Big Data and Data Quality

Thomas Hoeren

Abstract Big data is closely linked to the new, old question of data quality. Whoever pursues a new research perspective such as big data and wants to zero out irrelevant data is confronted with questions of data quality. Therefore, the European General Data Protection Regulation (GDPR) requires data processors to meet data quality standards; in case of non-compliance, severe penalties can be imposed. But what does data quality actually mean? And how does the quality requirement fit into the dogmatic systems of civil and data protection law?

1 Introduction[1]

The demand for data quality is old. Already the EU data protection directive did contain "principles relating to data quality". Article 6 states that personal data "must be accurate and, where necessary, kept up to date". However, as sanctions for non-compliance were left out, the German legislator did not transfer those principles into national law, i.e., the German Federal Data Protection Act (BDSG).[2] Unlike Germany, other European countries such as Austria implemented the provisions concerning data quality.[3] Switzerland has even extended the regulations. According to Article 5 of the Swiss Data Protection Act,[4] the processor of personal data has to ensure its accuracy by taking all reasonable steps to correct or erase data

[1]In the following, footnotes only refer to the documents necessary for the understanding of the text.
[2]Act amending the BDSG (Federal Data Protection Act) and other laws of 22 May 2001 (Federal Law Gazette I pp 904 et seqq.).
[3]Section 6 of the Federal Law on the Protection of Personal Data (Federal Law Gazette I No. 165/ 1999).
[4]Art. 5 of the Swiss Data Protection Act of 19 Jun 1992, AS 1993, 1945.

T. Hoeren (✉)
Institute for Information, Telecommunication and Media Law (ITM),
University of Münster, Münster, Germany
e-mail: hoeren@uni-muenster.de

T. Hoeren and B. Kolany-Raiser (eds.), *Big Data in Context*,
SpringerBriefs in Law, https://doi.org/10.1007/978-3-319-62461-7_1

that are incorrect or incomplete in light of the purpose of its collection or processing.

Against this background and considering the relevance of Article 6 of the EU Data Protection Directive in the legal policy discussion, the silence of the German law is astounding. The European Court of Justice (ECJ) emphasized the principles of data quality in its Google decision not without reason. It pointed out that any processing of personal data must comply with the principles laid down in Article 6 of the Directive as regards the quality of the data (Ref. 73).[5] Regarding the principle of data accuracy the Court also pointed out "even initially lawful processing of accurate data may, in the course of time, become incompatible with the Directive where those data are no longer necessary in the light of the purposes for which they were collected or processed".[6]

However, embedding the principle of data quality in data protection law seems to be the wrong approach, since data quality has little to do with data protection. Just think of someone who needs a loan. If he receives a very positive credit score due to overaged data and/or his rich uncle's data, there is no reason to complain, while under different circumstances he would call for accuracy. At the same time, it is not clear why only natural persons should be affected by the issue of data quality. The fatal consequences of incorrect references on the solvency of a company became obvious in the German case *Kirchgruppe v. Deutsche Bank*, for example.[7]

At first, data quality is highly interesting for the data economy, i.e., the data processing industry. The demand of data processors is to process as much valid, up-to-date, and correct data as possible in the user's own interest. Therefore, normative fragments of a duty to ensure data quality can be found in security-relevant areas. Suchlike provisions apply to flight organizations throughout Europe,[8] statistical authorities[9] or financial service providers,[10] for example. In civil law, the data quality requirement is particularly important with regard to the general sanctions for the use of false data. Negative consequences for the data subject have often been compensated by damages from the general civil law, for example, by means of section 824 BGB or the violation of pre-contractual diligence obligations under section 280 BGB. However, there is no uniform case law on such information liability.

After all, the data quality regulation proved to be a rather abstract demand. Already in 1977, a commission of experts of the US government emphasized

---

[5]Cf. Österreichischer Rundfunk et al., C-465/00, C-138/01 and C-139/01, EU:C:2003:294, Ref. 65; ASNEF and FECEMD, C 468/10 and C 469/10; EU:C:2011:777, Ref. 26 and Worten, C 342/12, EU:C:2013:355, Ref. 33.

