 of the USA PATRIOT Act. Center for Strategic and International Studies. https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act
McGeveran W (2016) Friending the privacy regulators. Ariz Law Rev 58:959, 961
McGinnis K (2014) The ever expanding scope of employee privacy protections. Moore & Van Allen Blog. http://www.mvalaw.com/news-publications-373.html

hoeren@uni-muenster.de

Ombres D (2015) NSA domestic surveillance from the Patriot Act to the Freedom Act: the underlying history, constitutional basis, and the efforts at reform. Seton Hall Leg J 39(1):27–58
Perez E (2013) Secret court's oversight gets scrutiny. Wall Street Journal. http://online.wsj.com/news/articles/SB10001424127887324904004578535670310514616
Raul CA, Manoranjan TD, Mohan V (2014) United States. In: Raul AC (ed) The privacy, data protection, and cybersecurity law review. Law Business Research Ltd, London, p 268
Rich J (2015) Beyond cookies: privacy lessons for online advertising. AdExchanger Industry Preview. https://www.ftc.gov/public-statements/2015/01/beyond-cookies-privacy-lessons-online-advertising-adexchanger-industry
Saikali A (2012) Federal data breach notification laws. Data Security Law Journal. http://www.datasecuritylawjournal.com/2012/05/06/federal-data-breach-notification-laws/
Singer N (2013) Data protection laws, an ocean apart. New York Times. http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html?mcubz=0
Solove DJ, Hartzog W (2014) The FTC and the new common law of privacy. Columbia Law Rev 114:583
Sotto LJ, Simpson AP (2014) United States. In: Jay RP (ed) Data protection & privacy in 26 jurisdictions worldwide, 2nd edn. Gideon Roberton 191. https://www.hunton.com/files/Publication/1f767bed-fe08-42bf-94e0-0bd03bf8b74b/Presentation/PublicationAttachment/b167028d-1065-4899-87a9-125700da0133/United_States_GTDT_Data_Protection_and_Privacy_2014.pdfMark
Stanger AJ (2005) Document destruction after Enron: interpreting the New Sarbanes-Oxley Obstruction Statutes. U.C. Davis Bus Law J 5:13. http://blj.ucdavis.edu/archives/vol-5-no-2/document-destruction-after-enron.html
Stevens G (2010) Federal Information Security and Data Breach Notification Laws, Congressional Research Service. https://fas.org/sgp/crs/secrecy/RL34120.pdf
Surette EC. Liability of business to governments and consumers for breach of data security for consumers information. 1 A.L.R. 7th 2
Swire PP, Ahmad K (2012) Foundations of information privacy and data protection. International Association of Privacy Professionals, Portsmouth, p 4
Swire P, Kennedy-Mayo D (2017) How both the EU and the U.S. are "Stricter than Each Other for the Privacy of Government Requests for Information". Emory Law J 55:617
Terry N (2017) Existential challenges for health care data protection in the United States. Ethics Med Public Health 3:19
Toner A (2017) With new browser tech. Apple preserves privacy and Google preserves trackers. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2017/06/with-new-browser-tech-apple-preserves-privacy-google-preserves-trackers
Tosi RM, Bishop LS, Allensworth RB (2016) Proactive protection of consumers or premature penalty? Consumer Financial Protection Bureau bucks the trend in data security breach cases. K&L Gates Blog. http://www.klgates.com/proactive-protection-of-consumers-or-premature-penalty%2D%2D-consumer-financial-protection-bureau-bucks-the-trend-in-data-security-breach-cases
Ware WH (1973) Records, computers, and the rights of citizens. RAND. https://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf
Young DR (2001) Advising the corporate client on the duty to preserve electronic evidence. Farella Braun. http://www.fbm.com/files/Publication/523409e0-08a9-4ca6-8699-7ac3fa6b9e29/Presentation/PublicationAttachment/64095eae-b207-4ace-963c-7adb25385948/E4C58E30-9D15-4950-9AC8-30CCB4BE9A72_document.pdf
Zetter K (2014) The Feds cut a deal with in-flight Wi-Fi providers and privacy groups are worried. WIRED. https://www.wired.com/2014/04/gogo-collaboration-feds

hoeren@uni-muenster.de

Data Protection in the Internet: A European Union Perspective

Pedro A. de Miguel Asensio

1 General Data Protection Framework

1.1 Regulation (EU) 2016/679

The general framework on Data Protection in the EU is established in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR).[1] Pursuant to Article 99, the Regulation shall apply from 25 May 2018, and Directive 95/46/EC is repealed with effect from the same date. The GDPR shares the main objectives and principles of Directive 95/46/EC[2] but establishes a more detailed set of rules which are directly applicable in all Member States to prevent fragmentation in the implementation of data protection across the Union and to ensure a uniform high level of protection in all Member States. In contrast with the mere harmonization of national laws under Directive 95/46/EC, the GDPR establishes a one single set of rules for the Union.

This chapter has been made in the framework of research project DER-2015-64063-P (MINECO-FEDER).

[1] OJ L 119, 4.5.2016, p. 1. For an initial general overview of the GDPR, see De Hert and Papakonstantinou (2016), Härting (2016), Paal and Pauly (2017), and Albrecht and Jotzo (2017).

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

P. A. de Miguel Asensio (✉)
Complutense University of Madrid, Madrid, Spain
e-mail: pdmigue@der.ucm.es

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_18

hoeren@uni-muenster.de

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system [art. 2(1)].[3] The GDPR does not apply to personal data of deceased persons are not governed by the GDPR. Moreover, the GDPR does not cover the processing of personal data which concerns legal persons, such as undertakings established as legal persons. However, the fact that information concerning natural persons is provided as part of a professional activity does not mean that it cannot be characterised as personal data.[4]

The GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity [art. (2)(2)(c)]. This exception covers only activities that are carried out in the context of the private or family life of individuals. The CJEU has held that such an exception does not relate to the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.[5] Moreover, the CJEU has ruled that door-to-door preaching by members of a religious community is not a purely personal or household activity because the preaching extends beyond the private sphere of a member of a religious community who is a preacher.[6]

The GDPR does not apply to the processing of personal data in the course of activities which fall outside the scope of Union law, such as activities concerning national security, or to the processing of personal data by competent authorities for the purposes of the prevention or prosecution of criminal offences (see this chapter, Sect. 3.4, infra). The GDPR does not apply to matters concerning the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations (see this chapter, Sect. 3, infra). Moreover, the processing of personal data by the Union institutions is governed by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000.[7] This Regulation contains measures with regard to the processing of personal data by the Union institutions and the free movement of such data. It is based on the same principles that the general framework on data protection in EU law.

The Court of Justice of the European Union (CJEU) has developed a significant body of case law regarding the interpretation of the EU instruments in the field of

[3]The free movement of personal data within the EU granted by GDPR is intended to be complemented by a new Regulation on a framework for the free flow of non-personal, see the Proposal of 13 September 2017 by the Commission at COM(2017) 495 final.

[4]See Judgments of the CJEU of 16 July 2015, *ClientEarth and PAN Europe v. EFSA*, C-615/13 P, EU:C:2015:489, para. 30; and of 9 March 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, ECLI:EU:C:2017:197, para. 34.

[5]Judgment of the CJEU of 6 November 2003, Bodil Lindqvist, C-101/01, ECLI:EU:C:2003:596, para. 47.

[6]Judgment of the CJEU of 10 July 2018, Jehovan todistajat, C-25/17, ECLI:EU:C:2018:551, para. 50.

[7]OJ L 8, 12.1.2001, p. 1.

hoeren@uni-muenster.de

data protection law, founded on the basic idea that the general framework on Data Protection in EU Law seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data.[8]

Furthermore, an independent European advisory body on data protection and privacy, composed of a representative of the supervisory authority of each Member State, the European Data Protection Supervisor and a representative of the Commission, has played a very significant. The so-called Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC has become particularly influential in the interpretation, application and evolution of EU Data Protection Law by means of the opinions and other documents.[9] As of 25 May 2018 the Article 29 Working Party ceased to exist and was replaced by the European Data Protection Board (EDPB)[10] established under the GDPR. The EDPB is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor [Art. 68(3) GDPR].

1.2 The Concept of Personal Data and Data Protection as Fundamental Right

For the purposes of the GDPR, personal data means: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" [Art. 4(1) GDPR]. The case-law of the CJEU has confirmed that the concept of personal data encompasses IP addresses.[11]

[8] See, *e.g.*, Judgment of the CJEU of 13 May 2014, rendered in case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317, para. 66 with further references.

[9] Available at http://ec.europa.eu/justice/article-29/documentation/index_en.htm.

[10] https://edpb.europa.eu/.

[11] See Judgment of the CJEU of 19 October 2016, case C-581/14, *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, establishing that Article 2(a) of Directive 95/46/EC "must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person". Furthermore, see Judgments of the CJEU of 8 April 2014, Digital Rights Ireland and Seitlinger, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, para. 26; and of 21 December 2016, Tele2 Sverige AB and Secretary of State for the Home Department, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, para 98. See also Judgment of the ECtHR of 24 April 2018, *Benedik v. Slovenia* (app. no. 62357/14) regarding dynamic IP addresses.

hoeren@uni-muenster.de

The protection of natural persons in relation to the processing of personal data is considered a fundamental right under EU law.[12] Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. The CJEU had previously made clear that Union data protection law establish a specific and reinforced system of protection compared with the right to privacy[13] which is laid down in Article 7 of the Charter. Notwithstanding this, both the CJEU and the European Court of Human Rights (ECtHR) tend to treat data protection as closely related to the right to privacy. It is noteworthy that the European Convention on Human Rights (ECHR) has no corresponding provision to Article 8 of the Charter which addresses specifically the fundamental right to data protection and provides that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or on some other legitimate basis laid down by law. In the absence of a similar provision, the ECtHR has derived the right of data protection from Article 8 of the ECHR on the right to privacy.[14] From the perspective of EU law, it can be considered that both rights are closely linked and overlap to a significant extent but differences in their respective scopes may also be identified. For instance, EU legislation on data protection is limited to information relating to natural persons but the right to privacy encompasses legal persons.[15]

The CJEU has constantly held that EU Data Protection Law, in so far as it governs the processing of personal data liable to infringe fundamental freedoms, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter[16] (and the case-law cited). Given the position of data protection law as a fundamental right the case-law of the CJEU on the balancing of the fundamental right to data protection with others, such as the protection of intellectual property, the fundamental freedom to conduct a business enjoyed by internet intermediaries,[17] has become particularly significant.

[12]See on this matter González Fuster (2014).

[13]Judgment of the CJEU of 29 June 2010, Comisión/Bavarian Lager, C-28/08 P, ECLI:EU:C:2010:378.

[14]See Judgments of the ECtHR of 16 February 2000, *Amann v. Switzerland*, App. no. 27798/95, para. 65; and 4 May 2000, *Rotaru v. Romania*, App. No. 28341/95, para. 43, available at http://hudoc.echr.coe.int.

[15]Kokottand and Sobotta (2013), p. 225.

[16]See Judgment of the CJEU of 6 October 2015, C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:6506, para. 38, with further references.

[17]See, *e.g.*, Judgments of the CJEU of 24 November 2011, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; of 16 February 2012, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, C-360/10, ECLI:EU:C:2012:85; and 19 April 2012, *Bonnier Audio and Others v. Perfect Communication Sweden AB*, C-461/10, ECLI:EU:C:2012:219.

hoeren@uni-muenster.de

1.3 Special Categories of Personal Data

The GDPR subjects the processing of special categories of personal data, which are particularly sensitive and create significant risks, to reinforced protection in addition to the general rules of the Regulation for lawful processing. Pursuant to Article 9 of the GDPR, such special categories encompass: "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" as well as "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". Article 4 of the GDPR provides definitions of the terms 'genetic data', 'biometric data' and 'data concerning health' relevant for these purposes.

The processing of the special categories of data listed in Article 9(1) is prohibited unless one of the exceptions laid down in Article 9(2) applies: express consent by the data subject to the extent that the prohibition may be lifted; processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law; processing is necessary to protect the vital interests of the data subject; processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation or any other not-for-profit body with a political, philosophical, religious or trade union aim; processing relates to personal data which are manifestly made public by the data subject; processing is necessary for the establishment, exercise or defence of legal claims; processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law... Furthermore, the GDPR allows Member States to maintain or introduce further conditions with regard to the processing of genetic data, biometric data or data concerning health.

The GDPR imposes similar obligations with regard to the processing of personal data on public actors and private parties. However, public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission are not regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law [Article 4(9) GDPR].

1.4 Supervisory Authorities

Under the GDPR, the establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States are able to establish more than one supervisory authority to reflect their constitutional and organisational structure (art. 51 GDPR). Each supervisory authority is competent on the territory of its own

hoeren@uni-muenster.de

Member State. Unlike the previous regime,[18] the provisions of the Regulation on its territorial scope (Art. 3 GDPR) do not determine the competent national supervisory authority. The Regulation includes specific provisions on the distribution of competences between the supervisory authorities of the Member States with regard to cross-border situations. The GDPR introduces the so-called one-stop-shop mechanism that ensure that one national data protection authority (DPA) is responsible for the supervision of cross-border data operations carried out by a controller or processor in the EU. The GDPR establishes a consistency mechanism for cooperation between the national supervisory authorities.

With a view to guarantee consistent enforcement of the GDPR throughout the Union, the supervisory authorities have in each Member State the same powers. The tasks of the DPA's are listed in Article 57 of the GDPR and the powers are dealt with in Article 58. The tasks include to monitor and enforce the application of the Regulation; promote public awareness on data protection issues; perform advisory functions; handle complaints lodged by a data subject; conduct investigations on the application of the Regulation. The powers of the supervisory authorities are classified in Article 58 in three main groups: investigative powers (such as request and obtain access to information an premises, carry out data protection audits, notify alleged infringements); corrective powers (including to issue warnings and reprimands, order to comply with a data subject's request, to impose a limitation including a ban on processing or to impose an administrative fine); and authorisation and advisory powers (such as to issue opinions, to issue certifications or to adopt certain authorisations). Supervisory authorities are empowered to bring infringements of the GDPR to the attention of the judicial authorities and engage in legal proceedings. The exercise of the powers conferred on the supervisory authority is the subject to effective judicial remedy and due process.

2 Personal Data Processed by Electronic Means

2.1 Main Principles

The general legislative framework established in the GDPR applies also to the protection of personal data in the context of services provided at a distance, by electronic means. It covers the processing of personal data wholly or partly by automated means [Arts. 2(1)], including the collection, recording, structuring, storage, alteration, retrieval, consultation, use, disclosure and making available of such data [Art. 4(2)]. Therefore, the GDPR applies to the protection of personal data in

[18]CJEU Judgment of 1 October 2015 in case C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639 and CJEU Judgment of 5 June 2018 in case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388.

hoeren@uni-muenster.de

social networks.[19] As regards internet intermediaries, it is noteworthy that pursuant to article 2(4) the GDPR is without prejudice to the application of Directive 2000/31/EC on electronic commerce,[20] in particular of the rules on the limitation of liability of intermediary service providers laid down in Articles 12–15 of that Directive. However, the latter provisions do not establish rules on the protection of personal data.[21]

The processing of personal data is only deemed lawful on the basis of at least one of the grounds listed in Article 6 GDPR: (a) the data subject has given consent to the processing of his or her personal data for specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights of the data subject.

Where processing is based on the data subject's consent, the controller has to be able to demonstrate that consent has been given [Art. 7(1) GDPR]. Consent is not being regarded as freely given if the data subject is unable to refuse consent without detriment. Consent requires a clear affirmative act by the data subject establishing a freely given, specific, informed and unambiguous indication of his or her agreement to the processing of personal data. Therefore, Recital 32 to the GDPR acknowledges that consent may be given by electronic means, such as by ticking a box when visiting an internet website or choosing technical settings for information society services. However, pre-ticked boxes or inactivity are not regarded as appropriate since they do not clearly indicate the data subject's acceptance.

The principles of transparency and fair processing require that the data subject be informed of the purposes of the processing. Under the GDPR the specific purposes for which personal data are processed have to be explicit and determined at the time of the collection of the personal data. Otherwise consent by the data subject can not be regarded as informed. Consent is to be given for all purposes in those situations where processing has multiples purposes. The processing has to be restricted to personal data which are adequate and relevant and limited to what is necessary for the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

[19]See, *e.g.*, Article 29 Working Party on Data Protection, Opinion 5/2009 on online social networking, WP 163, adopted on 12 June 2009.

[20]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

[21]De Miguel Asensio (2015), pp. 218–383.

hoeren@uni-muenster.de

2.2 Minors

Article 8 of the GDPR provides for special conditions regarding child's consent in relation to information society services. As noted in the Preamble, such specific protection applies, in particular, to the use of personal data for the purposes of marketing or creating personality or user profiles of children and the collection of personal data when using services offered directly to a child (Recital 38). Where processing is based on the consent given by the data subject, the processing of data of children below the age of 16 years is only deemed lawful to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States are granted certain discretion in this regard, since they may provide by law for a lower age provided that it is not below 13 years. Furthermore, in those situations controllers are under a "reasonable efforts" obligation to verify that consent is given by the holder of parental responsibility over the child, taking into consideration available technology.

2.3 Right to Erasure and Right to Object

Article 17 of the GDPR is devoted to the right to erasure, also known as the 'right to be forgotten', which was admitted under Directive 95/46/EC by the CJEU in its landmark judgment in the *Google Spain* case.[22] Data subjects are granted the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies: data are no longer necessary in relation to the purposes for which they were collected or processed; the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing; the data subject objects to the processing of the data and there are no overriding legitimate grounds for the processing; the data have been unlawfully processed; the data have to be erased for compliance with a legal obligation to which the controller is subject; the data have been collected in relation to the offer of information society services directly to a child.

However, the obligation of the controller to erase the personal data does not apply to the extent that processing is necessary for any of the grounds listed in Article 17 GDPR. Such grounds include: exercising the right of freedom of expression and information; for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority; for reasons of public interest in the area of public health; for archiving purposes in the public

[22]CJEU Judgment of 13 May 2014, case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317. See Article 29 Working Party on Data Protection, "Guidelines on the Implementation of the CJEU Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12", 26 November 2014.

hoeren@uni-muenster.de

interest, scientific or historical research purposes or statistical purposes; or for the establishment, exercise or defence of legal claims. The CJEU has held that the right to be forgotten cannot be generally applied to a company register.[23]

Article 21 of the GDPR grants data subject the right to object at any time to processing of personal data concerning him or her for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing. Moreover, the legislation on the protection of personal data in electronic communications regulates the conditions under which under which unsolicited communications for direct marketing may be conducted. The proposed new ePrivacy Regulation (see this chapter, Sect. 3.1, infra) applies to persons who use electronic communications services to send direct marketing commercial communications, including advertising messages sent by political parties and non-profit organisations. The safeguards provided for by the ePrivacy Regulation to protect end-users against unsolicited communications for direct marketing purposes are to be found in Article 16 of the Proposal.

The ePrivacy Regulation is based on an opt-in approach. Commercial electronic communications for direct marketing purposes may only be sent to end-users who are natural persons that have given their consent. As an exception, the use of e-mail contact details within the context of an existing customer relationship is allowed for the offering of similar products or services, provided that customers are clearly given the opportunity to object. Moreover, end-users that have provided their consent to receiving unsolicited communications for direct marketing purposes are enabled to withdraw their consent at any time in an easy manner. To facilitate effective enforcement of the rules on unsolicited messages for direct marketing, the masking of the identity and the use of false identities and the use of false return addresses are prohibited. Unsolicited marketing communications are required to be clearly recognizable as such. They have to indicate the identity of the person transmitting the communication or on behalf of whom the communication is transmitted, and to provide the necessary information for recipients to exercise their right to oppose to receiving further marketing messages. A link or an email address has to be provided to end-users so that they can easily withdraw their consent.

2.4 Processing of Personal Data in the Context of Employment

The ePrivacy Regulation does not include specific provisions on the processing of personal data of employees through electronic means. The general data protection framework applies to the processing of personal data in the context of employment with some additional provisions laid down in Article 88 of the GDPR. Processing

[23]CJEU Judgment of 9 March 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, ECLI:EU:C:2017:197, paras 55–56.

hoeren@uni-muenster.de

personal data in the field of employment law is one of the grounds that allow derogating from the prohibition on processing special categories of personal data (see this chapter, Sect. 1.3, supra).

According to Article 88 of the GDPR, Member State law or collective agreements may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights.

2.5 Data Security and Data Breach

The basic storage limitation in the GDPR is applicable to data conveyed and stored through electronic means. Pursuant to Article 5(1)(e) of the GDPR a basic principle relating to the processing of personal data is that such data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. At the time when personal data are obtained, the controller is obliged to provide the data subject information regarding the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. Moreover, pursuant to Article 25 of the GDPR the controller is under an obligation to implement measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed, including the period of their storage. Furthermore, pursuant to Article 32, the controller and the processor are obliged to implement technical and organisational measures, such as encryption, to ensure a level of security appropriate to the risks inherent in the processing. Such risks include accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted or stored.