[6]Google Spain, C 131/12, EU:C:2014:317, Ref. 93.

[7]For this purpose, BGH, NJW 2006, p 830 and Derleder, NJW 2013, p 1786 et seqq.; Höpfner/Seibl 2006, BB 2006, p 673 et seq.

[8]Art. 6 of the Air Quality Requirements Regulation.

[9]Art. 12 of Regulation (EC) No. 223/2009 of 11 Mar 2009, OJ L 87, pp 169 et seqq.

[10]Section 17 Solvency Ordinance of 14 Dec 2006, Federal Law Gazette I pp 2926 et seqq. and section 4 of the Insurance Reporting Ordinance of 18 Apr 2016, Federal Law Gazette I pp 793 et seqq.

correctly: "The Commission relies on the incentives of the marketplace to prompt reconsideration of a rejection if it turns out to have been made on the basis of inaccurate or otherwise defective information."[11]

The market, and therefore also the general civil law, should decide on the failure of companies to use obsolete or incorrect data.

2 Background to Data Quality[12]

2.1 Origin Country: The USA

Surprisingly (at least from a European data protection perspective), the principle of data quality stems from US legislation. The US Privacy Act 1974,[13] which is still in effect today, contains numerous requirements for data processing with regard to "accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness".[14]

However, this regulation is only applicable if the state ("agencies") processes personal data and ensures the concerned person a fair decision process by the authority concerning the guarantee of the data quality.

Incidentally, in the United States, the Data Quality Act (DQA), also known as the Information Quality Act (IQA), was adopted in 2001 as part of the Consolidated Appropriations Act. It empowers the Office of Management and Budget to issue guidelines, which should guarantee and improve the quality and integrity of the information that is published by state institutions ("Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies"[15]).[16] Furthermore, it requires federal agencies to "establish administrative mechanisms allowing affected persons to seek and obtain correction of information maintained and disseminated by the agency that does not comply with the guidelines".[17]

However, the provisions do not differentiate between non-personal data and personal data. Additionally, the scope of the Data Quality Act is exhausted in

[11]Epic.org, Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, https://epic.org/privacy/ppsc1977report/c1.htm.

[12]The history of data protection remains to be part of the research in the field of legal history. Initial approaches: Büllesbach/Garstka 2013, CR 2005, p 720 et seqq., v. Lewinski (2008), in: Arndt et al. (eds.), p 196 et seqq.

[13]http://www.archives.gov/about/laws/privacy-act-1974.html (Accessed 4 Apr 2017).

[14]5 U.S.C. 552 a (e) (5) concerning the processing of data by state 'agencies'.

[15]White House, Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies, https://www.whitehouse.gov/omb/fedreg_final_information_quality_guidelines/ (Accessed 4 Apr 2017).

[16]https://www.whitehouse.gov/omb/fedreg_reproducible (Accessed 4 Apr 2017).

[17]Subsection (2) (B) of the DQA.

distribution of information by the state against the public.[18] Moreover, there is no federal law that establishes guidelines for the data quality of personal data in the non-governmental sector. Since in the US data protection is regulated by numerous laws and guidelines at both federal and state level, there are some area-specific laws that contain rules on data quality (e.g. the Fair Credit Reporting Act or the Health Insurance Portability and Accountability Act of 1996).

For example, the Fair Credit Reporting Act requires users of consumer reports to inform consumers of their right to contest the accuracy of the reports concerning themselves. Another example is the Health Insurance Portability and Accountability Act (HIPAA) Security Rule according to which the affected institutions (e.g., health programs or health care providers) must ensure the integrity of electronically protected health data.[19]

2.2 The OECD Guidelines 1980

The US principles were adopted and extended by the OECD Guidelines 1980.[20] However, it must be noted that the guidelines were designed as non-binding recommendations from the outset.[21] Guideline 8 codifies the principle of data "accuracy" and was commented as follows: "Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept".[22] The issue of data quality was regulated even more extensively and in more detail in a second OECD recommendation from 1980 referred to as the "15 Principles on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters".[23]

Principle no. 5 contained detailed considerations about data quality surpassing today's standards.

> Personal data must be: (…) -accurate and, where necessary, kept up to date; 2. Personal data must be evaluated taking into account their degree of accuracy or reliability, their source, the categories of data subjects, the purposes for which they are processed and the phase in which they are used.

[18] Wait/Maney 2006, Environmental Claims Journal 18(2), p 148.

[19] Sotto/Simpson 2014, United States, in: Roberton, Data Protection & Privacy, pp 210 et seq.

[20] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (23 Sep 1980), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Accessed 4 Apr 2017). Concerning this Patrick 1981, Jurimetrics 1981 (21), No. 4, pp 405 et seqq.

[21] Kirby 2009, International Data Privacy Law 2011 (1), No. 1, p 11.

[22] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborder-flowsofpersonaldata.htm#comments (Accessed 4 Apr 2017).

[23] http://www.statewatch.org/news/2007/may/oecd-1980s-data-protection-principles.pdf (Accessed 4 Apr 2017).

Some members of the OECD Expert Group doubted as to whether or not data quality was part of privacy protection in the first place:

> In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection.[24]

Even external experts[25] were divided on the correct classification of such:

> Reasonable though that expression is, the use of a term which bears an uncertain relationship to the underlying discipline risks difficulties in using expert knowledge of information technology to interpret and apply the requirements.[26]

It was noted rightly and repeatedly that this was a general concept of computer science:

> Data quality is a factor throughout the cycle of data collection, processing, storage, processing, internal use, external disclosure and on into further data systems. Data quality is not an absolute concept, but is relative to the particular use to which it is to be put. Data quality is also not a static concept, because data can decay in storage, as it becomes outdated, and loses its context. Organizations therefore need to take positive measures at all stages of data processing, to ensure the quality of their data. Their primary motivation for this is not to serve the privacy interests of the people concerned, but to ensure that their own decision-making is based on data of adequate quality (see footnote 26).

2.3 *Art. 6 of the EU Data Protection Directive and its Impact in Canada*

Later on, the EU Data Protection Directive adopted the OECD standards which were recognized internationally ever since.[27] The first draft[28] merely contained a general description of elements permitting the processing of data through public authorities.[29] It was not until the final enactment of Art. 16 when the duty to process *accurate* data was imposed on them, notwithstanding the question as to whether the data protection was (in-)admissible. In its second draft from October 1992,[30] the provision was moved to Art. 6, thus standing subsequent to the provision on the admissibility of data processing. Sanctions are not provided and the uncertainty

[24]It is explicitly laid down in the explanations of the guidelines, Explanatory Memorandum, p 53.

[25]Cf. Fuster 2014, The Emergence of Personal Data Protection as a Fundamental Right of the EU, p 78 et seq.

[26]Clarke, The OECD Guidelines, http://www.rogerclarke.com/DV/PaperOECD.html (Accessed 4 Apr 2017).

[27]Concerning this Cate, Iowa Law Review 1995 (80), p 431 et seq.

[28]http://aei.pitt.edu/3768/1/3768.pdf (Accessed 4 Apr 2017).

[29]COM (90) 314, final, SYN 287, p 53.

[30]http://aei.pitt.edu/10375/ (Accessed 4 Apr 2017).

regarding the connection of data principles to the admissibility of data processing remained.

Thus, the data principles maintained their character as recommendatory proposals.