The GDPR establishes specific obligations on controllers to notify a personal data breach to the supervisory authority (art. 33) and to the data subject (art. 34). A definition of 'personal data breach' is provided for in Article 4(12) of the GDPR. It means a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

An obligation is imposed on the controller to notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 h after having become aware of it, unless the controller is able to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Such notification shall include information on the nature of the breach including where possible, the categories and approximate number of data subjects and personal data records concerned; the likely consequences of the breach; and the measures taken or proposed to be taken by the controller. The obligation of the controller to communicate the personal data breach to the data subject without undue delay

hoeren@uni-muenster.de

applies to the situations where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

2.6 Codes of Conduct

The drawing up and approval of codes of conduct in the field of data protection and certification mechanisms in this area are regulated in detail in Article 40–43 of the GDPR. Associations and bodies representing controllers or processors are encouraged to draw up codes of conduct in order to facilitate the effective application of the Regulation. The main goal of such codes of conduct is to specifying the application of the data protection legislation on issues such as fair and transparent processing; the interests pursued by controllers in specific contexts; the collection of personal data; the information provided to data subjects; the exercise of the rights of data subjects; the international transfer of personal data; or alternative dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing. Draft codes of conducted submitted by associations and other bodies may be approved by the competent supervisory authority if it finds that it provides sufficient appropriate safeguards. Such codes are registered and published by the competent supervisory authority. The Commission may decide that an approved code of conduct which relates to processing activities in several Member States has general validity within the Union. The monitoring of compliance with a code of conduct may be carried out by a body which is accredited for that purpose by the competent supervisory authority.

The GDPR encourages associations or other bodies representing categories of controllers or processors to draw up codes of conduct to facilitate the effective application of the Regulation and calibrate the obligations of controllers and processors. Pursuant to Article 40 of the GDPR, the drafting of such codes is deemed of particular interest to take account the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. Relevant stakeholders, including data subjects, should be consulted in the process of adopting a code of conduct. Where a draft code of conduct relates to processing activities in several Member States, it may be submitted to a procedure at European level that can lead to a decision by the Commission establishing that an approved code of conduct has general validity within the Union. The Commission shall ensure appropriate publicity for such codes [Article 40(10) GDPR].

In the previous practice of the Article 29 Working Party, a reference can be made to Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing[24] and to Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing,[25] concluding that the code provided important

[24]WP 174, adopted on 13 July 2010.

[25]WP 232, adopted on 22 September 2015.

hoeren@uni-muenster.de

guidance to cloud computing providers with regard to applicable data protection and privacy rules in Europe, but could not be formally approved, since it did not always meet the minimal legal requirements, and its added value with respect to Directive 95/46/EC and national legislation was not always clear.

The establishment of certification mechanisms and data protection seals and marks are also encouraged under the GDPR to promote transparency by allowing data subjects to easily assess the level of data protection of products and services.

3 Data Protection in the Electronic Communications Sector

3.1 From the ePrivacy Directive to the ePrivacy Regulation

Since the content and metadata of electronic communications may reveal sensitive information about the persons involved, the EU has traditionally adopted special legislation concerning data protection for users of electronic communications services. Previously that special regime was contained in the so-called ePrivacy Directive or Directive 2002/58/EC.[26] In order to ensure consistency with the new GDPR and to adapt the previous regime to the technological and market evolution, Directive 2002/58/EC was intended to be replaced with effect from 25 May 2018 by a the new ePrivacy Regulation. However, pending the final approval of the new Regulation, the current survey is based on the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) of 10 January 2017 (ePrivacy Regulation).[27]

The e-Privacy Regulation is regarded as *lex specialis* to the GDPR. It particularises and complements the general rules on the protection of personal data laid down in the GDPR as regards electronic communications data that qualify as personal data (Recital 6 of the ePrivacy Regulation). All matters concerning the processing of personal data not specifically addressed by the ePrivacy Regulation are covered by the GDPR as the general legal framework in the field. It is noteworthy that the e-Privacy Regulation applies to both natural and legal persons who are end users of electronic communications.

[26]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

[27]COM (2017) 10 final.

hoeren@uni-muenster.de

3.2 Scope of Application

The scope of application of the ePrivacy Regulation is very much influenced by its close connection to the EU regulatory framework for electronic communications. The ePrivacy Regulation covers electronic communications data processed in connection with the provision and use of electronic communications services in the Union. It applies to providers of electronic communications services, to providers of publicly available directories, to software providers permitting electronic communications, and to persons who use electronic communications services to send direct marketing commercial communications or collect information related to or stored in end-users' terminal equipment.

The ePrivacy Regulation relies on the definition of 'electronic communications services' provided for by the proposal for a Directive establishing the European Electronic Communications Code.[28] Such an approach is intended to ensure an equal protection of end-users when using functionally equivalent services, for instance, traditional text messages (SMS) and electronic mail conveyance services and new messaging services and web-based e-mail services. Therefore, the definition of 'electronic communications services' encompasses not only internet access services—including wireless networks provided to an undefined group of end-users in public and semi-private spaces—and services consisting wholly or partly in the conveyance of signals, but also interpersonal communications services, such as voice over IP, messaging services and web-based e-mail services. The ePrivacy Regulation covers as well interpersonal communications services that are ancillary to another service and have communication functionality. Moreover, it applies to the transmission of machine-to-machine communications since it is intended to ensure the protection of privacy and confidentiality with regard to the Internet of Things. Electronic communications services which are not publicly available are not included.

Electronic communications data are defined in Article 4 of the ePrivacy Regulation in a broad and technological neutral way. It encompasses any information concerning the content transmitted and the information concerning an end-user processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Therefore, electronic communications metadata are covered by the Regulation.

[28]Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final—2016/0288 (COD)).

hoeren@uni-muenster.de

3.3 Legal Framework

The basic rule is provided for in Article 5 of the ePrivacy Regulation which establishes that electronic communications data shall be confidential and prohibits any interference with electronic communications data, such as by listening, monitoring or any kind of interception or processing of electronic communications data, by persons other than the end-users, except when permitted by the Regulation. Article 6 of the ePrivacy Regulation establishes the restrictive conditions under which providers of electronic communications networks and services may process electronic communications data (6.1), electronic communications metadata (6.2) and electronic communications content (6.3). Moreover, pursuant to Article 7 of the ePrivacy Regulation providers of electronic communications services are under strict obligations to erase electronic communications content and metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication or billing.

Providers of electronic communications services are obliged to inform end-users of measures they can take to protect the security of their communications, such as using specific types of software or encryption technologies. Moreover, they are also obliged to take, at their own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. Pursuant to article 10 of the ePrivacy Regulation, software placed on the market permitting electronic communications shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting. Additionally, specific obligations on the protection of information stored in and related to end-users' terminal equipment are laid down in Article 8. The use of processing and storage capabilities of terminal equipment, the collection of information from end-users' terminal equipment and the collection of information emitted by terminal equipment to enable it to connect are prohibited except on the grounds provided for in Article 8(1) and (2).

The enforcement of the provisions of the ePrivacy Regulation is entrusted to the same authorities competent for the enforcement of the GDPR (see this chapter, Sect. 1.4, supra). The tasks and powers of those supervisory authorities are also basically those established in the GDPR, but they have the additional task of monitoring the application of the ePrivacy Regulation regarding electronic communications data for legal entities. The ePrivacy Regulation confirms expressly the power of each supervisory authority to impose penalties including administrative fees for any infringement of the Regulation and indicates infringements and the upper limit and criteria to be followed by the supervisory authority when setting administrative fines. According to Article 23, infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant are subject to administrative fines up to €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

hoeren@uni-muenster.de

3.4 Digital Forensics

The ePrivacy Regulation contains provisions on the protection of electronic communications of natural and legal persons and of information stored in their terminal equipment. Such provisions include rules on the confidentiality of electronic communications data, permitted processing of electronic communications data, and storage and erasure of electronic communications data and protection of information stored in and related to end-users' terminal equipment. However, the ePrivacy Regulation does not apply to the activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security [Art. 2(2)(d)].

The ePrivacy Regulation does not include any specific provisions in the field of data retention. In line with Article 23 of the GDPR, Article 11 of the ePrivacy Regulation provides for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. In sum, the ePrivacy Regulation does not affect the ability of Member States to create national data retention frameworks and to carry out lawful interception of electronic communications, in accordance with the Charter[29] and the ECHR.[30]

[29]See Judgment of the CJEU of 8 April 2014, Digital Rights Ireland and Seitlinger, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, on the invalidity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Additionally, see Judgment of the CJEU of 21 December 2016, joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Secretary of State for the Home Department*, ECLI:EU:C:2016:970. For instance, the latter considered that the equivalent to Article 11 in the previous version of the ePrivacy Regulation (Art. 15 of Directive 2002/58) read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precluded national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. Additionally, the Court established that those provisions precluded national legislation governed access of the national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

[30]See Judgment of the ECtHR of 13 September 2018, *Big Brother Watch and Others v. The United Kingdom* (Apps. nos. 58170/13, 62322/14 and 24960/15).

hoeren@uni-muenster.de

At EU level the basic instrument providing common rules for the processing of the personal data of individuals involved in criminal proceedings is Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.[31] It entered into force on 5 May 2016 and it has to be transposed into national law by Member States by 6 May 2018.

Directive (EU) 2016/680 is aimed at ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States. It focuses in strengthening the rights of data subjects and of the obligations of those who process personal data. A criminal offence within the meaning of Directive (EU) 2016/680 is an autonomous concept of Union law and it is not limited to crimes committed through electronic means. The Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

EU Data Protection Law and particularly the GDPR, the ePrivacy Regulation and Directive (EU) 2016/680 do not apply to the processing of personal data related to activities which fall outside the scope of Union law, such as those concerning national security and defence. Hence, the processing of personal data by the Member States when carrying activities concerning national security is not covered by those instruments.

4 Remedies and International Dimension of EU Law

4.1 Remedies and Sanctions

EU Data Protection Law grants significant corrective powers to supervisory authorities, which are empowered, among others, to issue warnings and reprimands to controllers and processors; to impose a temporary or definitive limitation including a ban on processing; and to impose administrative fines [see, particularly, Article 58 (2) of the GDPR]. Data subjects are granted the right to lodge a complaint with a supervisory authority (art. 77 GDPR); to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them (art. 78 GDPR); and the right to an effective judicial remedy where the rights of the subject under the GDPR have been infringed (art. 78 GDPR). The latter is particularly relevant with respect to the right to receive compensation from the controller or

[31] OJ L 119, 4.5.2016, p. 89.

hoeren@uni-muenster.de

processor for the damage suffered which is granted to any data subject who has suffered material or non-material damage as a result of an infringement of the GDPR (art. 82).

Article 83 GDPR establishes the general conditions under which the supervisory authorities of the Member States shall impose administrative fines in respect of infringements of the Regulation, including the general data protection rules, activities in the context of services provided by electronic means, the electronic processing of personal data of employees, the security of personal data processed by electronic means. Concerning the protection of personal data in the context of electronic communications for marketing purposes, it is to be noted that the ePrivacy Regulation establishes that in principle the relevant provisions of the GDPR are also applicable to infringements of the ePrivacy Regulation and includes specific provisions with similarities regarding the right to compensation and liability (Article 22); and the general conditions for imposing administrative fines (Article 23).

Article 83 GDPR envisages the imposition of administrative fines up to €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Such fines may be imposed, for example, in case of infringement of: the basic principles for processing, including conditions for consent; the data subjects' rights; or transfer of personal data to third countries. The maximum limit of fines is the same in Article 23 of the ePrivacy Regulation and applies to infringements of the principle of confidentiality of communications, permitted processing of electronic communications data and certain time limits for erasure.

EU Law does not provide for criminal sanctions but it establishes that Member States shall lay down the rules on other penalties applicable to infringements of data protection law, particularly for infringements which are not subject to administrative fines [see Article 84 GDPR, Article 24 ePrivacy Regulation; and Article 57 Directive (EU) 2016/680].

4.2 Territorial Reach of EU Data Protection Law

The territorial scope of the GDPR is governed by Article 3.[32] First, the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not [Article 3(1)]. The GDPR maintains a broad concept of establishment in line with the case law of the CJEU regarding the previous regime.[33] Establishment implies the effective and real exercise of activity

[32]De Miguel Asensio (2017), pp. 78–86. On some concerns raised by the territorial reach of EU Data Protection Law, see Svantesson (2013), pp. 89–111.

[33]CJEU Judgment of 1 October 2015 in case C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639, and CJEU Judgment of 28 July 2016, C-191/15, *Verein für Konsumenteninformation v. Amazon EU Sàrl*, ECLI:EU:C:2016:612, para. 31, and paras 73–81.

hoeren@uni-muenster.de

through stable arrangements regardless of the legal form (branch, subsidiary…) of such arrangements (Recital 22). According to the guidance provided by the CJEU in its Google Spain judgment, the processing of personal data can be regarded as carried out "in the context of the activities of an establishment" where the activities of a processor not established in the Union, such as a provider of a search engine or social network service, are inextricably linked those of its establishment situated in the Member State concerned.[34]

Second, the GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. [Article 3(2).] Recital 23 of the GDPR clarifies that in order to determine whether goods or services are being offered to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. The mere accessibility of a website in the Union or the use of a language generally used in the third country where the controller is established is not regarded as sufficient to ascertain such intention, but factors such as the use of a language or a currency generally used in one Member State or the mentioning of customers who are in the Union, may be significant to conclude that the controller envisages offering goods or services to data subjects in the Union. The factors provided by the CJEU in its *Pammer and Hotel Alpenhof* Judgment concerning the application of the special jurisdiction provisions protecting consumers to persons that direct their commercial activities to the Member State of the consumer's domicile may also be relevant in this context.[35] Furthermore, pursuant to Recital 24 of the GDPR, in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether persons are tracked on the internet including potential subsequent use of profiling a natural person for behavioural advertising practices.[36]

Finally, the third group of situations where the GDPR applies is the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law, such as in a Member State's diplomatic mission or consular post.

[34]CJEU Judgment of 13 May 2014, rendered in case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317, paras 55 and 56. See also Article 29 Working Party on Data Protection, "Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain", 16 December 2015, Annex II; Kuner (2015), Oro Martínez (2015) and Van Alsenoy and Koekkoek (2015).

[35]Judgment of the CJEU of 7 December 2010, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG* (C-585/08) and *Hotel Alpenhof GesmbH v. Oliver Heller* (C-144/09), ECLI:EU:C:2010:740, paras. 77–78.

[36]On the data protection implications of those practices, see Article 29 Working Party on Data Protection, Opinion 2/2010 on online behavioural advertising, WP 171, adopted on 22 June 2010.

hoeren@uni-muenster.de

4.3 International Data Transfers

A basic goal of the development of common rules on the protection of personal data within the EU is to ensure the free flow of data. Therefore, Article 1(3) of the GDPR makes clear that the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. However, in order to ensure that when the personal data of Europeans are transferred abroad the protection level is not undermined, transfers of personal data to third countries or international organisations are only allowed if the conditions laid down in Chapter V of the GDPR are complied with by the controller and processor. These provisions are based on the significant enforcement experience in this area developed by the EU in previous years.[37]

Transfers to a non-EU country may take place without further safeguards or a specific authorisation on the basis of a Commission "adequacy decision" establishing that a third country—or a particular territory of a third country, or a specific sector or industry within a third country—provides a level of data protection that is essentially equivalent to that in the EU.[38] Article 45(2) GDPR contains a catalogue of elements that the Commission must take into account when adopting decisions on adequacy, which include: the rule of law, respect for human rights and relevant legislation, as well as the implementation of such legislation; the existence and effective functioning of independent supervisory authorities; and the international commitments the third country or international organisation concerned has entered into. The EU-US Privacy Shield is a self-certification mechanism for US based companies which has been recognized by the Commission as providing an adequate level of protection for personal data transferred from an EU entity to US based companies. It is in full effect since 1August 2016.

In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor provides appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Instruments to provide adequate safeguards without requiring a specific authorisation from a supervisory authority include: standard contractual clauses establishing obligations between the EU exporter and the third country importer; binding corporate rules adopted by a multinational group of companies a group of enterprises engaged in a joint economic activity to carry out transfers within the group; and approved codes of conduct or certification mechanisms.

Where no adequacy decision is applicable and no appropriate safeguards have been provided pursuant to Article 46 GDPR, transfers of personal data to a third country are only allowed under one of the conditions laid down in Article 49 GDPR.

[37] See Kuner (2013), pp. 151–154.

[38] Judgment of the CJEU of 6 October 2015, C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:6506, paras. 73–74.

hoeren@uni-muenster.de

Such derogations for specific situations include: explicit consent by the data subject to the proposed transfer, performance of a contract, important reasons of public interest and protection of the vital interests of the data subject.

Chapter V of Directive (EU) 2016/680 (see number 20, supra) contains the common rules on international transfers in the law enforcement sector in order to facilitate cross-border cooperation between police and judicial authorities, both within the EU and with third States. The specific adequacy assessment elements to be made by the Commission when adopting adequacy decisions for the law enforcement sector are listed in Article 36(2) Directive (EU) 2016/680.

4.4 Private Enforcement and Conflict of Laws

EU law does not provide for common conflict-of-laws rules to determine the law applicable to liability for damages caused by the unlawful processing of personal data. The prevailing view is that such claims are excluded from the scope of application of Regulation (EC) No 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) pursuant to Article 1(2)(g). According to this provision, the Regulation does not apply to non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation.

Although this situation has remained unaffected by the adoption of the GDPR, it is noteworthy that the Regulation includes new special jurisdiction rules concerning private claims by data subjects against a controller or processor as a result of the infringement of the rights granted to them by the Regulation. Such rules, which are intended to supplement those of the Brussels I (Recast) Regulation are of special significance in a context in which private enforcement of data protection law has become prominent.[39] In particular, that is the case with regard to the enforcement of the right to compensation where damage results from an infringement of the GDPR. In this respect, Article 79 contains a specific provision on international jurisdiction regarding claims brought by a data subject against a controller or processor where he or she considers that his or her rights under the GDPR have been infringed, including court proceedings for exercising the right to receive compensation.[40] Article 82 of the GDPR provides some common substantive rules on the right of any person who has suffered material or non-material damage as a result of an infringement of the Regulation to receive compensation from the controller or processor for the damage suffered.

[39]CJEU Judgment of 25 January 2018, C-498/16, *Maximilian Schrems v. Facebook Ireland Limited*, ECLI:EU:C:2018:37.

[40]Brkan (2015), pp. 257–278; Kohler (2016), pp. 653–675; De Miguel Asensio (2017), pp. 92–106.

hoeren@uni-muenster.de

References

Albrecht JP, Jotzo F (2017) Das neue Datenschutzrecht der EU. Nomos, Baden-Baden
Brkan M (2015) Data protection and European private international law: observing a bull in a China shop. Int Data Privacy Law:257–278
De Hert P, Papakonstantinou V (2016) The New General Data Protection Regulation: still a sound system for the protection of individuals? Comput Law Secur Rev 32:179–194
De Miguel Asensio PA (2015) Derecho Privado de Internet, 5th edn. Civitas Thomson Reuters, Madrid
De Miguel Asensio PA (2017) Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea. Revista española de Derecho internacional 69 (1):75–108
González Fuster G (2014) The emergence of personal data protection as a fundamental right of the EU. Springer, Heidelberg
Härting N (2016) Datenschutz-Grund-verordnung. Otto Schmidt, Cologne
Kohler C (2016) Conflict of law issues in the 2016 data protection regulation of the European Union. Rivista di Diritto Internazionale Privato e Processuale:653–675
Kokottand J, Sobotta C (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. Int Data Privacy Law 3(4):222–228
Kuner C (2013) Transborder data flows and data privacy law. OUP, Oxford
Kuner C (2015) The Court of Justice of the EU Judgment on data protection and internet search engines: current issues and future challenges. In: Hess B, Mariottini CM (eds) Protecting privacy in private international and procedural law and by data protection. Ashgate, Nomos, Baden-Baden, pp 19–44
Oro Martínez C (2015) The CJEU Judgment in Google Spain: notes on its causes and perspectives on its consequences, protecting privacy in private international and procedural law and by data protection. Ashgate, Nomos, Baden-Baden, pp 45–55
Paal BP, Pauly DA (2017) Datenschutz-Grundverordnung. C.H. Beck, Munich
Svantesson DJB (2013) Extraterritoriality in data privacy law. Ex Tuto, Copenhagen
Van Alsenoy B, Koekkoek M (2015) Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'. Int Data Privacy Law 5(2):105–120

hoeren@uni-muenster.de

Data Protection in International Trade Law

José Augusto Fontoura Costa

1 Introduction

Data protection is often regarded as an issue pertaining to the field of human rights and, particularly, privacy. However, the effective implementation of measures on the issue may have very significant impacts on worldwide flows of information and, therewith, on wealth. Consequently, it is important to take the relations between international trade and data protection into account, in order to better understand the sometimes unstable balance between the reliance of persons involved in international transactions and the freedom of data flows.

This report presents a panoramic picture of the provisions on personal data protection in trade agreements. After a brief conceptual discussion on the relevance of the protection of privacy to international trade of goods and services (Sects. 2–4), it presents a study of the provisions in WTO law (Sect. 5) and the 75 regional trade agreements which hold norms on electronic commerce and are registered in the multilateral system (Sects. 6–8).

Considering that the WTO system is almost universal and that the multilateral system covers a wide array of trade transactions, the report sets its basis on the Regional Trade Agreement Information System, particularly the search in WTO website by "topics covered" in the page http://rtais.wto.org/UI/PublicSearchByCr.aspx, consulted in the period from January 10–31, 2018.

The report is focused on the documents found under the search reference "e-commerce". Nevertheless, the presence of a chapter, annex or section in these agreements on "data protection" or similar expressions is also noticed and analysed in Sect. 6. Since the international liberalisation of financial services is also important to data protection, particularly due to provisions on (a) the free transfer and processing of data and (b) the domestic regulations on protection of confidential

J. A. F. Costa (✉)
University of São Paulo, Law Faculty, São Paulo, Brazil

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_19

hoeren@uni-muenster.de

and sensitive information, the provisions in these agreements on these issues are also studied in Sect. 7. At last, provisions on e-commerce are scrutinized in Sect. 8.