Being pressured by the EU, several states accepted and adopted the principles on data quality, i.e. Canada by enacting the PIPEDA Act 2000:

> Personal information shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used. The extent to which personal information shall be accurate, complete and up to date will depend upon the use of the information, taking into account the interests of the individual.[31]

In Canada, the principle of data accuracy was specified in guidelines:

> Information shall be sufficiently accurate, complete and up to date to minimize the possibility that inappropriate information may be used to make a decision about the individual. An organization shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected. Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up to date, unless limits to the requirement for accuracy are clearly set out.[32]

Within the EU, the United Kingdom was first to implement the EU Principles on Data Protection by transposing the Data Protection Directive into national law through the Data Protection Act 1998.

While the Data Protection Act 1998 regulates the essentials of British data protection law, concrete legal requirements are set in place by means of statutory instruments and regulations.[33] The Data Protection Act 1998 establishes eight Principles on Data Protection in total. Its fourth principle reflects the principle of data quality, set out in Article 6 (1) (d) of the EU Data Protection Directive, and provides that personal data must be accurate and kept up to date.[34]

To maintain the practicability, the Act adopts special regulations for cases in which people provide personal data themselves or for cases in which personal data are obtained from third parties: If such personal data are inaccurate, the inaccuracy will, however, not be treated as a violation of the fourth Principle on Data Protection, provided that (1) the affected individual or third party gathered the inaccurate information in an accurate manner, (2) the responsible institution

---

[31]Personal Information Protection and Electronic Documents Act (PIPEDA), (S.C. 2000, c. 5); see Austin, University of Toronto Law Journal 2006, p 181 et seq.

[32]Section 4.6 of the Principles Set out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information CAN/CSA-Q830-96; see Scassa/Deturbide 2012, p 135 et seq.

[33]Taylor Wessing, An overview of UK data protection law, http://united-kingdom.taylorwessing.com/uploads/tx_siruplawyermanagement/NB_000168_Overview_UK_data_protection_law_WEB.pdf (Accessed 4 Apr 2017).

[34]Sch. 1 Pt. 1 para. 4 Data Protection Act 1998. Further information on the fourth principle of data protection under https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/ (Accessed 4 Apr 2017).

undertook reasonable steps to ensure data accuracy and (3) the data show that the affected individual notified the responsible institution about the inaccuracies.[35] What exactly can be considered as "reasonable steps" depends on the type of personal data and on the importance of accuracy in the individual case.[36]

In 2013, the UK Court of Appeal emphasized in *Smeaton v Equifax Plc* that the Data Protection Act 1998 does not establish an overall duty to safeguard the accuracy of personal data, but it merely demands to undertake reasonable steps to maintain data quality. The reasonableness must be assessed on a case-to-case basis. Neither does the fourth Principle on Data Protection provide for a parallel duty in tort law.[37] Despite these international developments shortly before the turn of the century, the principle of data quality was outside the focus as "the most forgotten of all of the internationally recognized privacy principles".[38]

3 Data Quality in the GDPR

The data principle's legal nature did not change until the GDPR was implemented.

3.1 Remarkably: Art. 5 as Basis for Fines

Initially, the GDPR's objective was to adopt, almost literally, the principles from the EU Data Protection Directive as recommendations without any sanctions.[39] At some point during the trilogue, the attitude obviously changed. Identifying the exact actors is impossible as the relevant trilogue papers remain unpublished. Somehow the trilogue commission papers surprisingly mentioned that the Principles on Data Regulation will come along with high-level fines (Art. 83 para. 5 lit. a). Ever since, the principle of data quality lost its status as simple non-binding declaration and has yet to become an offense subject to fines. It will be shown below that this change, which has hardly been noticed by the public, is both a delicate and disastrous issue. Meanwhile, it remains unclear whether a fine of 4% of annual sales for violating the provision on data quality may, in fact, be imposed because the criterion of factual

[35]Sch. 1 Pt. 2 para. 7 Data Protection Act 1998.

[36]https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/ (Accessed 4 Apr 2017).

[37]Smeaton v Equifax Plc, 2013, ECWA Civ 108, http://www.bailii.org/ew/cases/EWCA/Civ/2013/108.html (Accessed 4 Apr 2017).