Finally, the conclusions show that different methodologies adopted in order to internationally allow and limit measures on data protection and to control possible negative effects of wealth flows are still far from a wide consensus. The European model, well developed in the European Union and generally replicated in the European Free Trade Area countries, also finds expression in trade agreements that encompass partners from other continents. The United States, nevertheless, puts less pressure on the issue and looks to favour economic flows and more flexible data protection policies. Other countries and organisations have no clear policies on the issue and the differences among domestic legal systems look to be a crucial knot to be untied.

The report, consequently, as far as it reveals the diversified array of treatments and tentative solutions in free trade and economic cooperation agreements, seeks to contribute to the discussion of the data protection effects in trade and, as a consequence, on the international economic governance.

2 Definitions

In this report "international trade" is broadly defined as trans-boundary transfer of wealth in which there is the exchange of goods or services for a payment in money. It encompasses both trade on goods and on services, as well as some investment operations regarding, for instance, the international transfer of productive assets, monetary or not.

"Data protection" is defined as sets of measures adopted to protect personal data from improper use, loss and transfer. It may be adopted by companies, private associations, domestic authorities, legal enactment, and international legal texts, such as model laws, guidelines and treaties. The meaning of information related to marketing authorisation of medical products, such as pharmaceuticals and plants,[1] is not covered by the definition adopted hereby.

"International Trade Law" is the system of international legal documents and institutions aiming at the regulation and liberalisation of international trade. It is a

[1]For instance, EU-GEO FTA, Article 187 (5): "Protection of data submitted to obtain a marketing authorisation for medical products. (. . .) 5. Georgia undertakes to align its legislation concerning data protection for medicinal products with that of the Union at a date to be decided by the Association Committee in Trade configuration, as set out in Article 408(4) of this Agreement." and EU-KOR FTA, Article 10.37 (2): "2. The Parties shall ensure that tests, study reports or information submitted for the first time by an applicant to obtain a marketing authorisation for a plant protection product are not used by third parties or relevant authorities for the benefit of any other person aiming at achieving a marketing authorisation for a plant protection product, unless proof of the explicit consent of the first applicant to use these data is provided. This protection will be hereinafter referred to as data protection."

hoeren@uni-muenster.de

part of International Economic Law, an expression that encompasses all legal and institutional international arrangements on economic issues, since it only covers the trade of goods and services, as well as measures specifically linked to it.

This report, consequently, deals with measures on the protection of personal data set, which are allowed and barred by International Trade Law.

3 General Remarks

The history of International Trade Law can be traced, at least, to the Renaissance and modern treaties of friendship, commerce and navigation. In the nineteenth century the international economic and institutional systems were centred in European and, particularly, British internal order. Most countries around the world held trade and navigation treaties with Britain, as well as the United States, France and Germany, *i.a.* A handful of intertwined networks of treaties that provide for most favoured nation clauses and the general use of British institutions, especially the currency, financial centre, navy and legal system, are the main features of international trade governance before the World War I.

After a relatively chaotic inter-war period, most precisely during the last year of the biggest international armed conflict in History, efforts were made to build an international economic system. The Breton Woods Conference, held in 1944, established two institutions: the International Monetary Fund, to control the value of currencies and mitigate crises of the payments balance, and the International Bank of Reconstruction and Development, to foster economic prosperity around the World.

Though trade issues were not treated in this conference, the United Nations promoted a conference in Havana, 1948, to discuss employment, investment and trade. Meanwhile, by invitation of the United States, 18 countries sat in Geneva to negotiate import tariffs in goods and also celebrate a General Agreement on Trade and Tariffs (GATT) to secure the positive effects of the reduction of commercial barriers. The Havana Charter failed to enter in force and the GATT became the most important international trade treaty and was incorporated to the World Trade Organisation (WTO) in 1995. In its multi decade trajectory, it changed from a relatively restricted club of trading nations to a worldwide, almost universal, trade system.

The GATT is an instrument to liberalize trade in goods as far as it produces positive effects in terms of prosperity. In order to secure that international flow of goods gets increasingly free and mutually beneficial, it lays down some operative rules that (a) protect the negotiated measures from state bypass, (b) ratchet up the liberalization benefits, and (c) grant non-discriminatory treatment to Contracting Parties, notably:

1. National treatment (national like goods cannot, *de jure* or *de facto*, receive better treatment than the goods originated from other Contracting Parties);

hoeren@uni-muenster.de

2. Multilateral and automatic most favoured nation clause (any benefit grant to like products from any country, Member of GATT or not, shall be automatically extended to all Contracting Parties),
3. Forbiddance of non-tariff measures (quantitative and alike),
4. Anti-dumping and compensatory measures, and
5. Exceptions system (also for free trade areas and custom unions).

The WTO gave birth to other multilateral agreements that follow the same structure of liberalising rules. The General Agreement on Trade of Services (GATS) and the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) are particularly important in the study of data protection.

Though this report cannot offer deeper explanations about the international multilateral trade system, it is necessary to stress that the understanding of principles of GATT, GATS and TRIPS, they are important for two reasons: (a) all bilateral and regional agreements regarding trade on goods or on services covered by GATT and GATS have to be harmonized with WTO rules (including TRIPS), since the most favoured nation clause sets that a benefit grant unilaterally or through any agreement shall be *automatically* extended to *all the other* Contracting Parties and (b) the bilateral and regional agreements, although far more detailed nowadays, share a structure that is very similar to the WTO multilateral agreements.

4 Economic Aspects of Data Protection and Free Trade

Data protection measures are focused on regulation of use and transfer of personal data, understood as information linked to the identity of a natural person. Consequently, it is possible to affirm that the pieces of information that are related to or compose the identity of a natural person is the object of protection and, therefore, the meaning of "data" in the expression "data protection".

These data can be economically defined as *goods*, since they can be used to satisfy wants and needs or, to say otherwise, are useful. They are goods to many firms since that make possible a wide use of marketing strategies targeted to specific clients, as well as can be pinned as reputational tags in customer in order to reduce transaction costs.

There is nothing new in it, since people have used registration data to construct direct mail databases for centuries. What is new, besides the very large scale and velocity of electronic environments, is the enhanced capacity to construct identities as jigsaw puzzles. It happens because it is possible to glue data from different sources and construct more complex subjects that bundle, for instance, consuming preferences, time spent in specific internet sites, financial information, political preferences and social circles. Marketing concepts such as personalization and localization are strong trends in e-commerce. Some of these constructions may be more accurate to identify the preferences of a consumer than her or his own awareness.

hoeren@uni-muenster.de

It is important to stress that this use of personal data is completely different from the techniques of big data. In this case, huge amounts of data are statistically treated as *aggregate and untraceable* information and, consequently, it is not possible to perform any kind of individual profiling there through.

In any case, many individuals whose data may be appropriated and processed by firms, associations and even governments may have their complaints, and in particular:

1. Data is a valuable good that belongs to the person and should be paid for;
2. Sharing and treating data may jeopardize the privacy;
3. Individuals get exposed to smart marketing techniques; and
4. Data may be replicated under lower safety measures and get in wrong hands.

Consequently, there is a tension between opposed interests of consumers and business regarding the free use and transfer of personal data. Customers increasingly fear the consequences of misuse of their personal data and that is a possible obstacle to the growth of direct purchases online.

E-commerce, nevertheless, steadily increases both in absolute and relative terms. It is expected to correspond to about 15% of retail shopping in 2021[2] and $3000 billion USD in 2019.[3] Though most of these operations are domestic, there is also a growing number of international transactions. The impacts of e-commerce on international trade of goods and services also are bigger than ever and, therefore, International Trade Law is applicable to many situations related to data protection and may be adapted to deal properly therewith.

It is possible to categorize the e-commerce transactions that have effects on international trade in terms of four variables: (a) agent (consumer or business), (b) territorial scope (domestic or international), (c) object (on goods, services or mixes), and (d) performance (online, actual or mixed). Many of these transactions depend on sharing personal data with other companies, as well as, not oddly, trans-boundary transfer. Nevertheless, it is also possible to imagine a myriad of situations in which misuse and illegitimate transfer of personal data could happen.

Considering this scenario, the challenge of International Trade Law is to secure that national policies on data protection do not unduly restrict trade and, particularly, are not used as measures to protect national markets from foreign goods and services. From this perspective, its primary aim is not to protect consumers' or individuals' privacy, since the multilateral WTO system as well as bilateral and regional trade and investment agreements are clearly designed to the legitimate objective of increasing international flows of wealth and a more efficient international economy.

[2]Data in https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/, access in January 20th, 2018.

[3]Data in https://www.statista.com/statistics/377624/leading-countries-retail-e-commerce-sales/, access in January 20th, 2018.

hoeren@uni-muenster.de

5 WTO Rules on Data Protection

International Law imposes limits to state activities. The WTO system, as an international law institution, also imposes some legal limits to domestic policies. As far as these policies do not affect the trade among its Members, States are free to do whatever they want. It is generally expected that sovereign governments do respect the rules and principles they agreed upon and, though the international dispute resolution and sanctions systems are relatively weak, these expectations are normally respected.

Data protection was no trendy topic when the WTO agreement was signed in 1994. Nevertheless, an important rule in this respect was included in the GATS agreement, namely:

> Art. XIV (c) (ii)
>
> (. . .) nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
>
> (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:
>
> (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

The purpose of this rule is to explicitly except state policies regarding the protection of personal data from the coverage of liberalization rules, including the most favoured nation clause, when applicable, and the national treatment standard. It is open to discussion whether the effects of a domestic measure that are openly discriminatory can be accepted on the basis of this exception and, so far, no case has been brought to the Dispute Settlement system under this article.[4]

The GATT contains no equivalent disposition. Consequently, measures on data protection have no special status in comparison with any other kind of policies. Since the GATS article XIV sets exceptions, the GATT cannot be construed to incorporate such rule. So, it shall not produce effects equivalent to an import tax or quantitative measure, just as it cannot be implemented in a discriminatory way or, in other words, contrary to most favoured nation clause or national treatment standards. The Dispute Settlement system discussed two cases (DS196 and DS171) on "test data protection for agricultural chemicals", which are not covered by the meaning of "data protection" in this report.

Nevertheless, there is a clear potential use of data protection policies to restrict or divert trade. In particular, the use of adequacy criteria to allow cross-border data transfers whenever the target jurisdiction is in a white list have a strong potential to be equated to a restrictive discriminatory measure.

[4]Data in https://www.wto.org/english/tratop_e/dispu_e/dispu_agreements_index_e.htm, consulted in January 21st, 2018.

hoeren@uni-muenster.de

From a panoramic perspective it is possible to assert that the multilateral systems on the trade of goods and services treat in diverse ways the data protection issues. In the field of covered services, which potentially encompasses many e-commerce flows, there is an explicit rule protecting the policy space of Members. Nevertheless, it is not clear how far this rule reaches, since the malicious use of data protection standards to protect domestic markets may be construed as being beyond a reasonable and proportional use of these measures and, therefore, falling outside the scope of allowed policies. The GATT system sets no rule on data protection. Consequently, domestic, bilateral and regional policies on this issue may be non-compliant with WTO, insofar as they unduly restrict trade.

6 European Agreements' Annexes and Chapters on Data Protection

A Chapter on data protection is relatively odd in FTAs, though the European efforts for the creation of Comprehensive Economic Trade Agreements (CETAs) open a wider space to the establishment of common bottom lines for regulatory standards. However, more frequently the European agreements use annexes to indirectly extend the Union's standards to other parties. It is an important instrument both in order to prevent the diminishing of production and marketing costs through regulatory *races to the bottom* and to cooperate and aid the adoption of minimum regulatory standards. Since the EU and its Member States hold high standards on the legal defence of fundamental individual rights, particularly privacy through data protection, there is a case for the inclusion of this issue in international agreements.

It is important to stress that, although sometimes the data protection chapters sound too idealistic and hortatory, provisions on minimum protection standards are very important to set clear limits to the exercise of regulatory jurisdiction of the states. The need to transfer data to offer and perform liberalised services, as well as to make electronic commerce operations effective, makes it very clear that the imposition of high standards on data protection and, consequently, on the transfer and processing of personal information produce impacts on these transactions and, therefore, may be considered as a barrier to international trade. So, the agreement on minimum standards on data protection draws a clearer line dividing legitimate and illegitimate measures, since everything below it allows, on basis of international consensus, correcting defences.

6.1 Council of Europe: European Treaty Series N. 108

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CE Convention 108), signed under the Council of

hoeren@uni-muenster.de

Europe in Strasbourg, 1981, sets the underpinnings to the European data protection system, which grew steadily on its basic structure and preserves its core categorical concepts. It is in force in 51 Parties, 47 of which are European.[5]

Though the Convention was conceived in the pre-internet era, its substantive structure is well adapted to the intense international transfer and processing of personal data under an adequate protective structure. The Chapter II, on principles of data protection, has a deep influence in all European law there-since.

At first, it establishes the duty of parties to "take the necessary measures in [their] domestic law to give effect to the basic principles for data protection" (Article 4) and undertake "to establish appropriate sanctions and remedies for violations" (Article 10). Though this report is not the best place to discuss these principles, a short account may be useful because the European agreements on international trade and economic cooperation rely on the structure provided for in the CE Convention 108.

The *lawfulness*, *purposefulness* and *accuracy* are the criteria for the quality of data established in Article 5. These criteria require notably: (a) fair and lawful access and processing, (b) no use that is incompatible with specified and relevant purposes, (c) adequacy, relevance and no excess in relation to the purpose, (d) information that accurate and updated, and (e) time limits "for no longer that is required for the purpose". It is important to stress that the purpose of the storage, transfer or processing of data strictly determines *how long*, *for which uses* and *which* data can be processed.

Sensitive data are subject to special concerns and limits. Article 6 forbids the automatic processing, unless under appropriate safeguards provided by domestic law, of information revealing, *i.a.*, "racial origin, political opinions or religious or other beliefs, (. . .) health or sexual life (. . .) [and] criminal convictions".

Data security is provided for in Article 7, which states that "appropriate security measures shall be taken (. . .) against accidental or unauthorised destruction, accidental loss as well as against unauthorised access, alteration or dissemination".

Finally, any person is entitled to obtain information about and from the data controller and obtain "rectification or erasure of such data" and "to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred (. . .) is not complied with".

6.2 The European Economic Area

The European Economic Area (EEA) was constituted in 1994 and congregates the EU and the EFTA areas in a single market. Switzerland is the only EFTA Member that has not yet ratified the Agreement. The EFTA Members of the EEA agree to

[5]Data in https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=VteZzbU0, consulted in January 30, 2018.

hoeren@uni-muenster.de

enact normative instruments similar to EU law in areas related to economic integration.

Regarding the data protection system, all EU and EFTA Members are Parties of the CE Convention 108. Moreover, EFTA EEA Members adopt the EU norms on this issue through the incorporation of dispositions recollected in the Annex XI of the EEA Agreement on "Electronic Communication, Audiovisual Services and Information Society", which incorporates one EU Regulation (611/2013/EU), the two EU Directives on the issue (95/94/EC and 2002/58/EC), as well as many Decisions (namely Decisions nos. 2000/518/EC, 2001/497/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2004/915/EC, 2008/393/EC, 2010/87/EU, 2010/146/EU, 2010/625/EU, 2011/61/EU, 2012/484/EU, 2013/65/EU, 2016/2295/EU, 2012/2297/EU, 2016/1250/EU, and 2016/2297/EU).

6.3 The EU-CARIFORUM Agreement

The general structure of a chapter on data protection that can perform these functions needs to include at least two aspects: the material scope of the chapter and the establishment of a legal duty to adopt and make effective a minimum regime of data protection. The EU-CARIFORUM Agreement (2008) sets the scope by articles on *objectives* and *definitions*. An article on *principles* describes the minimum regime, which is composed both of a set of standards and rights, and of indicative rules on enforcement. The chapter is complemented by hortatory rules on cooperation and mandatory notification and consultation procedures to keep the international coherence of the standards agreed.

The objectives make clear the double nature of data protection: a principiological one, which protects privacy, freedom and rights of natural persons, and a functional one, which is justified by the need to increase cross-border flows of personal data for a more efficient international market. It also includes principles of transparency and fairness. Moreover, the central objective of the chapter is the agreement on the duty to establish "appropriate regulatory regimes" and "appropriate administrative capacity", including independent supervisory authorities, to "ensure and adequate level of protection" in line with "high international standards".[6] The definitions include

[6]EU-CARIFORUM FTA (2008), Chapter 6, Article 197: "General Objective. 1. The Parties and the Signatory CARIFORUM States, recognising: (a) their common interest in protecting fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, (b) the importance of maintaining effective data protection regimes as a means of protecting the interests of consumers, stimulating investor confidence and of facilitating transborder flows of personal data; (c) that the collection and processing of personal data should be accomplished in a transparent and fair manner, with due respect accorded to the data subject, agree to establish appropriate legal and regulatory regimes, as well as appropriate administrative capacity to implement them, including independent supervisory authorities, in order to ensure an adequate level of protection of individuals with regard to the processing of personal data, in line with existing high international standards (1). 2. The Signatory CARIFORUM States shall endeavour to

hoeren@uni-muenster.de

"personal data", "processing of personal data" and "data controller".[7] In other words, there is a legal mandatory rule that obliges the parties to adopt an effective regime on data protection.

Nevertheless, if the *normative* Chapter's core is the article on objectives, the Article on "principles" delineates its substantive content. It establishes not only principles, but also the basis for rights and parameters of enforcement.[8] In analytic terms:

---

implement the provisions of paragraph 1 as soon as possible and no later than seven years after the entry into force of this Agreement."

[7]EU-CARIFORUM FTA, Chapter 6, Article 198: "Definitions. For the purposes of this Chapter: (a) 'personal data' means any information relating to an identified or identifiable individual (data subject); (b) 'processing of personal data' means any operation or set of operations which is performed upon personal data, such as collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, combination, blocking, erasure or destruction, as well as transfers of personal data across national borders; (c) 'Data Controller' means the natural or legal person, authority or any other body which determines the purposes and means of the processing of personal data."

[8]EU-CARIFORUM, Article 199: "Principles and general rules. The Parties agree that the legal and regulatory regimes and administrative capacity to be established shall, at a minimum, include the following content principles and enforcement mechanisms: (a) Content principles (i) the purpose limitation principle — data should be processed for a specific purpose and subsequently used or further communicated only in so far as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those provided by legislation and necessary in a democratic society for important public interests; (ii) the data quality and proportionality principle — data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed; (iii) the transparency principle — individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information in so far as this is necessary to ensure fairness. The only exemptions permitted should be those provided by legislation and necessary in a democratic society for important public interests; (iv) the security principle — technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller; (v) the rights of access, rectification and opposition — the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be those provided by legislation and necessary in a democratic society for important public interests; (vi) restrictions on onward transfers — as a matter of principle, further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (*i.e.* the recipient of the onward transfer) is also subject to rules affording an adequate level of protection; (vii) sensitive data — where special categories of data are involved, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning health or sex life, and data relating to offences, criminal convictions or security measures, data may not be processed unless domestic law provides additional safeguards. (b) Enforcement mechanisms Appropriate mechanisms shall be in place to ensure that the following objectives are achieved: (i) to ensure a good level of compliance with the rules, including a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them; the existence of effective and dissuasive sanctions; and systems of direct verification by authorities, auditors, or independent data protection officials; (ii) to

hoeren@uni-muenster.de

1. Principles:
   a. transfer and processing limited to the *purpose* (the data is to be the *minimum* to reach the objectives of its collection, transfer and processing);
   b. guarantee of data *quality* and *proportionality* of data processed (data is to be accurate, kept up to date, adequate, relevant and not excessive in relation to the purpose);
   c. *transparency* (on the purpose of processing and identity of data controller);
   d. data *security* (technical and organisational measures);
   e. rights to *access, rectification and opposition*;
   f. restrictions on *onward transfers* (second recipients under rules that afford an adequate level of protection); and
   g. special regimes for *sensitive data*.
2. Enforcement mechanisms:
   h. promotion of awareness of duties and rights;
   i. effective and dissuasive sanctions;
   j. systems of direct verification;
   k. rights enforced rapidly and effectively, and without prohibitive cost;
   l. adequate redress; and
   m. exceptions.

Principles a, c and e suffer the *only* allowed exception if (a) it is provided by statutory law *and* (b) is required by public interests in a democratic society.

These principles and minimum framework for enforcement are enough to set high standards of data protection. Such rules may justify domestic or community measures that affect obligations on trade in goods and in services. It is true that no individual effective right is set by the chapters, since they depend on domestic enactment of specific legislation and regulation on data protection. Nevertheless, its effects on international trade law are immediate.

6.4 Articles and Sections on Data Protection

Articles on cooperation are clearly hortatory and have no direct effect on trade issues. Expressions such as "acknowledge the importance of cooperation"[9] and

provide support and help to individual data subjects in the exercise of their rights, who must be able to enforce their rights rapidly and effectively, and without prohibitive cost, including through appropriate institutional mechanisms allowing independent investigation of complaints; (iii) to provide appropriate redress to the injured party where rules are not complied with allowing compensation to be paid and sanctions imposed where appropriate in accordance with applicable domestic rules."

[9]EU-CARIFORUM FTA, Article 201: "Cooperation. The Parties acknowledge the importance of cooperation in order to facilitate the development of appropriate legislative, judicial and

hoeren@uni-muenster.de

"agree to cooperate"[10] clearly denote the absence of any legal duty to cooperate. Nevertheless, a disposition on cooperation in this issue, in agreements with no specific structured rules but an isolated provision,[11] is an evidence of a shared awareness of the questions to be dealt with.

Moreover, the EU-Ukraine FTA (2014)[12] includes an express reference to "relevant Council of Europe instruments". This rule is a non-explicit reference to the Convention 108, which is the original matrix of further EU legislation.

The adoption of annexes is far more effective than a simple reference in an open rule on cooperation. This is the case of the EU-Moldova FTA (2014), which includes an annex on Freedom, Security and Justice. The adoption of the relatively short Annex I to Title III[13] (Freedom, Security and Justice) is aimed to produce deep

institutional frameworks as well as an adequate level of protection of personal data consistent with the objective and principles contained in this Chapter."

[10]EU-Central America FTA, Article 34: "Personal data protection. 1. The Parties agree to cooperate in order to improve the level of protection of personal data to the highest international standards, such as the Guidelines for the Regulation of Computerised Personal Data Files, modified by the General Assembly of the United Nations on December 14th 1990, and to work towards the free movement of personal data between the Parties, with due regard to their domestic legislation. 2. Cooperation on protection of personal data may include, *inter alia*, technical assistance in the form of exchange of information and expertises taking into account the laws and regulations of the Parties." EU-Chile FTA (2005), Article 30: "Data protection. 1. The Parties agree to cooperate on the protection of personal data in order to improve the level of protection and avoid obstacles to trade that requires transfers of personal data. 2. Cooperation on personal data protection may include technical assistance in the form of exchange of information and experts and the establishment of joint programmes and projects."

[11]*Inter alia,* EU-Central America FTA (2013) Article 34; EU-Chile FTA (2005), Article 30; EU-Ukraine FTA (2014), Article 15.

[12]EU-Ukraine (2014), Article 15: "Protection of personal data The Parties agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, including the relevant Council of Europe instruments. Cooperation on personal data protection may include, *inter alia*, the exchange of information and of experts."

[13]EU-Moldova FTA, Annex I to Title III (Freedom, Security and Justice: "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks Commitments and Principles on personal data protection 1. The Parties shall, in the context of the implementation of this or other Agreements, ensure a legal level of data protection which at least corresponds to that set out in Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed on 28 January 1981 (ETS No 108) and its Additional Protocol, regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No 181). Where relevant, the Parties shall take into account Recommendation No. R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector. 2. In addition the following principles shall apply: (a) both the transferring authority and the receiving authority shall take every

hoeren@uni-muenster.de

effects, since its mandatory force and effects are pervasive and it introduces the whole European standards and principles in the agreement with no need for a specific chapter, albeit achieving similar results.

The EU-Georgia FTA (2014), though negotiated and signed in the same context as the Moldova and the Ukraine treaties, does not hold a specific chapter on the issue, although it contains scattered provisions on data protection throughout its text and a general regime in the Annex I,[14] which incorporates the European regime on the issue into the agreement. Separate articles concern cooperation against terrorism,[15] electronic commerce,[16] and civil enforcement.[17] The Japan-Singapore FTA (2002)

reasonable step to ensure, as appropriate, the rectification, erasure or blocking of personal data where the processing does not comply with the provisions of Article 13 of this Agreement, in particular because those data are not adequate, relevant, or accurate, or because they are excessive in relation to the purpose of processing. This includes the notification of any rectification, erasure or blocking to the other Party; (b) upon request, the receiving authority shall inform the transferring authority of the use of the transferred data and of the results obtained there-from; (c) personal data may only be transferred to the competent authorities. Further transfer to other authorities requires the prior authorisation of the transferring authority; (d) the transferring and the receiving authorities are under an obligation to make a written record of the communication and receipt of personal data."

[14]EU-GEO FTA, Annex I: "Each Party shall, in the context of the implementation of this or other Agreements, ensure a legal level of data protection which at least corresponds to that set out in Directive ECUADOR of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed on 28 January 1981 (ETS No. 108) and the Additional Protocol thereto, regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No. 181). Where relevant, each party shall take into account Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, and Recommendation No R (87)15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector."

[15]EU-GEO FTA, Article 20 (1) (b): "1. In full accordance with the principles underlying the fight against terrorism as set out in Article 12 of this Agreement, the Parties reaffirm the importance of a law enforcement and judicial approach to the fight against terrorism and agree to cooperate in the prevention and suppression of terrorism in particular by: (. . .) (b) exchanging information on terrorist groups and individuals and their support networks, in accordance with international and national law, in particular as regards data protection and the protection of privacy;"

[16]EU-GEO FTA, Article 127 (2): "Objectives and principles. (. . .) 2. The Parties agree that the development of electronic commerce must be compatible with the international standards of data protection in order to ensure the confidence of users of electronic commerce."

[17]EU-GEO FTA, Article 200 (5): "Border measures. (. . .) 5. The Parties agree to effectively implement Article 69 of the TRIPS Agreement in respect of international trade in goods suspected of infringing intellectual property rights. For that purpose, the Parties shall establish and notify contact points in their customs administrations and shall be ready to exchange data and information on trade in such goods affecting both Parties. They shall, in particular, promote the exchange of information and cooperation between customs authorities with regard to trade in counterfeit trademark goods and pirated copyright goods. Without prejudice to the provisions of Protocol II on Mutual Administrative Assistance in Customs Matters to this Agreement customs authorities shall, where appropriate, exchange such information swiftly and with due respect to data protection laws of the Parties."

hoeren@uni-muenster.de

protects personal data through the establishment of exceptions under the chapters on trade in services,[18] investment,[19] and the free movement of natural persons.[20]

7 Financial Services

Agreements with chapters or annexes on financial services may deal with two main questions regarding data protection: trans-boundary transfer of information and limits of public access to sensitive or confidential data.

The first question is addressed because general interdiction of transfer of personal data is a possible domestic measure to protect individuals through, for instance, the adoption of white lists of countries and regions to which data may flow. Since financial services eventually depend on personal data and information, the regulatory management of lists and criteria of data protection could bypass treaty provisions on financial services' liberalisation. So, although it should be regarded as implicit in a financial services agreement, some texts include an explicit disposition that allows financial data transfer consistent with the conduct of ordinary business.

The second question is related to the limits of the effects of an agreement on liberalisation of financial services. Albeit in different degrees and structures, public entities often collect and hold information on individual customers of financial institutions. The management of such data follows the standards established in domestic law, which is expressly recognized as being outside the scope of international instruments of financial services liberalisation, such as the Annex on this issue of GATS, which states:

> *2. Domestic regulation.*
>
> (. . .)
>
> (b) Nothing in the Agreement shall be constructed to require a Member to disclose information relating to the affairs and accounts of individual customers or any confidential proprietary information in the possession of public entities.

Somewhat equivalent texts can be found in many free trade and economic cooperation agreements, always preserving the state jurisdiction in this regard. As a matter of fact, some degree of protection of identity and sensitive financial

[18] JPN-SIN FTA, Article 69: "General Exceptions under Chapter 7. 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination on trade in services between the Parties, nothing in this Chapter shall be constructed to prevent the adoption or enforcement by either Party of measures: (. . .) (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to: (. . .) (ii) the protection of the privacy of individuals in relations to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;"

[19] JPN-SIN FTA, Article 83: identical wording as Article 69, quoted above.

[20] JPN-SIN FTA, Article 95: identical wording as Article 69, quoted above.

hoeren@uni-muenster.de

information is very important to direct the choices of international customers of these services. Although it is generally accepted that access to financial data and the identification of the natural and legal entities in the end of sometimes intricate and complex chains of assets transfer and ownership is very important for tax and security efforts, it is also fair to consider that a liberalisation agreement is not necessarily the best place to set rules on access to private and sensitive information. That is the rationale of rules in many agreements, as it will be shown below.

It is important to stress that this analysis does not cover the trans-border offer of financial services of data processing. Although it is clear that these services often depend on international information flow and treaty provisions in this regard impact the legal regime of personal data protection, the relatively narrow scope of their norms and their predominantly technical function suggest that it can be better studied in connection to financial services.

7.1 Transfer and Processing of Information

The Agreement Establishing the ASEAN-Australia-New Zealand Free Trade Area (ASEAN-AUT-NZL FTA) (2010) prohibits, in its annex on financial services, measures that prevent the transfer or processing of information "necessary for the conduct of the ordinary business of a financial service supplier" (Art. 7 (1) (a) (b)). Moreover, Art. 7 (2) (a) makes clear that States can protect personal data in according to domestic law and regulations "so long as such right shall not be used as means of avoiding the Party's commitments or obligations under this Agreement".[21] There are also provisions that secure the power of administrative or regulatory authorities. The Chile-Thailand FTA (2015) holds very similar rules

[21] Agreement Establishing the ASEAN-Australia-New Zealand Free Trade Area, Annex on Financial Services, Article 7: "Transfers of Information and Processing of Information 1. A Party shall not take measures that: (a) prevent transfers of information, including transfers of data by electronic means, necessary for the conduct of the ordinary business of a financial service supplier; 115 (b) prevent the processing of information necessary for the conduct of the ordinary business of a financial service supplier; or (c) prevent transfers of equipment necessary for the conduct of the ordinary business of a financial service supplier, subject to importation rules consistent with international agreements. 2. Nothing in Paragraph 1: (a) restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts including in accordance with its domestic laws and regulations so long as such right shall not be used as a means of avoiding the Party's commitments or obligations under this Agreement; (b) prevents a regulator of a Party for regulatory or prudential reasons from requiring a financial service supplier in its territory to comply with domestic regulation in relation to data management and storage and system maintenance, as well as to retain within its territory copies of records; or (c) shall be construed to require a Party to allow the cross-border supply or the consumption abroad of services in relation to which it has not made specific commitments, including to allow non-resident suppliers of financial services to supply, as a principal, through an intermediary or as an intermediary, the provision and transfer of financial information and financial data processing as referred to in Article 2(a)(xv) (Definitions)."

hoeren@uni-muenster.de

regarding the transfer of data necessary to ordinary business and on confidential information.[22] The EFTA-Colombia FTA (2011), although by a far simpler text, also sets a general permission of data transfers "necessary for the conduct of regular business" and reserves State jurisdiction to protect "personal data, personal privacy and the confidentiality of individual records and accounts", insofar as "not used to circumvent" the provisions on trade in services.[23]

The EU-CARIFORUM FTA (2008) also allows expressly the transfer of personal data for normal business, although it sets a duty to "adopt adequate safeguards to the protection of privacy and fundamental rights, and freedom of individuals".[24] The EU-Central America FTA (2013),[25] the EU-Colombia, Peru and Ecuador FTA

[22]CHI-THA FTA, Chapter 10, Articles 10.7 and 10.8.: "Article 10.7: Data Processing in the Financial Services Sector 1. In sectors where specific commitments are undertaken, each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other forms, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Nothing in paragraph 1 shall: (a) restrict the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts including in accordance with its domestic laws and regulations so long as such right shall not be used as a means of avoiding the Party's commitments or obligations under this Agreement; (b) prevent a regulator of a Party for regulatory or prudential reasons from requiring a financial service supplier in its territory to comply with domestic regulation in relation to data management and storage, and system maintenance, as well as to retain within its territory copies of records; or (c) be construed to require a Party to allow the cross-border supply or the consumption abroad of services in relation to which it has not made specific commitments including to allow non-resident suppliers of financial services to supply, as a principal, through an intermediary or as an intermediary, the provision and transfer of financial information and financial data processing as referred to in subparagraph (o) of Article 10.1. Article 10.8: Confidential Information Nothing in this Chapter shall: (a) require any of the Parties to provide confidential information, the disclosure of which would impede law enforcement, or otherwise be contrary to the public interest, or which would prejudice legitimate commercial interests of particular juridical persons, whether public or private; and (b) be construed to require a Party to disclose information relating to the financial affairs and accounts of individual customers, or any confidential or proprietary information in the possession of public entities."

[23]EFTA-COL FTA, Annex XV, Article 8: "No Party shall take measures that prevent transfers of information into or out of the Party's territory or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier of another Party. Nothing in this Article restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of Chapter 4."

[24]EU-CARIFORUM FTA, Article 107: "Data processing. 1. The EC Party and the Signatory CARIFORUM States shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of their territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. The EC Party and the Signatory CARIFORUM States shall adopt adequate safeguards to the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data."

[25]EU-Central America FTA, Article 198: "1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for

hoeren@uni-muenster.de

(2013),[26] the EU-Georgia FTA (2014),[27] the EU-Korea FTA (2011),[28] the EU-Moldova FTA (2014),[29] and the EU-Ukraine FTA (2014)[30] regulate the same issue with little differences in their wording. These provisions establish a general permission of trans-boundary data transfer. Moreover, a general minimum human rights standard of protecting privacy also limits the duty to allow the transfers.

data processing where such processing is required in the ordinary course of business of the financial service supplier (1). 2. Each Party shall adopt or maintain adequate safeguards to the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data."

[26]EU-COL, PER, ECU, Article 157: "Data processing. 1. Each Party shall permit a financial service supplier of another Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of the right to privacy and the freedom from interference with the privacy, family, home or correspondence of individuals, in particular with regard to the transfer of personal data."

[27]EU-GEO FTA, Article 118: "1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data."

[28]EU-KOR FTA, Article: "Data processing No later than two years after the entry into force of this Agreement, and in no case later than the effective date of similar commitments stemming from other economic integration agreements: (a) each Party shall permit a financial service supplier of the other Party established in its territory to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier; and (b) each Party, reaffirming its commitment to protect fundamental rights and freedom of individuals, shall adopt adequate safeguards to the protection of privacy, in particular with regard to the transfer of personal data."

[29]EU-MOL FTA, Article 245: "Data processing. 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights and freedoms of individuals, in particular with regard to the transfer of personal data."

[30]EU-UKR FTA, Article 128: "Data processing. 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 29.5.2014 Official Journal of the European Union L 161/63 EN 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights and the freedom of individuals, in particular with regard to the transfer of personal data."

hoeren@uni-muenster.de

The India-Singapore CE CA (2005),[31] the Japan-Switzerland (2009)[32] and the Korea-Vietnam FTA (2015)[33] also protect the transfer of data necessary to business, although they reserve the right of Parties to regulate the issue as far as they do not circumvent the Agreement. The Korea-Australia FTA (2014) also admits both the need of transfer and the right to regulate of parties to "protect sensitive information of customers".[34]

The EU-Chile FTA (2005) provides for a general permission of transfer whenever it is consistent with the ordinary course of business, although the domestic legal protection of privacy shall prevail. There is no express reference to international standards, which allows the construction of the agreement as recognising an almost boundless State jurisdiction on this issue. However, the provisions on exceptions make it clear that measures on data protection cannot constitute "a

[31]IND-SIN CECA, Annex 7C, Article 6: "No Party shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this paragraph restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of this Agreement."

[32]JPN-SWI FTA, Annex VI—Financial Services, Article VIII "Transfers of Information and Processing of Information. Neither Party shall take measures that prevent transfers of information into or out of its Area or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfer of financial information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier of the other Party. Nothing in this Article restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of Chapter 6."

[33]KOR-VNM FTA, Annex 8-A, Article 6: "Data Protection. (a) Each Party shall permit a financial service supplier of the other Party established in its territory to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. (b) Nothing in subparagraph (a) restricts the right of a Party to adopt or maintain measures to protect personal data, personal privacy, and to require a financial service supplier to obtain prior authorization from the relevant regulator to transfer such information, based on prudential considerations."

[34]KOR-AUT FTA, Annex 8-B, Section A: "Transfer of information: 1. Each Party shall allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the institution's ordinary course of business. Korea shall give effect to this commitment no later than two years after the date of entry into force of this Agreement, and in no case later than the effective date of similar commitments stemming from other international trade agreements. 2. Nothing in paragraph 1 shall restrict the right of a Party to protect sensitive information of consumers and to prohibit unauthorised reuse of such information so long as such right is not used as a means of avoiding the Party's commitments or obligations under this Agreement. The Parties reserve the right of their financial regulators to have access to records of financial services suppliers relating to the handling of such information and to require for the location of technology facilities."

hoeren@uni-muenster.de

means of arbitrary or unjustifiable discrimination".[35] The Japan-Australia FTA (2015),[36] the Japan-Mongolia FTA (2016),[37] and the Singapore-Australia FTA (2017)[38] regulate the issue similarly. Exceptions are also provided for in the

[35]EU-Chile FTA, Article 122: "Data processing in the financial services sector.1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Where the information referred to in paragraph 1 consists of or contains personal data, the transfer of such information from the territory of one Party to the territory of the other Party shall take place in accordance with the domestic law regulating the protection of individuals with respect to the transferring and processing of personal data of the Party out of whose territory the information is transferred"; Article 135 (1) (e) (ii): "Exceptions. 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in services, financial services or establishment, nothing in this Title shall be construed to prevent the adoption or enforcement by either Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."

[36]JPN-AUT FTA, Article 11.6: "Transfers of Information and Processing of Information Neither Party shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this Article restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of this Chapter and Chapters 9 (Trade in Services) and 14 (Investment)."

[37]JPN-MNG FTA, Annex 4 to Chapter 7, Article 11: "Transfers of Information and Processing of Information Neither Party shall take measures that prevent transfers of information into or out of its Area or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier of the other Party. Nothing in this Article restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of Chapter 7 or the Annexes referred to therein."

[38]SIN-AUT FTA, Chapter 9, Annex 9-B, Section B: "Each Party shall allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business. Nothing in this Section restricts the right of a Party to adopt or maintain measures to: (a) protect personal data, personal privacy and the confidentiality of individual records and accounts; or (b) require a financial institution to obtain prior authorisation from the relevant regulator to designate a particular enterprise as a recipient of such information, based on prudential considerations, provided that this right is not used as a means of avoiding the Party's commitments or obligations under this Section."

hoeren@uni-muenster.de

EU-Canada CETA (2017),[39] the EU-Korea FTA (2011),[40] the EU-Moldova FTA (2014),[41] and the EU-Ukraine FTA (2014)[42], which are extensive to other services and e-commerce.

[39]EU-CAN CETA, Chapter 28 (Exceptions), Article 28.3 (General exceptions) (2) (c) (ii): "2. For the purposes of Chapters Nine (Cross-Border Trade in Services), Ten (Temporary Entry and Stay of Natural Persons for Business Purposes), Twelve (Domestic Regulation), Thirteen (Financial Services), Fourteen (International Maritime Transport Services), Fifteen (Telecommunications), Sixteen (Electronic Commerce), and Sections B (Establishment of investments) and C (Non-discriminatory treatment) of Chapter Eight (Investment), subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by a Party of measures necessary: (. . .) (c) to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;"

[40]EU-KOR FTA, Article 7.50 (e) (ii): "Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by either Party of measures: (. . .) (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to: (. . .)(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."

[41]EU-MOL FTA, Article 261 (2) (e) (ii) "General exceptions. 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by any Party of measures: (. . .) (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: (. . .) (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;"

[42]EU-Ukraine FTA, Article 141 (2) (e) (ii) "General exceptions. 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by any Party of measures: (. . .) (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: (. . .) (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;"

hoeren@uni-muenster.de

The Korea-United States FTA (2012)[43] and the Peru-Korea FTA (2011)[44] secure the normal transfer of information "required in the institution's ordinary course of business" with no specific exception concerning data protection or privacy measures.

The EU-Canada Comprehensive Economic and Trade Agreement (CETA) (2017) also generally allows the trans-boundary data transfer "required in the ordinary course of business". Nevertheless, it is stricter in terms of protection of personal data and privacy, since it sets a duty upon Parties to "maintain adequate safeguards to protect privacy" and defines as applicable the law of the territory of origin of data. The question, in this instance, does not concern the risk of undue use of data protection measures to circumvent the treaty effects. The provision is concerned to the establishment of a positive duty to lay down adequate regulation and a conflict of laws provisions on basis of the place of origin of information.[45] Similar solutions are given in the Mexico-Panama FTA (2015)[46] and the Pacific Alliance (2016),[47] although they adds the requirement of a previous permission from the regulating authority.

[43]KOR-USA FTA (2012), Section B—Transfer of information: "Each Party shall allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the institution's ordinary course of business. Korea shall give effect to this commitment no later than two years after the date this Agreement enters into force."

[44]PER-KOR FTA (2011) Annex 12C, Section A: "Transfer of information. Each Party shall allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the institution's ordinary course of business 1. Korea shall give effect to this commitment no later than two years after the date of entry into force of this Agreement."

[45]EU-CAN CETA, Chapter 13, Article 13.15: "1. Each Party shall permit a financial institution or a cross-border financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing if processing is required in the ordinary course of business of the financial institution or the cross-border financial service supplier. 2. Each Party shall maintain adequate safeguards to protect privacy, in particular with regard tithe transfer of personal information. If the transfer of financial information involves personal information, such transfers shall be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated."

[46]MEX-PAN FTA, Chapter 11, Article 11.8: "Data processing. 1. Under previous authorization of the regulator or authority in charge, whenever required, each Party shall permit a financial institution from the other Party to transfer information into or out of the Party's territory, by any means authorised therein, to its processing, whenever necessary to perform the ordinary course of business of these institutions. 2. To greater clarity, whenever the information referred to in paragraph 1 is composed of or includes personal data or confidential information, the transfer of such information is performed in conformity to the domestic law on protection of persons regarding the transfer and processing of personal data from the Party in which or from which territory the information is transferred." (My translation.)