[38]Cline 2007, Data quality—the forgotten privacy principle, Computerworld-Online 18 Sep 2007, http://www.computerworld.com/article/2541015/security0/data-quality-the-forgotten-privacy-principle.html (Accessed 4 Apr 2017).

[39]See Art. 5 para. 1 lit. d version from 11 Jun 2015, "Personal data must be accurate and, where necessary, kept up to date".

accuracy is vague. What does "factual" mean? It assumes a dual categorization of "correct" and "incorrect" and is based on the long-discussed distinction between facts and opinions which was discussed previously regarding section 35 BDSG (German Federal Data Protection Act).[40] In contrast to opinions, facts may be classified as "accurate"/"correct" or "inaccurate"/"incorrect". Is "accurate" equivalent to "true"? While the English version of the GDPR uses "accurate", its German translation is "richtig" (correct). The English term is much more complex than its German translation. The term "accurate" comprises purposefulness and precision in the mathematical sense. It originates from engineering sciences and early computer science and defines itself on the basis of these roots as the central definition in modern ISO-standards.[41] In this context, the German term can be found in the above-mentioned special rules for statistics authorities and aviation organizations. The term was not meant in the ontological sense and did thus not refer to the bipolar relationship between "correct" and "incorrect" but it was meant in the traditional and rational way in the sense of "rather accurate". Either way, as the only element of an offense, the term is too vague to fulfill the standard set out in Article 103 para. 2 German Basic Law.[42] Additionally, there is a risk that the supervisory authority expands to a super-authority in the light of the broad term of personal data as defined in Article 4 para. 1 GDPR. The supervisory authority is unable to assess the mathematical-statistical validity of data processes. Up until now, this has never been part of their tasks nor their expertise. It would be supposed to assess the validity autonomously by recruiting mathematicians.

3.2 Relation to the Rights of the Data Subject

Furthermore, the regulation itself provides procedural instruments for securing the accuracy of the subject's data. According to Article 16 GDPR, the person concerned has a right to rectification on "inaccurate personal data". Moreover, Article 18 GDPR gives the data subject the right to restrict processing if the accuracy of the personal data is contested by the data subject. After such a contradiction, the controller has to verify the accuracy of the personal data.

Articles 16 and 18 GDPR deliberately deal with the wording of Article 5 GDPR ("inaccurate", "accuracy") and insofar correspond to the requirement of data correctness. The rules also show that Article 5 is not exhaustive in securing the data which is correct in favor of the data subject. Article 83 para. 5 lit. b GDPR sanctions non-compliance with the data subjects' rights with maximum fines. However, "accuracy" here means "correctness" in the bipolar sense as defined above.

[40]See Mallmann, in: Simitis 2014, BDSG, section 20 ref. 17 et seq.; Dix, in: Simitis, BDSG, section 35 ref. 13.

[41]ISO 5725-1:1994.

[42]German Federal Constitutional Court, BVerfGE 75, p 341.

It is important not to confuse two terms used in the version: the technologically-relational concept of "accuracy" and the ontologically-bipolar concept of "correctness" of assertions about the person concerned in Articles 12 and 16 GDPR. The concept of accuracy in Articles 12 and 16 GDPR has nothing to do with the concept of accuracy in Art. 5 GDPR. It is therefore also dangerous to interpret the terms in Article 5 and Article 12, 16 GDPR in the same way.

3.3 Data Quality and Lawfulness of Processing

It is not clear how the relationship between Articles 5 and 6 GDPR is designed. It is particularly questionable whether the requirement of data accuracy can be used as permission in terms of Article 6 lit. f GDPR. A legitimate interest in data processing would then be that Article 5 GDPR requires data to be up-to-date at all times.