[47]Pacific Alliance, Article 11.7: "Data processing. 1. Under previous authorization of the regulator or authority in charge, whenever required, each Party shall permit a financial institution from the other Party to transfer information into or out of the Party's territory, by any means authorised therein, to its processing, whenever necessary to perform the ordinary course of business of these institutions. 2. To greater clarity, whenever the information referred to in paragraph 1 is composed of or includes personal data or confidential information, the transfer of such information is

hoeren@uni-muenster.de

7.2 Treatment of Certain Information

Most agreements provide in their chapters on financial services that nothing in them creates any duty of the Parties to offer access to sensitive information, notably data "related to the financial affairs and accounts of an individual customer" or "confidential information (...) of a particular enterprise". These provisions are often reinforced by general references to the consistency of the FTA with WTO system, particularly the GATS Annex on financial services, which reserves the jurisdiction in this field to domestic authorities.

Although these provisions cover personal data, there is no special reference to privacy. In fact, the function of these provisions is to make it clear that the Parties in the agreement keep their jurisdiction and control over the legislative and administrative aspects of the regime of confidentiality of private costumers. With little wording differences this is also the case of the Canada-Peru FTA (2009),[48] the Canada-Panama FTA (2013),[49] the Costa Rica-Colombia FTA (2016),[50] the CAFTA-Dominican Republic (2006),[51] the Korea-United States FTA (2012),[52] the

performed in conformity to the domestic law on protection of persons regarding the transfer and processing of personal data from the Party in which or from which territory the information is transferred." (My translation.)

[48]CAN-PER FTA, Chapter 11, Article 1107: "Nothing in this Chapter requires a Party to furnish or allow access to: a. information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or b. any confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[49]CAN-PAN FTA, Chapter 12, Article 12.8: "This Chapter does not require a Party to furnish or allow access to: information related to the financial affairs and accounts of an individual customer of a financial institution or a cross-border financial service supplier; or confidential information which if disclosed would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of a particular enterprise."

[50]CTR-COL FTA, Chapter 14, Article 14.7: "This Chapter does not require a Party to furnish or allow access to: information related to the financial affairs and accounts of an individual customer of a financial institution or a cross-border financial service supplier; or confidential information which if disclosed would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of a particular enterprise." Though there is no official translation of the Spanish text, the text of the CAN-PAN FTA uses the text hereby transcribed as corresponding to the Spanish wording that is identical to the COL-PAN FTA.

[51]CAFTA-DR, Chapter 12, Article 12.7: "Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[52]KOR-USA FTA, Chapter 13, Article 13.7: "Treatment of certain information. Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

hoeren@uni-muenster.de

Mexico-Panama FTA (2015),[53] the Nicaragua-Chinese Taipei (2008),[54] the Pacific Alliance (2016),[55] the Panama-Singapore FTA (2006),[56] the Peru-Korea FTA (2011),[57] the Singapore-Australia FTA (2017),[58] the United States-Bahrain FTA (2006),[59] the United States-Chile FTA (2004),[60] the United States-Colombia FTA

[53]MEX-PAN FTA, Chapter 11, Article 11.9: "Treatment of certain type of information. Nothing in this Chapter requires a Party to reveal or allow access to: a. information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or b. any confidential information which disclosure would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises." (My translation.)

[54]NIC-TWN, Chapter 12, Article 12.07: "Treatment of Certain Information. Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information which disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[55]Pacific Alliance, Article 11.8: "Treatment of certain information. No disposition in this Chapter requires a Party to reveal or allow access to: a. information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or b. any confidential information which disclosure would impede law enforcement or otherwise be contrary to public interest or prejudice legitimate commercial interests of a certain person."

[56]PAN-SIN FTA. Article 11.8: "Treatment of Certain Information Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interests or prejudice legitimate commercial interests of particular enterprises."

[57]PER-KOR FTA, Article 12.7: "Treatment of Certain Information. Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[58]SIN-AUT FTA, Chapter 9, Article 8: "Treatment of Certain Information. Nothing in this Chapter shall require a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[59]USA-BHR FTA, Article 11.7: "Treatment of Certain Information. Article 20.4 (Disclosure of Information) does not apply to this Chapter. Nothing in this Chapter shall be construed to require a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[60]USA-CHI FTA, Article 12.7: "Treatment of Certain Information. Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any

hoeren@uni-muenster.de

(2012),[61] the United States-Morocco FTA (2006),[62] the United States-Oman FTA (2009),[63] the United States-Panama FTA (2012),[64] the United States-Peru FTA (2009),[65] and the United States-Singapore FTA (2003).[66]

The China-Korea FTA (2015) does not explicitly include the protection of legal persons' data, although "individual customers" potentially can be construed as including these entities, as long as the expression "personal data" is not used to qualify the information.[67] The EU-Canada CETA uses the term "individual consumers" and complements it with "cross-border financial service suppliers, financial

confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[61]USA-COL FTA, Article 12.7: "Treatment of Certain Information. Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[62]USA-MOR FTA, Article 12.7: "Treatment of Certain Information. Article 12.5 (Disclosure of Information) does not apply to this Chapter. Nothing in this Chapter shall be construed to require a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[63]USA-OMA FTA, Article 12.7: "Treatment of Certain Information. Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[64]USA-PAN FTA, Article 12.7: "Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[65]USA-PER FTA, Article 12.7: "Treatment of Certain Information. Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[66]USA-SIN FTA, Article 10.7: "Treatment of Certain Information. Nothing in this Chapter requires a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; or (b) any confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest or prejudice legitimate commercial interests of particular enterprises."

[67]CHI-KOR FTA, Chapter 9, Article 9.4: "Treatment of certain information. Nothing in this Chapter shall be construed to require a Party to disclose information relating to the affairs and accounts of individual customers or any confidential or proprietary information in the possession of public entities." It is important to stress that the "personal information" is the expression employed in Chapter 13—Electronic Commerce—on the issue of data protection.

hoeren@uni-muenster.de

institutions [and] (. . .) particular enterprises".[68] The Korea-Australia FTA (2014),[69] the Malaysia-Australia FTA (2013)[70] and the United States-Australia FTA (2005)[71] treat information of "individual customers" in a similar way. The Korea-Singapore FTA (2006) protects "confidential information" related to "legitimate commercial interests of particular enterprises, public or private" with no special reference to individuals or natural persons.[72] Also the EU-Chile FTA (2005)[73] provides for the protection of confidential information, although not identifying "personal data" or natural persons.

The Hong Kong-New Zealand FTA (2011) does protect privacy in general provisions, which covers the whole agreement and not only the Financial Services norms. It does not, however, refer to "data protection" or "personal data".[74]

[68]EU-CAN CETA Chapter 13, Article 13.17 (2): "This Agreement does not require a Party to furnish or allow access to information relating to the affairs and accounts of individual consumers, cross-border financial service suppliers, financial institutions, or to any confidential information which, if disclosed, would interfere with specific regulatory, supervisory, or law enforcement matters, or would otherwise be contrary to public interest or prejudice legitimate commercial interests of particular enterprises."

[69]KOR-AUT FTA, Article 8.7: "Treatment of Certain Information. Further to Article 22.4 (Disclosure of Information), nothing in this Chapter requires a Party to furnish or allow access to information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers."

[70]MAL-AUT FTA, Annex on Financial Services, Article 5 (3): "Prudential and Regulatory Supervision. (. . .) 3. Nothing in this Agreement shall be construed to require a Party to disclose information relating to the affairs and accounts of individual customers or any confidential or proprietary information in the possession of public entities."

[71]USA-AUT FTA, Article 13.7: "Treatment of Certain Information. Nothing in this Chapter requires a Party to furnish or allow access to information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers."

[72]KOR-SIN FTA, Article 12.8: "Treatment of certain information. Nothing in this Chapter shall require a Party to furnish confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest, or which would prejudice legitimate commercial interests of particular enterprises, public or private."

[73]EU-CHI FTA, Article 124: "Nothing in this Chapter: (a) shall require any of the Parties to provide confidential information, the disclosure of which would impede law enforcement, or otherwise be contrary to the public interest, or which would prejudice legitimate commercial interests of particular enterprises, public or private. (b) shall be construed to require a Party to disclose information relating to the financial affairs and accounts of individual customers of financial service suppliers, or any confidential or proprietary information in the possession of public entities."

[74]HKG-NZL, Article 18.2 (a): "Disclosure of information. Nothing in this Agreement shall be construed to require either Party to furnish or allow access to information the disclosure of which it considers: 28 In the case of New Zealand, references to local governments and authorities include regional government and authorities. 272 (a) would be contrary to any of its domestic law, including those protecting personal privacy or the financial affairs and accounts of individual customers of financial institutions;"

hoeren@uni-muenster.de

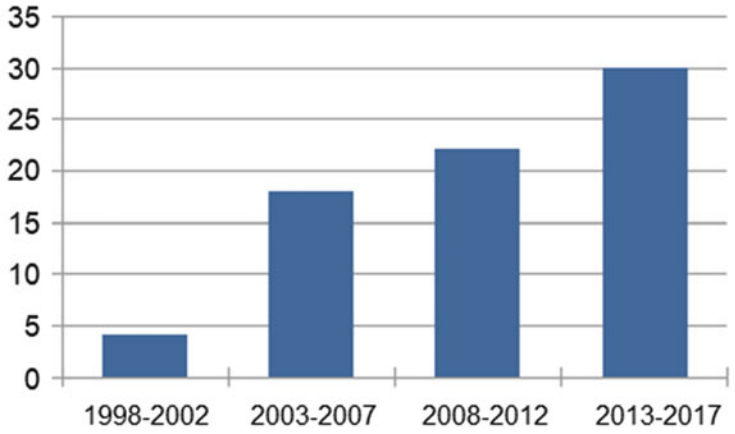

Fig. 1 By the author

8 E-Commerce on Regional and Bilateral Trade Agreements

The WTO informs the existence of 284 regional trade agreements (RTAs) in force by the end of 2017.[75] From these, 75 hold provisions on e-commerce (67 of which on goods and services, 7 on goods and 1 on services). 70 of them entered into force from 2003 onwards.[76] This section analyses the e-commerce provisions on data protection in all these agreements.

8.1 RTAs with E-Commerce Rules (1998–2017)

The general structure of a chapter on e-commerce includes (a) hortatory rules on cooperation, (b) liberalisation rules, that forbid import or export tariffs to goods delivered electronically, which, nevertheless, may be internally taxed, (c) rules on paperless transactions and certification and, in many instances (d) personal data protection rules (Fig. 1).

The Australia-Singapore FTA (2017)[77] holds a detailed disposition on "personal information protection" in which Parties (a) recognise the need to protect data in

[75]Data in http://rtais.wto.org/UI/publicsummarytable.aspx, consulted on 21st January 2018.

[76]Data in the WTO website, consulted on 21st January 2018.

[77]SIN-AUT FTA (2017), Chapter 14, Article 9: "Personal Data Protection. Personal Information Protection 1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce. 2. To this end, each Party shall adopt or maintain a

hoeren@uni-muenster.de

order to enhance confidence in electronic commerce, (b) accept the duty to adopt or maintain a legal framework, (c) accept that the Parties will take into account rules from international bodies to set their legal frameworks, (d) accept that domestic practices shall be non-discriminatory, (e) are obliged to publish information on remedies and legal requirements, (f) recognise different legal approaches, (f) recognise the advantages of the compatibility between domestic systems, (h) recognise the need of cooperation to establish compatible legal systems, (i) recognise that regulatory jurisdiction on transfer of information belong to the Parties, (j) accept the obligation to allow cross-border transfer of information, including personal data, (k) keep policy space to the adoption of measures for legitimate public policy objective, and (l) do not admit the use of policy space to "arbitrary or unjustifiable discrimination or a disguised restriction to trade" or disproportional to the purpose of the policy.

The Mexico-Panama FTA (2015) regulates the personal data protection through the obligation to endeavour the creation and maintenance of legal rules on data protection observing the "international practice" (*"tomarán en consideración las prácticas internacionales"*). It also includes in the chapter on electronic commerce a provision on the cross-border flow of information that, nevertheless, is somehow vague, since the obligation to allow the transmission is accompanied by a loose reference to the "applicable law" that specifies no connecting criterion and a

---

legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies. (∗) 3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction. 4. Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how: (a) an individual can pursue remedies; and (b) business can comply with any legal requirements. 5. Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them (∗) [footnote] For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy." Article 13: "Cross-Border Transfer of Information by Electronic Means. 1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means. 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective."

hoeren@uni-muenster.de

hortatory disposition on "international standards".[78] The Pacific Alliance (2016)[79] does regulate the protection of personal data, by setting the obligation to adopt or maintain legal and administrative protection of personal data and taking into account the international standards. In a separate Article, its chapter on electronic commerce deals very loosely with the issue of cross-border data transfer, keeping the issue open to future negotiations.

The EU-Central America FTA (2013),[80] the EU-Colombia, Peru and Ecuador FTA (2013),[81] the EU-Georgia (2014),[82] the EU-Korea (2011),[83] the EU-Moldova (2014),[84] the EU-Ukraine (2014)[85] do not set a duty to regulate data protection domestically, although the admit that the compatibility with "international standards" is necessary in order to increase confidence of e-commerce.

[78]MEX-PAN FTA, Article 14.8: "Personal data protection. The Parties shall endeavour to adopt or maintain legislation and regulation to the protection of personal data from the electronic commerce users. The Parties will consider the international practice in this issue." (My translation.) Article 14.10 "International Flow of Information. Each Party will allow their persons and the persons from the other Party to transfer electronic information into and out its territory, whenever it is requested by this person, accordingly to the applicable law on protection of personal data and taking into consideration the international practice." (My translation.)

[79]Pacific Alliance. Chapter 13, Article 13.8: "Protection of Personal Information. 1. The Parties shall adopt or maintain legislation, regulation or administrative measures to the protection of personal information of users that take part in the electronic commerce. 2. The Parties shall exchange information and experiences in regard to their legislation on personal data protection." (My translation.) Article 13.11: "Cross-border Information Flow. With the aim of deepening their relations in the field of electronic commerce, the Parties admit to endeavour the future negotiation of commitments related to the cross-border flow of information."

[80]EU-Central America FTA, Title III, Chapter 6, Article 201 (2): "Objective and Principles. 2. The Parties recognise that the development of e-commerce shall be compatible with international standards of data protection, in order to ensure the confidence of users of ecommerce."

[81]EU-COL, PER, ECU FTA, Chapter 6, Article 162 (2): "The Parties agree that the development of electronic commerce shall be consistent with the international standards of data protection, in order to ensure the confidence of users of electronic commerce."

[82]EU-GEO, Article 127 (2): "Objective and principles. (. . .) 2. The Parties agree that the development of electronic commerce must be compatible with the international standards of data protection in order to ensure the confidence of users of electronic commerce."

[83]EU-KOR FTA, Article 7.48 (2): "Objectives and principles. (. . .) 2. The Parties agree that the development of electronic commerce must be fully compatible with the international standards of data protection, in order to ensure the confidence of users of electronic commerce."

[84]EU-Moldova FTA, Article 254 (2): "Objective and principles. (. . .) 2. The Parties agree that the development of electronic commerce must be fully compatible with the highest international standards of data protection, in order to ensure the confidence of users of electronic commerce."

[85]EU-Ukraine FTA, Article 139 (2): "Objective and principles. (. . .) 2. The Parties agree that the development of electronic commerce must be fully compatible with the highest international standards of data protection, in order to ensure the confidence of users of electronic commerce."

hoeren@uni-muenster.de

Chapter 10 of the ASEAN-AUT-NZL FTA (2010), on e-commerce, deals with data protection in its Article 7.[86] According to it, Parties hold the jurisdiction to legislate and shall regulate data protection. There is a hortatory provision in favour of international standards. This is also the case of the Australia-Chile FTA (2009),[87] the Australia-China FTA (2015),[88] the Canada-Korea FTA (2015),[89] the Chile-Thailand FTA (2015),[90] the China-Korea FTA (2015),[91] the Costa Rica-Colombia FTA (2016),[92] the EU-Canada CETA (2017),[93] the EU-CARIFORUM FTA

[86]ASEAN-AUT-NZL FTA, Chapter 10, Article 7: "1. Subject to Paragraph 2, each Party shall, in a manner it considers appropriate, protect the personal data of the users of electronic commerce. 2. A Party shall not be obliged to apply Paragraph 1 before the date on which that Party enacts domestic laws or regulations to protect the personal data of electronic commerce users. 3. In the development of data protection standards, each Party shall consider the international standards and criteria of relevant international organisations."

[87]AUT-CHI FTA, Article 16.8: "Online Personal Data Protection Each Party shall adopt or maintain a domestic legal framework which ensures the protection of the personal data of the users of electronic commerce. In the development of personal data protection standards, each Party shall take into account the international standards and criteria of relevant international bodies."

[88]AUT-CHN FTA, Chapter 12, Article 12.8: "1. Notwithstanding the differences in existing systems for personal information protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal information of users of electronic commerce. 2. In the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organisations."

[89]CAN-KOR FTA, Chapter 13, Article 13.4: "Protection of Personal Information. Each Party shall adopt or maintain measures for the protection of the personal information of the users of electronic commerce. In the development of personal information protection standards, each Party shall take into account international standards of relevant international organisations."

[90]CHI-THA FTA, Article 11.7 (1) (j) (Electronic Commerce): "1. Recognizing the global nature of electronic commerce, the Parties shall endeavour to: (. . .) (j) take appropriate measures and take into account international standards on personal data protection: (i) notwithstanding the differences in existing systems for personal data protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal data of users of electronic commerce; and (ii) in the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organizations."

[91]CHI-KOR FTA, Chapter 13, Article 13.5: "Protection of Personal Information in Electronic Commerce: Recognizing the importance of protecting personal information in electronic commerce, each Party shall adopt or maintain measures which ensure the protection of the personal information of the users of electronic commerce and share information and experience on the protection of personal information in electronic commerce."

[92]CTR-COL FTA, Chapter 16, Article 16.6: "Protection of personal information. 1. Each Party shall adopt or maintain regulation or administrative measures to protect personal information of users that take part in electronic commerce. The Parties may take into account international rules and criteria of international organisations on this issue. 2. The Parties will endeavour their best efforts to exchange information and experiences on domestic regimes of personal data protection." (My translation.)

[93]UE-CAN CETA, Chapter 16, Article 16.4: "Trust and confidence in electronic commerce. Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into

hoeren@uni-muenster.de

(2008),[94] the Hong Kong-New Zealand FTA (2011),[95] the Japan Australia FTA (2015),[96] the Korea-Colombia FTA (2016),[97] the Korea-Australia FTA (2014),[98] the Korea-Vietnam FTA (2015),[99] the Malaysia-Australia FTA

due consideration international standards of data protection of relevant international organisations of which both Parties are a member."

[94]EU-CARIFORUM FTA, Article 119 (2): "Objective and principles 2. The Parties agree that the development of electronic commerce must be fully compatible with the highest international standards of data protection, in order to ensure the confidence of users of electronic commerce."

[95]HKG-NZL FTA, Article 10.2 (1) (b) (c) (f) (i): "1. The Parties agree to: (. . .) (b) promote the efficient functioning of E-commerce domestically and internationally by, wherever possible, developing domestic regulatory frameworks which are open, avoiding undue restrictions and costs on E-commerce and, as appropriate, ensuring that relevant processes are compatible with evolving international norms and practices; (c) ensure a predictable and simple legal environment for E-commerce, taking into account the UNCITRAL Model Law on Electronic Commerce 1996 and other model law(s) on E-commerce as may be adopted or revised by UNCITRAL or other such international organisations from time to time, that supports the maintenance of a secure infrastructure, enables public key infrastructure solutions to develop, and includes laws to facilitate the use of electronic methods in meeting statutory requirements; (. . .) (f) work to build consumer and business confidence to support the fullest economic and social benefits from E-commerce by: (i) maintaining privacy protection laws and consumer laws relating to E-commerce."

[96]JPN-AUT FTA, Article 13.8: "Personal Data Protection. 1. Each Party shall adopt or maintain measures to protect the personal data of electronic commerce users. 2. In the development of protection standards for the personal data of electronic commerce users, each Party shall take into account relevant international standards and criteria of relevant international bodies."

[97]KOR-COL FTA, Article 12.3: "Online Personal Data Protection. Each Party shall adopt or maintain measures which ensure the protection of the personal data of the users of electronic commerce. In the development of personal data protection standards, each Party shall take into account international standards and the criteria of relevant international organizations." Article 12.6: "Cooperation. 1. The Parties shall endeavour to establish cooperation mechanisms on issues arising from electronic commerce, which will, *inter alia*, address the following: (. . .) (b) the protection of personal data;"

[98]KOR-AUT FTA, Article 15.8: "Online Personal Data Protection. Each Party shall adopt or maintain measures which ensure the protection of the personal data of the users of electronic commerce. In the development of personal data protection standards, each Party shall take into account the international standards, guidelines and recommendations of relevant international organisations."

[99]KOR-VNM FTA, Article 10.6: "Personal data protection. 1. Each Party shall endeavour to adopt or maintain legislative measures which ensure the protection of the personal data of the users of electronic commerce. In the development of personal data protection standards in electronic commerce, each Party recognizes the importance of taking into account the international standards and the criteria of relevant international organizations. 2. Each Party recognizes the necessity of taking an adequate level of safeguards for the protection of personal data of the users of electronic commerce that is transferred between the Parties."

hoeren@uni-muenster.de

(2013),[100] the Thailand-Australia FTA (2005)[101], and the Thailand-New Zealand FTA (2005).[102]

The Canada-Peru FTA (2009)[103] and Canada-Colombia FTA (2011)[104] provide that Parties "should" regulate the protection of personal data, although there are no indications of international standards as a general parameter. The Eurasian Economic Union-Vietnam FTA (2016)[105] also employs the weak expression "shall endeavour" and does not link data protection to any standards, international or domestic.

[100]MAL-AUT FTA, Article 15.8: "Online Personal Data Protection. 1. Each Party shall establish or maintain legislation or regulations that protect the personal data of the users of electronic commerce. 2. In the development of personal data protection standards, each Party shall take into account the international standards and criteria of relevant international organisations."

[101]THA-AUT FTA, Chapter 11, Article 1106: "Online Personal Data Protection. 1. Notwithstanding the differences in existing systems for personal data protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal data of users of electronic commerce. 2. In the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organisations."

[102]THA-NZL FAT, Article 10.5: "Online Data Protection. 1. Notwithstanding the differences in existing systems for personal data protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal data of users of electronic commerce. 2. In the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organisations."

[103]CAN-PER FTA, Chapter 15, Article 1507: "The Parties recognize the importance of the protection of personal information in the on-line environment. To this end, each Party should: adopt or maintain legal, regulatory and administrative measures for the protection of personal information of users engaged in electronic commerce; and exchange information and experiences regarding their domestic regimes on the protection of personal information."

[104]CAN-COL FTA, Chapter 15, Article 1506: "Protection of Personal Information 1. Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce. 2. The Parties should exchange information and experiences regarding their domestic regimes for the protection of personal information."

[105]EAEU-Vietnam FTA, Article 13.5: "The Parties shall endeavour to adopt and maintain in force measures aimed at the protection of private data of electronic commerce users." Article 13.6 (1): "Cooperation on Electronic Technologies in Trade. The Parties shall exchange information and experience with regard to laws and regulations and programmes in the field of electronic technologies in trade, in particular with regard to private data protection and improvement of consumer confidence".

hoeren@uni-muenster.de

The Japan-Switzerland FTA (2009)[106] and Japan-Mongolia FTA (2016),[107] in their chapters on electronic commerce, set no separate rules on data protection, although they include the issue in the articles on consumers' protection and cooperation.

Another group of agreements does not provide for any specific duty related to data protection, although it recognizes it as a topic for cooperation between the Parties. This is the case of the Canada-Honduras FTA (2014),[108] the Chile-Colombia FTA (2009),[109] the Colombia-Northern Triangle (2009),[110] the CAFTA-Dominican Republic (2006),[111] the Mexico-Central America (2012),[112] the Nicaragua-Chinese

[106]JPN-SWI FTA, Article 80: "Protection of Online Consumers. 3. The Parties recognise the importance of: (a) adopting or maintaining measures, in accordance with their respective laws and regulations, to protect the personal data of electronic commerce users; and (b) taking international standards and criteria into account in developing such measures." Article 82: "Cooperation (. . .) 2. The Parties shall endeavour to share information and experiences, including on related laws, regulations and best practices in the field of electronic commerce in relation to, *inter alia*: (a) data privacy;"

[107]JPN-MNG FTA, Article 9.6 (3): "Consumer Protection. 3. The Parties shall adopt or maintain measures in accordance to their respective laws and regulations, to protect the personal data of electronic commerce users"; Article 9.12 (2) "Cooperation. (. . .) 2. The parties shall, where appropriate, share information and experiences, including on related laws, regulations and best practices with respect to electronic commerce, related to, *inter alia*, (. . .) personal data protection."

[108]CAN-HON FTA, Chapter 16, Article 16.5: "Cooperation: Recognizing the global nature of electronic commerce, the Parties affirm the importance of: (. . .) (b) sharing information and experiences on laws, regulations, and programs involving electronic commerce, including those related to data privacy, consumer confidence, security in electronic communications, authentication, intellectual property rights, and electronic government; (c) working to maintain cross-border flows of information as an essential element in fostering a vibrant environment for electronic commerce . . ."

[109]CHI-COL FTA, Chapter 12, Article 12.5(b): "Taking into account the global nature of electronic commerce, the Parties recognize the importance of: (b) share information and experience about statutes, regulation and programs on electronic commerce, including in reference to data privacy, confidence of the consumers, cybernetic security, electronic signature, intellectual property rights and electronic government." (My translation.)

[110]COL-Northern Triangle, Chapter 14, Article 14.8(b): "Taking into account the global nature of electronic commerce, the Parties recognize the importance of: (b) share information and experience about statutes, regulation and programs on electronic commerce, including in reference to data privacy, confidence of the consumers, cybernetic security, electronic signature, intellectual property rights and electronic government." (My translation.)

[111]CAFTA-DR FTA, Chapter 14, Article 14.5(b): "Cooperation. Recognizing the global nature of electronic commerce, the Parties affirm the importance of: (. . .) (b) sharing information and experiences on laws, regulations, and programs in the sphere of electronic commerce, including those related to data privacy, consumer confidence in electronic commerce, cyber-security, electronic signatures, intellectual property rights, and electronic government."

[112]MEX-Central America, Article 15.5: "Cooperation. The Parties recognise the importance of the implementation of programs that promote electronic commerce, which focuses the following activities: (. . .) (b) share information and experiences on statutes, regulation and programs in the field of electronic commerce, including those related to data privacy, consumers' confidence in electronic commerce, cybernetic safety, electronic signatures, intellectual property rights and electronic governance;" (My translation.)

hoeren@uni-muenster.de

Taipei Cooperation Agreement (2008),[113] the Panama-Singapore FTA (2006),[114] the Peru-Korea FTA (2011),[115] the Singapore-Chinese Taipei FTA (2014),[116] the United States-Chile FTA (2004),[117] and the United States-Panama FTA (2012).[118] Although the UE-Canada CETA (2017) deals with data protection in other provisions, it also includes the issue of personal data protection, extended to legal persons, in the Article 16.6 (1) (c, d).

Another group of agreements also expresses the concerns on data protection in a general clause, although they recognise explicitly the functional relation between the reliance on e-commerce and effective instruments of data protection. This is the case of EFTA-Central America FTA (2014),[119] the EFTA-Colombia FTA (2011),[120] the

[113]NIC-TWN FTA, Article 14.05: "Cooperation. Recognizing the global nature of electronic commerce, the Parties affirm the importance of: (. . .) (b) sharing information and experiences on laws, regulations, and programs in the sphere of electronic commerce, including those related to data privacy, consumer confidence in electronic commerce, cyber-security, electronic signatures, intellectual property rights, and electronic government."

[114]PAN-SIN FTA. Article 13.4: "Cooperation Recognizing the global nature of electronic commerce, the Parties affirm the importance of: (. . .) (b) sharing information and experiences on issues in the sphere of electronic commerce, including those related to data privacy, consumer confidence in electronic commerce, cyber-security, electronic signatures, intellectual property rights, and electronic government;"

[115]PER-KOR FTA, Article 14.9: "Cooperation. Recognizing the global nature of electronic commerce, the Parties commit to: (. . .) (b) sharing information and experiences on laws, regulations, and programs in the area of electronic commerce, including those related to data privacy, consumer confidence, security in electronic communications, authentication, intellectual property rights, and electronic government;"

[116]SIN-TWN FTA, Article 11.47: "Cooperation. Recognising the global nature of electronic commerce, the Parties affirm the importance of: (. . .) (b) sharing information and experiences on laws, regulations, and programs in the sphere of electronic commerce, including those related to data privacy, consumer protection and promoting confidence in electronic commerce and electronic signatures;"

[117]USA-CHI FTA, Article 15.5: "Cooperation. Having in mind the global nature of electronic commerce, the Parties recognize the importance of: (. . .) (b) sharing information and experiences on regulations, laws, and programs in the sphere of electronic commerce, including those related to data privacy, consumer confidence, cyber-security, electronic signatures, intellectual property rights, and electronic government;"

[118]USA-PAN FTA, Article 14.5: "Cooperation. Recognizing the global nature of electronic commerce, the Parties affirm the importance of: (. . .); (b) sharing information and experiences on laws, regulations, and programs in the sphere of electronic commerce, including those related to data privacy, consumer confidence in electronic commerce, cyber-security, electronic signatures, intellectual property rights, and electronic government;"

[119]EFTA-CA FTA, Annex II, Article 1, (c) (i, ii): "General. The Parties recognise: (. . .) (c) the need to create an environment of trust and confidence for users of electronic commerce which covers, *inter alia*: (i) protection of privacy of individuals in relation to the processing and dissemination of personal data; (ii) protection of confidentiality of individual records and accounts."

[120]EFTA-COL FTA, Annex I, Article 1 (c) (i, ii): "General. The Parties recognise: (. . .) (c) the need to create an environment of trust and confidence for users of electronic commerce which covers, *inter alia*: (i) protection of privacy of individuals in relation to the processing and dissemination of personal data; (ii) protection of confidentiality of individual records and accounts."

hoeren@uni-muenster.de

EFTA-Peru FTA (2011),[121] and the New Zealand-Chinese Taipei (2013).[122] The EU-Canada CETA (2017) denominates its Article 16.4, on the protection of personal data, "trust and confidence in electronic commerce" and, therefore, confirms the function of the related measures. The EU-CARIFORUM (2008), the EU-Colombia, Peru and Ecuador (2013), the EU-Georgia FTA (2014), the EU-Korea FTA (2011), the Hong Kong-New Zealand FTA (2011), and the Panama-Singapore FTA (2006) also admit the need of data protection to increase confidence.

The Canada-Costa Rica FTA (2002), the Canada-Jordan FTA (2012), the Canada-Panama FTA (2013), the Canada-Ukraine FTA (2017), the Costa Rica-Singapore FTA (2013), the Gulf Cooperation Council-Singapore (2013), the India-China CECA (2005), the Jordan-Singapore (2005), the Korea-Singapore FTA (2006), the Peru-Singapore FTA (2009), the Turkey-Malaysia FTA (2015), the United States-Australia FTA (2005), the Korea-United States FTA (2012),[123] the United States-Bahrain FTA (2006), the United States-Colombia FTA (Ch. 15) (2012), the United States-Morocco FTA (Ch. 14) (2006), the United States-Oman FTA (Ch. 14) (2009), the States-Peru FTA (Ch. 15) (2009) and the United States-Singapore FTA (Ch. 14) (2003) do not hold provisions that link e-commerce to personal data protection.

The China Mainland and Hong Kong Closer Partnership Arrangement and the China Mainland and Macao Closer Partnership Arrangement (both of 2003) hold, in identical texts, contained in their Articles 17, only hortatory provisions on cooperation in the field of "electronic business". The Economic Agreement Between the Gulf Cooperation Council States (2003) also limits itself to a simple non binding provision on cooperation in its chapter on Transportation, Communication and Infrastructure.[124]

[121] EFTA-PER FTA, Annex I, Article 1 (c) (i, ii): "General. The Parties recognise: (. . .) (c) the need to create an environment of trust and confidence for users of electronic commerce which covers, *inter alia*: (i) protection of privacy of individuals in relation to the processing and dissemination of personal data; (ii) protection of confidentiality of individual records and accounts."

[122] NZL-TWN Cooperation Agreement, Chapter 9, Article 2: "Promotion of E-Commerce. The Parties agree to: (. . .) (d) work to build consumer and business confidence in support of the wider utilisation of e-commerce between the Parties and globally by: (i) maintaining privacy protection laws and consumer laws relating to e-commerce;"

[123] KOR-USA FTA, Article 15.8: "Cross-border information flows. Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavour to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."

[124] GCC EA, Article 25: "Member States shall take all necessary actions to facilitate banking and trade exchange through electronic means of communication, and unify their electronic commerce legislation."

hoeren@uni-muenster.de

9 Discussion

From a very general perspective, it is possible to distribute the data protection aspects of trade agreements into three groups roughly linked to patterns fostered by the major players of the international economic and legal overlapping arenas: (a) the European group, focusing on the protection of personal data as a fundamental right and interest in spread worldwide the high standards adopted within the EU; (b) the American group, focusing on freedom of trade, regarding privacy issues as something to be dealt with private regulation and market; and (c) the less radical options in agreements among other players, especially Latin American and Pacific basin countries.

An imaginary *ideal* European agreement would reinforce the internal standards of the EU in international instruments that effectively oblige the other Parties. Not surprisingly, it is the case of the EEA, since EFTA Members reproduce in their internal law not only the original standards from the time of the Agreement, but they also incorporate virtually all new changes set by European decisions, directives and regulations.

Recent European agreements, such as the EU-CAN CETA (2017) and the EU Agreements signed in 2014, use a general exception for key chapters (cross-border services, financial services, entry and stay of persons, maritime transports, telecommunications, electronic commerce, investments etc.). This makes it very clear that domestic privacy protection rules that affect trade flows are, *prima facie*, legitimate and cannot be considered as a breach of the treaties *unless* they are "means of arbitrary or unjustifiable discrimination" or "a disguised restriction".

American agreements also protect the domestic jurisdiction on issues related to data protection and privacy. Most of the United States treaties' texts fail to make an express reference to privacy or data protection either in their chapters on electronic commerce, or in any other specific chapter or section. Therefore, whenever measures on protection of personal data do affect trade, they are supposed to be evaluated by regular standards, with no special status.

Other agreements vary between the European and American poles, but except for a handful, they do not address the issue. There are no special cases that propose substantially differential solutions.

In the three studied dimensions—special section, financial services and electronic commerce—the presence of a separate chapter or isolated reference to personal data protection standards is specific to European texts. Financial services are regulated in very similar ways throughout the whole sample. Electronic commerce presents the highest variance of dispositions and tried solutions, as it is to be described in the sessions below.

hoeren@uni-muenster.de

9.1 Chapters and Annexes on Data Protection

From the sample under analysis, a rather narrow set of agreements presents explicit references to European standards on data protection. The EEA incorporates virtually all EU rules on the issue and made continuous efforts to keep apace with the whole regime in order to achieve a quite integrated market. The EU-CARIFORUM Agreement, albeit being the only instance in the sample, incorporates a complete chapter that repeats most of the European minimum protection standards. The EU-Moldova and EU-Ukraine agreements make references to EU legislation.

Agreements among non-European countries obviously make no such link, but it is necessary to stress that the general reference to "international standards", sometimes made more specific through the indication of the UNCITRAL Model Law on Electronic Commerce (1996) or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), are always hortatory and are set in the chapters on electronic commerce, not in general provisions.

It is difficult to generalise a pattern from such a narrow set of cases, each of which presenting different solutions, both formally and materially. Nevertheless, it looks reasonable to expect that agreements with countries that are in a list of possible future EU Members incorporate standards closer to those already in force in the Union.

9.2 Data Access and Transfer in Financial Services Chapters

Chapters on financial services treat data protection in articles on transfer and processing of information and on the treatment of certain information. The first issue is normally addressed by an Article protecting the freedom of trade through the grant of transfer and processing of data necessary and proportional to the service. The second one makes clear that nothing on the liberalisation of financial services may be construed as a means to oblige Parties to allow access to sensitive and confidential information.

The general permission of proportional and purposeful data transfer is adopted in virtually all European treaties under analysis and is quite common in the agreements between Asian and Latin American Countries. Only one American FTA, entered into with Korea, has a provision of this class, although in the minimalist form, as far as data protection is regarded.

Most of these provisions make reference to the "ordinary course of business". However, the wording varies more in other aspects of those provisions, sometimes with significant results. Many treaties with European countries refer not only to personal data, but also to "fundamental rights" and "liberties". These expressions do principiologically link the text to the European approach to the issue, since they stress the dimension of fundamental right protection over the mere trade adjustment necessary, *i.a.*, to enhance the customers' confidence.

hoeren@uni-muenster.de

Many texts refer the risk of using data protection as a measure to protect domestic suppliers. Hence the provisions that make clear that measures in this respect cannot "circumvent" trade liberalisation or be the means of "arbitrary or unjustifiable discrimination". The most complete guarantee of European standards is in the EU-CAN CETA. It sets the obligation of the Parties to "maintain adequate safeguards to protect privacy" (similar dispositions do exist in electronic-commerce chapters). A couple of agreements with no European Parties (MEX-PAN FTA and Pacific Alliance) points to the need of a permission from a regulating authority.

The second kind of rules on data protection in financial services chapters does not reveal a significant variation. In fact, the general treatment of certain information is already made in the GATS, Annex on Financial Services, Article 2. The rule thereby laid down, with more or less changed wording, is repeated in many regional and bilateral agreements with little differences.

9.3 Data Protection Measures and Electronic Commerce

There is a wide variety of provisions on data protection and electronic commerce. It varies from a great deal of chapters with no direct reference to the issue to the quite complete regime of AUT-SIN FTA (2017). From the ten American FTAs under analysis, seven contain no provisions on data protection in their chapters on electronic commerce and the other two (with Chile and Panama) only include it in cooperation issues. The USA-JOR FTA (2001) contains no chapter on the issue and the sole article on the issue does not refer to data protection. Nevertheless, it is necessary to remember that the Trans Pacific Partnership, aborted by the present American Presidency, held a provision thereon.[125]

[125]TTP, Chapter 14, Article 14.8: "Personal Information Protection. 1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce. 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.6 3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction. 4. Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) business can comply with any legal requirements. 5. Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them."

hoeren@uni-muenster.de

In short, it is possible to identify at least 16 dimensions in which some variance is found:

1. The relation with customers' confidence;
2. The relation with fundamental rights and liberties;
3. The express duty to adopt and maintain legal framework and measures;
4. The mandatory reference to international standards;
5. The hortatory reference to international standards;
6. The non-discriminatory nature of the measures;
7. The transparency and notification of domestic rules and measures;
8. The recognition of different legal approaches;
9. The recognition of domestic jurisdiction on the issue;
10. The recognition of advantages of legal harmonisation;
11. The recognition of the need to cooperate to make domestic systems compatible;
12. The definition of the applicable law;
13. The obligation to allow cross-border transfer;
14. The reserve of the domestic policy space on personal data protection;
15. The prohibition of discriminatory measures; and
16. The prohibition of disproportional measures.

The relation between all dimensions in the analysed agreements is, so far, not conclusive, except insofar as Europeans lean towards stronger protection of personal data, probably as a strategy in order to prevent future breaches of liberalisation duties under trade agreements.

It seems that provisions on data protection are spreading to other chapters, notably on investment, cross-border services and movement of natural persons. Nevertheless, since this study focuses on agreements with electronic commerce chapters, further research would be necessary to confirm this.

10 Conclusions

Since data protection became an important instrument to secure privacy and liberties in contemporary societies, in which internet and electronic means of data storage and circulation are pervasive, international trade relations and their legal framework also are supposed to keep this issue in mind.

The present report focused on the rules on data protection contained in trade agreements, particularly in chapters dealing with electronic commerce. Internet is a preferential space for many transactions, not only on electronic goods and related services, but also in more traditional areas, such as trade of goods and consumer sales. Payments and their security also happen very often with the cross-border circulation of data necessary to the clearing and transference of values. Therefore, the control of data flows may have a heavy and deep effect on the worldwide flow of wealth. That is the main reason why data protection and international trade should be studied in tandem.

hoeren@uni-muenster.de

Beyond the general WTO rules, a set of 75 agreements was used in the search for provisions on personal data protection, notably those contained in their general chapters, or in provisions on financial services and electronic commerce. The results points to an unfinished picture.

As a matter of fact, general chapters are odd and concentrated on agreements with European countries. Consequently, their purpose is not very clear beyond the foreseeable enlargement of European legal and economic influence zone to eastern countries. Nevertheless, some general provisions on the issue, as well as the fact that it is addressed in chapters on investment, free movement of persons and cross-border services, suggest that a possible development of increasingly complex agreements could be to isolate these provisions in general chapters on exceptions and on fundamental rights and duties.

The rules on financial services point at some stability, since the provisions on the transfer and processing of information, as well as on the protection of certain information, are very repetitive. However, there is a handful of innovations that could have some impact on the design of similar dispositions in general or regarding other cross-border services.

The treatment of electronic commerce is far richer. The many dimensions and differences of treatments both regionally and chronologically suggest the need for further debate in multilateral fora. United Nations commissions and conferences, such as UNCITRAL and UNCTAD, could be good places to debate the issue, as well as WTO and OECD.

Regarding the formal aspect of legal protection of personal data, there are two possible radical approaches: the complete prevalence of domestic jurisdiction or the predominance of international standards. The actual solutions are in the middle. The agreements generally secure the application of reasonable and proportional domestic regulation and measures on data protection, although they do not admit it as a means to unduly discriminate or close markets. In other words, there is no agreement that regards the domestic jurisdiction on data protection, as well as on any other right, as absolute and unchallengeable. There are limits set by the treaties in two ways: (a) open principles and standards set by the own treaty or (b) reference to external standards, namely international (UNCITRAL, OCDE etc.) or European (Council of Europe, EU).

This formal approach is also reflected in the possible paths of substantive rules. As a matter of fact, due to many reasons not under discussion in this report, European regulation is quite complete and complex and, due to the intricate processes of decision making, difficult to change. Therefore, Europeans are concerned with the maintenance and the dissemination of their own standards. The United States have no such complex set of rules and resist laying it down, though the adoption of the EU-US Privacy Shield in 2016 and, formerly, the safe harbour principles, show the wilfulness to agree upon a common basis with the EU.

The analysis of international trade agreements evidences the advantages and a possible need for common efforts of harmonisation and unification of legal standards on personal data protection. It also clarifies that economic agreements may encourage the adoption of domestic legislation and administrative measures that prevent a race to the bottom and help disseminating higher standards of personal rights protection.

hoeren@uni-muenster.de

UN Regulations

Thomas Hoeren

1 General Data Protection Framework

1.1 Legislation and Relevant Case Law

Within the legal framework of international law, a wide variety of legislation and standards are applicable regarding personal data protection. United Nations and other subjects of international law like the Council of Europe (CoE), the OECD, ECOWAS or APEC need to be considered. Due to the variety, the distinction between the scopes of application for each corpus of legislation is vital.