3.4 Art. 5—An Abstract Strict Liability Tort?

Another question is whether Article 5 GDPR constitutes an abstract strict liability tort or whether it should be interpreted rather restrictively.[43] This leads back to the aforementioned question: Is it necessary to reduce Article 5 GDPR from a teleological point of view to the meaning that the accuracy of the data is only necessary if non-compliance has a negative impact to the affected person? The Australian Law Commission has understood appropriate regulations in the Australian data protection law in this sense[44]: "In the OPC Review, the OPC stated that it is not reasonable to take steps to ensure data accuracy where this has no privacy benefit for the individual."

The above-mentioned British case law is similar. However, the general source of danger and the increased risks posed by large data pools in the age of big data argue for the existence of a strict liability tort. Foreign courts, including the Canadian Federal Court Ottawa, also warn against such dangers. The Federal Court emphasized in its "Nammo"[45] decision:

[43]Anastasopoulou 2005, Deliktstypen zum Schutz kollektiver Rechtsgüter, p 63 et seq.; Graul 1989, Abstrakte Gefährdungsdelikte und Präsumptionen im Strafrecht, p 144 et seq.; Gallas 1972, Abstrakte und konkrete Gefährdung, in: Lüttger et al., Festschrift für Ernst Heinitz zum 70. Geburtstag, p 171.

[44]Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC Report 108), http://www.alrc.gov.au/publications/27.%20Data%20-Quality/balancing-data-quality-and-other-privacy-interests (Accessed 4 Apr 2017).

[45]Nammo v. TransUnion of Canada Inc., 2010 FC 1284: see http://www.fasken.com/files/upload/Nammo_v_Transunion_2010_FC_1284.pdf (Accessed 4 Apr 2017).

> An organization's obligations to assess the accuracy, completeness and currency of personal information used is an ongoing obligation; it is not triggered only once the organization is notified by individuals that their personal information is no longer accurate, complete or current. Responsibility for monitoring and maintaining accurate records cannot be shifted from organizations to individuals.

And the Privacy Commissioner in Ottawa emphasized in her 2011 activity report:[46]

> By presenting potentially outdated or incomplete information from a severed data source, a credit bureau could increase the possibility that inappropriate information is used to make a credit decision about an individual, contrary to the requirements of Principle 4.6.1.

In my opinion, both thoughts should be interlinked. As a basis for an abstract strict liability tort, Art. 5 lit. d GDPR must be interpreted restrictively. This is particularly important in view of the fact that Article 5 lit. d GDPR can also be the basis of an administrative offense procedure with massive fines (Article 83 para 5 lit. a GDPR). However, this cannot and must not mean that the abstract strict liability tort becomes a concrete one. That would be an interpretation against the wording of Article 5 lit. d GDPR. In my opinion, such an interpretation should be avoided right now as the text of the regulation has just been adopted. Therefore, Article 5 lit. d GDPR can be seen as an abstract strict liability tort which is subject to broad interpretation. However, the corresponding provisions for imposing administrative fines should be applied narrowly and cautiously.

4 Conclusions

The different provisions from Canada and the United States as well as the development from the European Data Protection Directive to the General Data Protection Regulation show that data quality is an issue of growing relevance. However, accuracy and veracity[47] can only be safeguarded as long as effective mechanisms guarantee adequate quality standards for data. Both the EU Directive and the DQA are giving a lead in the right direction.

---

[46]Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2011-009, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-009/ (Accessed 4 Apr 2017). Similarly already Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2003-224, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-224/ (Accessed 4 Apr 2017); Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2003-163, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-163/ (Accessed 4 Apr 2017).

[47]See overview "Four V's of Big Data" (Volume, Variety, Velocity und Veracity), Mohanty 2015, The Four Essential V's for a Big Data Analytics Platform, Dataconomy-Online, http://dataconomy.com/the-four-essentials-vs-for-a-big-data-analytics-platform/ (Accessed 4 Apr 2017).

However, the mere reference to the observance of quality standards is not sufficient to comply with Article 5 of the GDPR. Let us recall the Canadian Nammo case, which has already been recited several times:[48]

> The suggestion that a breach may be found only if an organization's accuracy practices fall below industry standards is untenable. The logical conclusion of this interpretation is that if the practices of an entire industry are counter to the Principles laid out in Schedule I, then there is no breach of PIPEDA. This interpretation would effectively deprive Canadians of the ability to challenge industry standards as violating PIPEDA.