One of the most important and greatest influences can be drawn back to the Guidelines for the Regulation of Computerized Personal Data Files. They cannot be considered legislation in a legal sense, but rather as recommendations.[1] The guidelines were adopted by the General Assembly resolution 45/95 on the 14th of December 1990. Procedures for implementing the guidelines are explicitly left to the initiative of each member state. The draft is subdivided in two chapters. The first one proclaims principles concerning the minimum guarantees that should be provided in national legislation. The second subdivision states the application of the guidelines kept by governmental international organizations.

Furthermore on UN level, article 12 Universal Declaration of Human Rights (UDHR) and article 17 of the International Covenant on Social and Political Rights (ICCPR) promote the protection of privacy.

[1] Burkert (2003), p. 100.

T. Hoeren (✉)
University of Münster, Münster, Germany
e-mail: Hoeren@uni-muenster.de

© Springer Nature Switzerland AG 2020

D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law 38,
https://doi.org/10.1007/978-3-030-28049-9_20

hoeren@uni-muenster.de

Due to the fact that the International Court of Justice (ICJ) is the only court within the United Nations legal system and focuses on interstate conflicts, no relevant case law dealing with data protection law in the proper sense exists. Nevertheless, national courts and international courts are aware of UN data protection law. For example, the Spanish Constitutional Court drew attention to the aforementioned UN Guidelines in its ruling that shaped the right to data protection as a fundamental right.[2] The European Court of Human Rights (ECHR) mentioned the UN Guidelines in its *Bărbulescu* judgment, too.[3]

New political awareness was raised with the release of resolution 68/167 in 2013, which discusses the right to privacy in the digital age. In the end of 2014, the UN General Assembly released Resolution 69/166 that made clear, rights were the same online and offline.[4] The United Nations Human Rights Council appointed a Special Rapporteur on the right to privacy in 2015. In March 2016, he presented his first annual report to the council.[5] The right to privacy in the digital age is also discussed by Resolution 71/199 of 19 December 2016 and, *inter alia*, by the United Nations Human Rights Council Resolution 34/7 of 23 March 2017. A single international data privacy regulatory framework is yet to be seen.[6] Nevertheless, legal scholars have identified the need for such a framework.[7] The call for a global framework does not come surprisingly as the data protection regulation on UN level has been described as "normatively inferior, highly fragmented, and devoid of clear institutional arrangements so as to serve as a reliable source of international digital privacy protection".[8]

The United Nations legal framework is accompanied by sector-specific guidelines and policies that address particular fields of UN activities such as the "Policy on the Protection of Personal Data of Persons of Concern to UNHCR" for the United Nations High Commissioner for Refugees. Its purpose is to ensure that UNHCR processes personal data in a way that is consistent with the 1990 UN General Assembly's Guidelines for the Regulation of Computerized Personal Data Files.

One could also mention the protection of personal and family privacy under the United Nations Convention on the Rights of Persons with Disabilities (CRPD). Article 22 of the CRPD has been inspired by the aforementioned provisions of the ICCPR and other privacy protection rules on UN level such as the Convention on the Rights of the Child and the Convention on Migrant Workers.[9]

[2] Yilma (2018), p. 10.

[3] Yilma (2018), p. 14 referencing judgment of the ECHR of 5 September 2017, application no. 61496/08, Bărbulescu v. Romania.

[4] Rotenberg (2017), p. 51.

[5] Available at: http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc.

[6] Bennett and Raab (2006), note 6, p. 295; see also Raab and Koops (2009), note 14, p. 209.

[7] Corley (2016), pp. 770 f. and 778.

[8] Yilma (2018), p. 1.

[9] Weber (2017), p. 2.

hoeren@uni-muenster.de

On UN level, there are also soft law instruments regarding data privacy.[10] These include the "UN Fundamental Principles of Official Statistics" and "The UN Principles and Guidelines on Access to Legal Aid in Criminal Justice Systems", but also instruments of specialized agencies of the UN. Namely, those are the United Nations Educational Science and Cultural Organization (UNESCO), International Labour Organization (ILO), International Organization for Migration (IOM) and the World Food Programme (WFP).[11]

Further regulation on supranational level can be found in collective institutions such as APEC, OECD or ECOWAS. Regulation by the CoE should be mentioned, too.

In summary, the following sources of law regarding data protection on both UN and supranational level need to be taken into consideration:

(1) Article 12 of the *Universal Declaration of Human Rights* (UDHR) of 1948:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

(2) Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) of 1966:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

(3) *UN Guidelines for the Regulation of Computerized Personal Data Files* (UN Guidelines) of 1990

(4) *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (UNHCR Policy) of 2015

(5) Article 22 of the *UN Convention on the Rights of Persons with Disabilities* (CRPD) of 2006:

1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.
2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.

[10] Yilma (2018), p. 6.

[11] Yilma (2018), pp. 7 f.

hoeren@uni-muenster.de

(6) Further acts on UN level:

- Principle 6 of the *UN Fundamental Principles of Official Statistics* of 1994, reaffirmed in 2013
- *UN Principles and Guidelines on Access to Legal Aid in Criminal Justice Systems* of 2012
- *Geneva Declaration of Principles* and *Geneva Plan of Action* of 2003
- *Tunis Agenda* of 2005

Acts on UNESCO level:

- *Universal Declaration on Human Genome and Human Rights* of 1997; *International Human Genetic Data Declaration* of 2003
- *Universal Declaration on Bio-ethics and Human Rights* of 2005

(7) *APEC Privacy Framework* of 2005
(8) *Supplementary act A/SA.1/01/10 on personal data protection* within the scope of ECOWAS
(9) *OECD Privacy Framework* of 2013 and a revised recommendation of *"Guidelines governing the protection of privacy and transborder flows of personal data"* of 1980
(10) Related acts on OECD level:

- Ministerial Declaration on the Protection of Privacy on Global Networks [Annex 1 to C(98)177]
- The Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks [C(2002)131/FINAL]
- The Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy [C(2007)67]
- The Declaration for the Future of the Internet Economy (The Seoul Declaration) [C(2008)99]
- The Recommendation of the Council on Principles for Internet Policy Making [C(2011)154]
- The Recommendation of the Council on the Protection of Children Online [C(2011)155]
- The Recommendation of the Council on Regulatory Policy and Governance [C(2012)37]

(11) *CoE Data Protection Convention 108* of 1981, Additional Protocol 2001, modernized version of 2018 (Convention 108+)

1.1.1 Definition of *Personal Data* in the Legislation

Within the aforementioned framework, most sources include precise definitions and address data protection as some sort of specific right:

hoeren@uni-muenster.de

- The *UNHCR Policy* defines personal data as "any data related to an individual who can be identified from that data; from that data and other information; or by means reasonably likely to be used related to that data".[12]
- With regard to Article 2 a) of the *CoE Privacy Framework* personal data "means any information relating to an identified or identifiable individual (data subject)". It addresses specifically the "Protection of Individuals with Regard to the Processing of Personal Data".
- The *APEC Framework* contains a definition of "personal information" in "9.": "Personal information means any information about an identified or identifiable individual". The Framework shall apply to information about natural persons, not legal persons. However, it seems that there is no specific right like personal data protection.
- Personal data in the definition of paragraph 1 b) of *OECD Privacy Framework* means "any information relating to an identified or identifiable individual (data subject)". Data Protection is recognized as a principle from which result different rights of the individuals, paragraph 19 e) OECD Privacy Framework. The Guidelines intend to establish minimum standards, paragraph 6 OECD Privacy Framework.
- According to Article 1 of the *ECOWAS Privacy Framework*, personal data means "any information relating to an identified individual or who may be directly or indirectly identifiable by reference to an identification number or one or several elements related to their physical, physiological, genetic, psychological, cultural, social, or economic identity".

However, the *United Nations Guidelines* for the Regulation of Computerized Personal Data Files itself do not provide a precise definition of the term personal data. They are more of a recommendable nature. The ICCPR does not contain explicit protection of personal information itself either, but as an aspect of the right to privacy.[13] Data protection and privacy cannot be used interchangeably. This would be an oversimplification.[14] The right to privacy is different from the right to data protection. Data privacy or information privacy should probably be used as synonyms to data protection, instead of merely "privacy".

In the case of Article 22 CRPD data protection derives from the term "privacy".

The *UN Fundamental Principles of Official Statistics* do not contain a definition of personal data. Nevertheless, "individual data" are protected in Article 6. And the right to privacy may be derived from Article 2 that demands statistical agencies to decide according to strictly professional considerations, including professional ethics, on the methods and procedures for the collection, processing, storage and presentation of statistical data.

[12]UNHCR Policy, p. 11.

[13]Stability Pact for South Eastern Europe International Standards on Data Protection, p. 1, available at: http://www.selec.org/doc/International_Standards_on_Data_Protection.doc.

[14]De Hert and Papakonstantinou (2013), p. 316.

hoeren@uni-muenster.de

Similarly, the *UN Principles and Guidelines on Access to Legal Aid in Criminal Justice Systems* do not contain a definition of the term "personal data", but acknowledge the right to privacy of children in Guideline 10–54.

Geneva Declaration of Principles and Geneva Plan of Action and Tunis Agenda both do not provide a definition of personal data, but mention the protection of personal data several times.

1.1.2 Classified Categories of *Personal Data* in the Legislation

Only some sources classify special categories of personal data:

- According to the definition in the *UNHCR Policy,* "personal data includes biographical data (biodata) such as name, sex, marital status, date and place of birth, country of origin, country of asylum, individual registration number, occupation, religion and ethnicity, biometric data such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as assessments of the status and/or specific needs".[15]
- Article 6 of the *CoE Privacy Framework* lists "special categories of [personal] data": genetic data, personal data relating to offences criminal proceedings and convictions, and related security measures, biometric data uniquely identifying a person and personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life. Those data are classified by section 2of article 6 as "sensitive data".
- Although the *OECD Privacy Framework* mentions different categories of data "depending upon their nature and the context in which they are collected, stored, processed or disseminated", paragraph 3 a) OECD Privacy Framework, the rights do not differ depending on the nature or context of data. According to paragraph 2, the guidelines should apply to personal data in public and private sectors.
- The *Universal Declaration on Bioethics and Human Rights* addresses "particularly privacy of medical data of persons".

1.2 Specific Regulation of Personal Data Protection

United Nations Level

- Report of the Office of the United Nations High Commissioner for Human Rights: "The right to privacy in the digital age" in 2014[16]

[15] UNHCR Policy, p. 11.

[16] Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

hoeren@uni-muenster.de

- United Nations Human Rights Council appointed: Special Rapporteur Prof. Joseph A. Cannataci of Malta in 2015
- Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci in 2016[17]

Beyond that, specific regulation exists within the following scope:

- The *UNHCR Policy* includes some sort of specific guidelines since it is mandatory for all UNHCR personnel. It applies to "all personal data held by UNHCR in relation to persons of concern to UNHCR" and regardless "whether processing takes place within one UNHCR office, between different UNHCR offices in the same or more than one country, or whether personal data is transferred to Implementing Partners or third parties. The policy continues to apply even after persons are no longer of concern to UNHCR".[18]
- The *UN Fundamental Principles of Official Statistics* state in Principle 6 that "individual data collected by statistics agencies must be strictly confidential and used exclusively for statistical purposes".
- The *UN Principles and Guidelines on Access to Legal Aid in Criminal Justice Systems* demand in Guideline 10–54. that "[t]he privacy and the personal data of a child who is or who has been involved in judicial or non-judicial proceedings and other interventions should be protected at all stages, and such protection should be guaranteed by law. This generally implies that no information or personal data may be made available or published, particularly in the media, which could reveal or indirectly enable the disclosure of the child's identity, including images of the child, detailed descriptions of the child or the child's family, names or addresses of the child's family members and audio and video records". Furthermore, Guideline 11–58. b) requires the state to establish "appropriate measures to establish child-friendly and child-sensitive legal aid systems (. . .) including: (. . .) privacy and protection of personal data (. . .)".
- Article 3 of the *CoE Privacy Framework* states: "1. Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, (. . .)".
- "10." of the *APEC Privacy Framework* defines what is to be understood under "personal information controller". The accompanying commentary states: "The APEC Privacy Framework applies to persons or organizations in the public and private sectors that control the collection, holding, processing, use, transfer or disclosure of personal information. Individual economies' definitions of personal information controller may vary. However, APEC economies agree that for the purposes of this Framework, where a person or organization instructs another person or organization to collect, hold, use, process, transfer or disclose personal information on its behalf, the instructing person or organization is the personal information controller and is responsible for ensuring compliance with the

[17]Available at: http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc.
[18]UNHCR Policy, p. 8.

hoeren@uni-muenster.de

Principles. There is a restriction for Individuals: "Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities."
- Article 3 of the *ECOWAS Supplementary Act* states that "collection, processing, transmission, storage, and use of personal data by any individual, by government, local authorities, and public or private legal entities" shall be subject to the Supplementary Act. There are no exclusions except the one in article 4, which only relates to individuals.

1.3 Supervising and Controlling Entities

The following supervising and/or controlling entities can be identified:

On UN Level

- Human Rights Council (UNHRC): The council is an intergovernmental body within the United Nations system made up of 47 member states responsible for the promotion and protection of all human rights around the globe. The UNHRC is the legal successor to the UN Commission on Human Rights.[19]
- The Office of the United Nations High Commissioner for Human Rights (OHCHR) is a United Nations agency that works to promote and protect the human rights that are granted by the Universal Declaration of the Human Rights.[20] Current commissioner is Prince Zeid bin Ra'ad.[21]
- All bodies rather enforce the right to privacy as a human right, but the processing of personal data as part of data protection law.
- The member states of the ICCPR are obliged to guarantee protective measures for assertion. They are responsible to enforce the treaties' rights within their own legal framework.[22] The Human Rights Committee supervises the ICCPR.[23]
- The *UNHCR Data Protection Policy* includes a sectorial supervision regime, which is regulated in section 7 of the policy.

[19]See United Nations Human Rights Council, http://www.ohchr.org/EN/HRBodies/HRC/Pages/AboutCouncil.aspx.

[20]See United Nations Human Rights Council, http://www.ohchr.org/EN/AboutUs/Pages/WhoWeAre.aspx.

[21]See United Nations Human Rights Council, http://www.ohchr.org/EN/AboutUs/Pages/HighCommissioner.aspx (accessed 20 February 2017).

[22]ICCPR, article 2.

[23]Yilma (2018), p. 14.

hoeren@uni-muenster.de

ECOWAS

- There is a data protection authority which "shall be an independent administrative authority responsible for ensuring that personal data is processed in compliance with the provisions of this Supplementary Act.", article 1: Definitions.
- "Within the ECOWAS space, each Member State shall establish its own data protection Authority. Any State that does not have [an institutional framework for the protection of personal data] shall be encouraged to establish one", article 14 section 1.
- "The data protection Authority shall be an independent administrative Authority responsible for ensuring that personal data is processed in compliance with the provisions of this Supplementary Act.", article 14 section 2.

The *OECD Privacy Framework* does not specify a supervising or controlling unity. The member countries should implement the guidelines by ensuring privacy enforcement authorities with the necessary means for an effective control of data protection, paragraph 19 c) OECD Privacy Framework.

A supervising or controlling can be identified with regard to article 15 of the *CoE Privacy Framework*.

It demands that "[e]ach Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention".

1.3.1 Supervisory Bodies

The *UNHRC* is a subsidiary body of the United Nations General Assembly.[24] It was established by adopting the resolution A/RES/60/251 in 2006 to replace the previous United Nations Commission on Human Rights (UNCHR). Subordinate entities like the Universal Periodic Review, the Advisory Committee, the Complaints Procedure and other subsidiary bodies report directly to the UNHRC. The Complaints Procedure is made up by the Working Group on Communications (WGC) and the Working Group on Situations (WGS).[25]

In 7.1 the *UNHCR Policy* states that "UNHCR's accountability and supervision structure referred to in Part 2.9 will consist of the following key actors:

- A Data Protection Officer within the Division of International Protection at UNHCR Headquarters,
- Data controllers in each country office/operation, and
- Data protection focal points in country offices/operations".[26]

[24]See United Nations, http://www.un.org/en/ga/about/subsidiary/councils.shtml.

[25]See United Nations, http://www.ohchr.org/EN/HRBodies/HRC/ComplaintProcedure/Pages/HRCComplaintProcedureIndex.aspx.

[26]UNHCR Policy, p. 41.

hoeren@uni-muenster.de

1.3.2 Main Powers of the Supervisory Bodies

On UN level, tasks fulfilled by the *UNHRC* and its subsidiary entities are of a reporting and advising nature. Unlike the United Nations Security Council for instance, the UNHRC does not hold sanctioning powers. It is not to be considered as an organ according to Chapter III of the Charter of the United Nations.

Under the *UNHCR Policy*, the *data controller* is a "UNHCR staff member, usually the representative in a UNHCR country office".[27] He or she bears the main responsibility for compliance with the policy in that specific country. The data controller should therefore designate a data protection focal point.[28] That is "in principle, the most senior UNHCR protection staff member in a UNHCR country office or operation, who assists the data controller in carrying out his or her responsibilities regarding this Policy".[29] In contrast, it is the task of the *data protection officer* to provide support for the Data Controllers and to draw an annual data protection report.

The Special Rapporteur on the Right to Privacy has the following duties according to Resolution 28/16:

> a) To gather relevant information, (. . .); b) To seek, receive and respond to information (. . .) from (. . .) any (. . .) relevant stakeholders or parties; c) To identify possible obstacles to the promotion and protection of the right to privacy, to identify, exchange and promote principles and best practices at the national, regional and international levels, and to submit proposals and recommendations to the Human Rights Council in that regard (. . .); (. . .) (g) To report on alleged violations, wherever they may occur, of the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Right (. . .); h) To submit an annual report to the Human Rights Council and to the General Assembly (. . .).

The *CoE Privacy Framework* requires authorities to have powers of investigation and intervention (article 15 section 2 a)) and to perform the functions relating to transfers of data provided under article 14 [Transborder flows of personal data], notably the approval of standardized safeguards (article 15 section 2 b)), to issue decisions with respect to violations of the provisions of the Convention and, in particular, to impose administrative sanctions.

Regarding sanctioning on *ECOWAS level*, "in case of emergency, when processing and use of personal data leads to a violation of rights and liberties", at first the supervisory body is obliged to conduct "a hearing *inter partes*". As next step, it can "suspend the processing", "block certain personal data processed" or "temporarily or permanently prohibit any processing that is contrary to the provisions of this Supplementary Act", article 19, paragraph 3.

[27] UNHCR Policy, p. 9.
[28] UNHCR Policy, p. 41.
[29] UNHCR Policy, p. 9.

hoeren@uni-muenster.de

Sanctions according to article 20 may be:

1) provisional withdrawal of the authorization granted;
2) definitive withdrawal of the authorization; and
3) a fine.

1.4 Self-Regulation Instruments on Data Protection

As aforementioned, member states of the ICCPR must guarantee protective measures to enforce the treaties' articles. Article 40 of the ICCPR binds the member states to answer to controlling procedures. Article 41 introduces an optional complaint procedure between the contracting states in front of the Human Rights Committee.

Regarding the *UNHCR Policy*, it is due to the *Data Protection Officer* to supervise, monitor and report on compliance with the Data Protection Policy. An *Ethics Officer* provides further guidance.

For APEC, self-regulation instruments are mentioned in the commentary accompanying "14.": "The Preventing Harm Principle recognizes that one of the primary objectives of the APEC Privacy Framework is to prevent misuse of personal information and consequent harm to individuals. Therefore, privacy protections, *including self-regulatory efforts*, education and awareness campaigns, laws, regulations, and enforcement mechanisms, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence, remedies for privacy infringements should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information."

The *OECD Privacy Framework* states that the *member countries should encourage and support models of self-regulation*, paragraph 19 d) OECD Privacy Framework.

2 Personal Data Processed by Electronic Means

2.1 Legislation and Case Law Covering the Protection of Personal Data in the Context of Services Provided at a Distance by Electronic Means

The *UN Guidelines* contain different principles[30] regarding the processing of personal data files and provide minimum guarantees as

[30]Burkert (2003), p. 100.

hoeren@uni-muenster.de

- the principle of lawfulness and fairness: collecting and processing data should not be unfair or unlawful and data should not be used for ends contrary to the Charter of the United Nations,
- the principle of accuracy: obligations to check accuracy and relevance,
- the principle of purpose-specification, and
- the principle of non-discrimination.

The principles of interested-person access and that of data security as well as that of transborder flow of data should be mentioned, too.[31]

The *CoE Privacy Framework* embodies several general principles of data processing, but not processing of personal data by electronic means in particular, according to article 5:

> 1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake. (...) 3. Personal data undergoing processing shall be processed lawfully. 4. Personal data undergoing processing shall be: a. processed fairly and in a transparent manner; b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; (...) c. adequate, relevant and not excessive in relation to the purposes for which they are processed; d. accurate and, where necessary, kept up to date; e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

With regard to *OECD*, there is no legislation covering especially personal data processing by electronic means. The Recommendation of the Council on Principles for Internet Policy Making covers the free flow of data and mentions data protection for internet services only referring to the OECD Privacy Framework. Still, the explanatory memorandum of the OECD Privacy Framework contains general principles of national data protections laws:

- setting limits to the collection of personal data in accordance with the objective of the data controller and similar criteria; the principle of purpose-specification,
- restricting the usage of data to conform with openly specified purposes,
- creating facilities for individuals to learn of the existence and contents of data and have data corrected, and
- identification of parties who are responsible for compliance with relevant privacy protection rules and decisions.[32]

Data protection in the *General Agreement on Trade in Services (GATS)* is rudimentary. However, Article III GATS states that "Nothing in this Agreement shall require any Member to provide confidential information, the disclosure of which would impede law enforcement, or otherwise be contrary to the public interest, or which would prejudice legitimate commercial interests of particular enterprises, public or private". This permits parties to keep information confidential

[31] Yilma (2018), p. 6.