This warning is important because there are no globally valid and recognized industry standards for data quality. We are still far from a harmonization and standardization. Insofar, the data protection supervisory authorities should take the new approach of criminal sanctioning of data quality very cautiously and carefully.

References

Anastasopoulou I (2005) Deliktstypen zum Schutz kollektiver Rechtsgüter. CH Beck, Munich

Austin LM (2006) Is consent the foundation of fair information practices? Canada's experience under Pipeda. Univ Toronto Law J 56(2):181–215

Büllesbach A, Garstka HJ (2013) Meilensteine auf dem Weg zu einer datenschutzgerechten Gesellschaft. CR 2005:720–724. doi: 10.9785/ovs-cr-2005-720

Cate FH (1995) The EU data protection directive, information privacy, and the public interest. Iowa Law Rev 80(3):431–443

Clarke R (1989) The OECD data protection guidelines: a template for evaluating information privacy law and proposals for information privacy law. http://www.rogerclarke.com/DV/PaperOECD.html. Accessed 4 Apr 2017

Cline J (2007) Data quality—the forgotten privacy principle, Computerworld-Online. http://www.computerworld.com/article/2541015/security0/data-quality—the-forgotten-privacy-principle.html. Accessed 4 Apr 2017

Derleder P (2013) Das Milliardengrab—Ein bemerkenswertes Urteil offenbart pikante Details in der Causa Kirch gegen Deutsche Bank. NJW 66(25):1786–1789

Fuster G (2014) The emergence of personal data protection as a fundamental right of the EU. Springer, Cham

Gallas W (1972) Abstrakte und konkrete Gefährdung. In: Lüttger H et al (eds) Festschrift für Ernst Heinitz zum 70. Geburtstag. De Gruyter, Berlin, pp 171–184

Graul E (1989) Abstrakte Gefährdungsdelikte und Präsumptionen im Strafrecht. Duncker & Humblot, Berlin

Höpfner C, Seibl M (2006) Bankvertragliche Loyalitätspflicht und Haftung für kreditschädigende Äußerungen nach dem Kirch-Urteil. Betriebs-Berater 61:673–679

Kirby M (2009) The history, achievement and future of the 1980 OECD guidelines on privacy. Int Data Priv Law 1(1):6–14

Lewinski K (2008) Geschichte des Datenschutzrechts von 1600 bis 1977. In: Arndt Fv et al. (eds) Freiheit—Sicherheit—Öffentlichkeit. Nomos, Heidelberg, pp 196–220

Mohanty S (2015) The four essential V's for a big data analytics platform. Dataconomy-Online, http://dataconomy.com/the-four-essentials-vs-for-a-big-data-analytics-platform/. Accessed 4 Apr 2017

[48]Nammo v. TransUnion of Canada Inc., 2010 FC 1284.

Patrick PH (1981) Privacy restrictions on transnational data flows: a comparison of the council of Europe draft convention and OECD guidelines. Jurimetrics 21(4):405–420
Simitis S (2014) Kommentar zum Bundesdatenschutzgesetz. Nomos, Baden-Baden
Sotto LJ, Simpson AP (2014) United States. In: Roberton G (ed) Data protection & privacy 2015. Law Business Research Ltd, London, pp 208–214
Scassa T, Deturbide ME (2012) Electronic commerce and internet law in Canada, vol 2. CCH Canadian Limited, Toronto
Wait A, Maney J (2006) Regulatory science and the data quality act. Environ Claims J 18(2): 145–162

Author Biography

Prof. Dr. Thomas Hoeren, professor for information, media and business law and head of the Institute for Information, Telecommunication and Media Law (ITM) at the University of Münster. He serves as head of the project ABIDA (Assessing Big Data).