[32] Corley (2016), p. 760, note 274.

hoeren@uni-muenster.de

in specific circumstances such as public interest. GATS Article XIV (General Exceptions) underlines the right of parties to adopt and enforce laws and regulations. This also applies to the protection of privacy in relation to the processing and dissemination of personal data. The GATS Annex on Financial Services, section 2 (Domestic Regulation) specifies that parties are under no obligation to reveal information relating to individuals' business bank and accounts, or to confidential and other information in the possession of public entities.

2.2 Previous Consent of the Data Holder

- According to Principle No. 3b) of the *UN Guidelines* (Principle of Purpose-Specification), the purpose which a file is to serve should be specified. Without the consent of the data subject, no personal data shall be used or disclosed for purposes incompatible with this specified purpose.
- Departures from those regulations shall be authorized only if necessary to protect national security, public order, public health or morality, as well as the rights and freedoms of others, especially persons being persecuted (humanitarian clause). Those departures have to be codified expressly in national law or equivalent regulation.
- Article 5 section 2 of the *CoE Privacy Framework* demands that "[e]ach Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law".
- *APEC Privacy Framework:* Consent of the data holder is mentioned in different locations of the framework.
- "18. The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned."
- The related commentary states that "the Principle also recognizes that there are circumstances where providing notice to, or obtaining consent of, individuals would be inappropriate".
- In accordance with the principle in "19." the consent of the individual can eliminate the earmarking: "Personal information collected should be used only to fulfil the purposes of collection and other compatible or related purposes except:
- with the consent of the individual whose personal information is collected;"
- In principle the individual should exercise choice in relation to the collection, use and disclosure of his personal information ("20."). But there are exceptions provided in the related commentary: "This Principle also recognizes, through the introductory words 'where appropriate', that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice."

hoeren@uni-muenster.de

- Furthermore, "26." stipulates that the consent of the individual can be appropriate, when information is transferred to another person or organization: "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."
- The consent and/or knowledge of the data subject is/are required, whenever it is appropriate according to paragraph 7 *OECD Privacy Framework*. Additionally the consent is always required, if the personal data should be collected for other than the predefined purposes, paragraph 9 OECD Privacy Framework, if there is no legal exception in the Member countries' law, paragraph 10 OECD Privacy Framework.
- According to article 23 section 1 *ECOWAS,* "processing of personal data shall be considered legitimate where the data subject has given his consent". However, section 2 allows for the requirement for consent to be waived when the processing is necessary, *i.e.*
  - in order to comply with a legal obligation that is binding upon the data controller;
  - for the implementation of a public interest mission or relevant to the exercise of public authority that is vested in the data controller or the third party to whom the data is disclosed;
  - for the performance of a contract to which the data subject is a party or for the application of pre-contractual measures adopted at his request;
  - for safeguarding the interests or rights and fundamental liberties of the data subject.

2.3 Limitation and Requirements of Electronic Processing of Personal Data

The *UN Guideline principles* shall be applicable

- to all public and private computerized files,
- to manual files (by means of optional extension and subject to appropriate adjustments).

According to Principle 1 of the guidelines, the processing of personal data may not be contrary to the purposes and principles of the Charter of the United Nations. Principle 5 of non-discrimination: Sensitive data should not be compiled if it likely gives rise to unlawful or arbitrary discrimination, including information on racial or

hoeren@uni-muenster.de

ethnic origin, colour, sex, life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union.

Special categories of data named in article 6 of the *CoE Privacy Framework* shall only be allowed where appropriate safeguards are enshrined in law.

Point 18 of the *APEC Privacy Framework* states that "[t]he collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned".

For *ECOWAS*, article 25 states the principles of purpose, relevance and preservation:

1) Personal data shall be obtained for specified, explicit, and lawful purposes and shall not be further processed in any manner incompatible with such purposes.
2) It shall be adequate and relevant in relation to the purposes for which it is collected and further processed.
3) It shall be kept for a period which shall not exceed the period required for the purposes for which they were obtained or processed.
4) Beyond the required period, data may only be kept with a view to responding specifically to processing for historical, statistical, and research purposes, in line with existing legal provisions.

Article 32: Case of personal data processing carried out for purposes of journalism, research, artistic or literary expression.

Processing of personal data that is carried out for the purposes of journalism, research, artistic or literary expression shall be allowed when such processing is executed solely for the purposes of literary and artistic expression; or in the exercise of the professional activity of journalist or researcher, in compliance with the ethical rules of these professions.

2.4 Specific Protection for Minors

As for the *UN Guidelines*, there are only general provisions such as the principle of security, *i.e.* that appropriate measures shall be taken to protect the files against both natural and human dangers (unauthorized access, fraudulent misuse or contamination by computer viruses).

The *UN Principles and Guidelines on Access to Legal Aid in Criminal Justice Systems* 10–54. and 11–58. b) address children specifically.

According to article 15 section 2 e) of the *CoE Privacy Framework,* "specific attention shall be given to the data protection rights of children" by supervisory authorities.

Regarding the *OECD Privacy Framework*, there is no specific protection for minors, but it is clarified in the explanatory memorandum, minors can be represented by another party regarding the knowledge and consent of personal data processing, paragraph 7.

hoeren@uni-muenster.de

2.5 "Right to Be Forgotten"

Principle of interested-person access in the *UN Guidelines*: Everyone who offers proof of identity has the right to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries. The cost of any rectification shall be borne by the person responsible for the file.

The *CoE Privacy Framework* lists in its article 9 the rights of the data subject. Article 9 section 1 e) states: "Every individual shall have a right: (. . .) e) to obtain, on request, free of charge and without excessive delay, rectification and erasure, as the case may be, of such data if these are being, or have been processed contrary to the provisions of this Convention."

APEC Guidelines: "21. Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use". There is a possibility for the individuals to have the information "rectified, completed, amended or deleted" in "23. c)". An exception to this is given in "24.".

Article 26 of the *ECOWAS Privacy Framework* addresses the principle of accuracy: "Personal data obtained shall be accurate and, where necessary, kept up to date. All reasonable measures shall be undertaken to ensure that data that is inaccurate and incomplete in relation to the purposes for which it is obtained and further processed shall be erased or rectified."

2.6 Additional or Specific Obligations

Only the UN Guidelines cover the *principle of accuracy*: Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

2.7 Information Duties

The *CoE Privacy Framework* contains a special provision about data security in article 7:

1. Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorized access to, destruction, loss, use modification or disclosure of personal data.
2. Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

hoeren@uni-muenster.de

There is no obligation for such a special case, but in general the data controller should be accountable according to paragraph 14 *OECD Privacy Framework*, which can include sanctions because of data breaches, as explained in the explanatory memorandum for paragraph 14 OECD Privacy Framework. In addition to that, personal data should be protected against risks such as unauthorized access, paragraph 11 OECD Privacy Framework.

Furthermore, article 27 *ECOWAS Privacy Framework* defines the principle of transparency, which implies that the data controller is obliged to provide information about the processing of personal data.

3 Data Protection in the Electronic Communications Sector

3.1 Specific Legal Rules and Case Law Regarding the Electronic Communications Sector

The *UN Guidelines* for the Regulation of Computerized Personal Data Files contain different principles regarding the processing of personal data files. They provide minimum guarantees as

- the principle of lawfulness and fairness: collecting and processing data should not be unfair or unlawful and data should not be used for ends contrary to the Charter of the United Nations,
- the principle of accuracy: obligations to check accuracy and relevance,
- the principle of purpose-specification, and
- the principle of non-discrimination.

Those principles involve the processing of computerized personal data files not only in the electronic communications sector, but in general.

Other legislations such as the *Supplementary Act* or the *OECD Privacy Framework* do not contain any particular rules.

3.1.1 Implementation of Security Measures by the Electronic Communications Providers

The *UN Guidelines*' Principle of Security (No. 7) requires appropriate measures in order to protect personal data against accidental loss, destruction, unauthorized access, fraudulent misuse or contamination by computer viruses.

hoeren@uni-muenster.de

3.1.2 Data Breaches

According to Principle No. 8 of the *UN Guidelines,* the law of every member state shall designate an impartial authority which is responsible for supervising observance of the minimum guarantees. In case of violation of the provisions implemented in national law, penalties shall be imposed.

3.2 Entities

The *UN Guidelines* address all member states and shall serve as orientation for national legislations.

4 Data Protection and Digital Forensics

4.1 Exceptions, Restrictions and Specific Rules for the Purpose of the Investigation, Detection and Prosecution of Crimes

According to section B. of the *UN Guidelines* for the Regulation of Computerized Personal Data Files, they should apply to personal data files kept by governmental international organizations. In addition, these organizations are asked to designate the authority statutorily competent to supervise the observance of these guidelines, Sentence 2 section B.

According to article 11 of the *CoE Privacy Framework,*

> no exception to the provisions set out in this Chapter [Chapter II: Articles 4-13] shall be allowed except to the provisions of Article 5 paragraph 4 [data quality], Article 7 paragraph 2 [data security], Article 8 paragraph 1 [transparency of processing] and Article 9 [Rights of the data subject], when such an exception is provided by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:
>
> a. the protection of national security, defense, public safety, [. . .], the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, (. . .); (. . .)
>
> 3. In addition to the exceptions allowed for in paragraph 1 (. . .), with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3 [evaluation process], Article 14 paragraph 5 and 6, and Article 15, paragraph 2, litterae a, b, c and d.
>
> This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

hoeren@uni-muenster.de

According to paragraph 4 *OECD Privacy Framework,* exceptions to the guidelines can be provided for purposes of national sovereignty, national security and public policy. These exceptions should be as few as possible and should be made known to the public.

According to article 30 *ECOWAS Supplementary Act,* it is prohibited to obtain and process specific types of data. But there are exceptions in article 31:

> The prohibition stipulated under (Article 30) shall not apply in the following instances:
>
> 1) processing of personal data relating to data manifestly made public by the data subject;
> 2) the data subject has given his written consent, on whatever medium, to such processing, and in line with texts in force;
> 3) processing of personal data is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent;
> 4) processing, in particular of genetic data, is necessary for establishing, exercising or defending a legal right;
> 5) where legal proceedings or a criminal investigation is underway;
>
> [. . .].

4.2 Interception of Communication Data

4.2.1 Legislation Regarding the Purpose of Investigation, Detection and Prosecution of Crimes

This matter is only addressed by article 6 of the *ECOWAS Privacy Framework*:

> Personal data processing that is carried out on behalf of the State, a public establishment or local authority, or a body incorporated under private law and running a public service, shall be decided upon by a legislative or regulatory Act passed subsequent to the reasoned opinion of the data protection Authority. Such processing shall concern:
>
> 1) National security, defence or public security;
> 2) *The prevention, investigation, detection or prosecution of criminal offences or the application of criminal sentences or security measures;*
>
> [. . .].

4.2.2 Requirements

Article 7 of the *ECOWAS Privacy Framework* regulates the formalities of requests for opinions and authorizations:

> Requests for opinions, notifications, and other requests for authorization must specify:
>
> 1) The identity and address of the data controller or, if the latter is not established on the territory of an ECOWAS or UEMOA Member State, those of his duly mandated representative;

hoeren@uni-muenster.de

2) The purpose(s) for which the data is intended to be processed, as well as general description of its functions;
3) The expected combinations or other forms of linkage with other processes;
4) The type of personal data processed, its origin, and the categories of data subjects covered by the processing;
5) The period of preservation of the processed data;
6) The office(s) responsible for executing the processing, as well as the categories of persons who, by virtue of their functions or for service requirements, have direct access to the recorded data;
7) The recipients to whom such data may be disclosed;
8) The function of the person or department to whom application shall be made for right of access;
9) The steps taken to ensure the security of the processing and of the data;
10) An indication that the data is processed by a data professor;
11) Where personal data is expected to be transferred to third countries that are not members of ECOWAS or UEMOA, subject to reciprocity.

Article 8 ECOWAS Privacy Framework: *Deadline*:

The data protection Authority shall give its opinion within a set period of time starting from the date of receipt of the request for opinion or authorization. Nevertheless, this period of time may or may not be extended, on the basis of a reasoned decision of the data protection Authority.

5 Data Protection and Electronic Surveillance for Security and Defence Purposes

5.1 Legislation and Case Law Regarding Security and National Defence Purposes

According to article 11 of the *CoE Privacy Framework,*

no exception to the provisions set out in this Chapter [Chapter II: articles 4-13] shall be allowed except to the provisions of Article 5 paragraph 4 [data quality], Article 7 paragraph 2 [data security], Article 8 paragraph 1 [transparency of processing] and Article 9 [Rights of the data subject], when such an exception is provided by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

a. the protection of national security, defense, public safety, [. . .]; (. . .)

3. In addition to the exceptions allowed for in paragraph 1 (. . .), with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3 [evaluation process], Article 14 paragraph 5 and 6, and Article 15 paragraph 2, litterae a, b, c and d.

This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

hoeren@uni-muenster.de

In "13." of the *APEC Privacy Framework* it says that even those exceptions of the principles

> relating to national sovereignty, national security, public safety and public policy should be:
>
> a) limited and proportional to meeting the objectives to which the exceptions relate; and,
>
> b) (i) made known to the public; or,
>
> (ii) in accordance with law.

However, in the related commentary it is stated that "although recognizing the importance of governmental respect for privacy, this Framework is not intended to impede governmental activities authorized by law when taken to protect national security, public safety, national sovereignty or other public policy".

According to paragraph 4 *OECD Privacy Framework*, exceptions to these guidelines can be provided for purposes of national sovereignty, national security and public policy. These exceptions should be as few as possible and should be made known to the public.

The *ECOWAS Supplementary Act* states that "any processing of data related to public security, defence, investigation and prosecution of criminal offences or State security, subject to such exemptions as are defined by specific provisions stipulated in other legal texts in force" shall be subject to its scope (article 3). In article 6 it says that

> Personal data processing that is carried out on behalf of the State, a public establishment or local authority, or a body incorporated under private law and running a public service, shall be decided upon by a legislative or regulatory Act passed subsequent to the reasoned opinion of the data protection authority.
>
> Such processing shall concern:
>
> 1) National security, defence or public security; [. . .].

5.2 Requirements

Relevant ECOWAS provisions:

> Article 7: Formalities of requests for opinions and authorizations
>
> Requests for opinions, notifications, and other requests for authorization must specify:
>
> 1) The identity and address of the data controller or, if the latter is not established on the territory of an ECOWAS or UEMOA Member State, those of his duly mandated representative;
> 2) The purpose(s) for which the data is intended to be processed, as well as general description of its functions;
> 3) The expected combinations or other forms of linkage with other processes;
> 4) The type of personal data processed, its origin, and the categories of data subjects covered by the processing;
> 5) The period of preservation of the processed data;

hoeren@uni-muenster.de

6) The office(s) responsible for executing the processing, as well as the categories of persons who, by virtue of their functions or for service requirements, have direct access to the recorded data;
7) The recipients to whom such data may be disclosed;
8) The function of the person or department to whom application shall be made for right of access;
9) The steps taken to ensure the security of the processing and of the data;
10) An indication that the data is processed by a data professor;
11) Where personal data is expected to be transferred to third countries that are not members of ECOWAS or UEMOA, subject to reciprocity.

Article 8: Deadline

The data protection Authority shall give its opinion within a set period of time starting from the date of receipt of the request for opinion or authorization. Nevertheless, this period of time may or may not be extended, on the basis of a reasoned decision of the data protection Authority.

6 Remedies and Sanctions

6.1 Remedies for the Breach of Data Protection Rules

Article 12 of *CoE Privacy Framework* states: "Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of [the] Convention".

According to article 15 paragraph 2 c) of *CoE Privacy Framework* authorities "shall have powers to issue decisions with respect to violations of the provisions of [the] Convention and may, in particular, impose administrative sanctions".

As for the *APEC Privacy Framework*, there are just recommendations containing possible remedies; *e.g.* in the commentary to "14.": "Hence, remedies for privacy infringements should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information."

See also "38.":

A Member Economy's system of privacy protections should include an appropriate array of remedies for privacy protection violations, which could include redress, the ability to stop a violation from continuing, and other remedies. In determining the range of remedies for privacy protection violations, a number of factors should be taken into account by a Member Economy including:

a) the particular system in that Member Economy for providing privacy protections (*e.g.*, legislative enforcement powers, which may include rights of individuals to pursue legal action, industry self-regulation, or a combination of systems); and
b) the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations.

hoeren@uni-muenster.de

The ECOWAS Privacy Framework includes provisions for sanctions and appeal:

Article 20: Sanctions
Where the data processor does not conform with the formal notice addressed to him, the protection Authority may, after procedures inter partes, take the following sanctions against him:

1) provisional withdrawal of the authorization granted;
2) definitive withdrawal of the authorization; and
3) a fine.

Article 21: Appeal
The sanctions and decisions of the Data Protection Authority may be subject to appeal.

6.2 General Personal Data Protection Rules

The Guidelines for the Regulation of Computerized Personal Data Files are not legally binding and need to be seen as advisory principles stating minimum guarantees every state should provide.[33]

The OECD Guidelines are neither binding and are as well rather seen as a minimum standard of data protection legislation.[34] In addition, they do not provide enforcement mechanisms such as remedies or sanctions.[35]

7 Private International Law Rules

7.1 Territorial Scope

The right of privacy in article 12 of the *Universal Declaration of Human Rights* (UDHR) is technically seen a resolution of the General Assembly. Still, in the meantime the Declaration has acquired the status of customary international law.[36]

In article 3 of the *ECOWAS Privacy Framework* it is written that the processing carried out in an UEMOA or ECOWAS Member State shall be subject to the Supplementary Act.

[33]Burkert (2003), p. 100.

[34]Corley (2016), p. 761.

[35]Corley (2016), p'. 762.

[36]See United Nations, http://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html.

hoeren@uni-muenster.de

7.2 Transfer of Personal Data

Only the UNHCR Policy, the APEC Privacy Framework and the ECOWAS Privacy Framework are relevant in this context:

Within the scope of 6.1 of the *UNHCR Policy*, "UNHCR may transfer personal data to third parties on condition that the third party affords a level of data protection the same or comparable to [the] Policy". This relates particularly to the following basic principles (6.1.2):

- Transfer is based on one or more legitimate bases;
- Transfer is for one or more specific and legitimate purpose(s);
- The personal data to be transferred is adequate, relevant, necessary and not excessive in relation to the purpose(s) for which it is being transferred;
- The data subject has been informed, either at the time of collection in accordance with Part 3.1, or subsequently, about the transfer of his/her personal data, unless one or more of the restrictions in Part 3.7 apply;
- The third party respects the confidentiality of personal data transferred to them by UNHCR. Whether or not a data transfer agreement has been signed between UNHCR and the third party, UNHCR must seek written agreement from the third party that the personal data will be kept confidential at all times. In order to ensure and respect confidentiality, personal data must be filed and stored in a way that is accessible only to authorized personnel and transferred only through the use of protected means of communication;
- The third party maintains a high level of data security that protects personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to it.

In addition, UNHCR needs to ensure that transferring personal data does not negatively impact:

- the safety and security of UNHCR personnel and/or personnel of Implementing Partners; and/or
- the effective functioning of an UNHCR operation or compromise UNHCR's mandate, for example due to the loss of the climate of trust and confidence between UNHCR and persons of concern or the loss of the perception of UNHCR as an independent, humanitarian and non-political Organization.[37]

The *APEC Privacy Framework* has no particular legislation but includes some recommendations for the development of Cross-border Privacy Rules:

> III. Cooperative Development of Cross-border Privacy Rules
>
> 46. Member Economies will endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection

[37] See UNHCR Policy, pp. 35 f.

hoeren@uni-muenster.de

requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.

47. To give effect to such cross-border privacy rules, Member Economies will endeavor to work with appropriate stakeholders to develop frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between and among the economies.

48. Member Economies should endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.

Within the *ECOWAS Privacy Framework*, article 36 provides particular provisions for the transfer of personal data to a non-member ECOWAS country:

1) The data controller shall transfer personal data to a non-member ECOWAS country only where such a country provides an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data.
2) The data controller shall inform the Data Protection Authority prior to any transfer of personal data to such a third country.

Acknowledgments The author would like to thank the ABIDA research team (ITM/Münster) including Charlotte Röttgen, Max von Schönfeld, Andreas Börding, Nicolai Culik, Steffen Uphues, Christian Döpke & Tim Jülicher for their efforts in drafting the paper.

References

Bennett C, Raab C (2006) The governance of privacy. MIT Press, Cambridge

Burkert H (2003) In: Roßnagel A (ed) Handbuch Datenschutzrecht, vol 1. C.H. Beck, Munich

Corley M (2016) The need for an International Convention on Data Privacy: taking a cue from the CISG. Brooklyn J Int Law 41:720

De Hert P, Papakonstantinou V (2013) Three scenarios for International Governance of Data Privacy: towards an International Data Privacy Organization, preferably a UN Agency? J Law Policy Inf Soc 9:271

Raab C, Koops B-J (2009) Privacy actors, performances and the future of privacy protection. In: Gutwirth S, Poullet Y, De Hert P, de Terwangne C, Nouwt S (eds) Reinventing data protection? Springer, Amsterdam

Rotenberg M (2017) Urgent mandate, unhurried response: an evaluation of the UN Special Rapporteur on the right to privacy. Eur Data Protect Law Rev 3:47

Weber M (2017) Protection for privacy under the United Nations Convention on the rights of persons with disabilities. Laws 6:10

Yilma K (2018) The United Nations Data Privacy System and its limits. Int Rev Law Comput Technol 32(1):2

hoeren@uni-muenster.de