Harmonisierung, engmaschiges Kontrollnetz und starke Aufsichtsbehörden

Der Datenschutz in Europa nach der neuen Datenschutz-Grundverordnung

PROFESSOR DR. THOMAS HOEREN · ANDRA GIURGIU*

Der vorliegende Aufsatz befasst sich mit dem Entwurf der europäischen Datenschutz-Grundverordnung (Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 25. 1. 2012, KOM(2012) 11 endgültig). Am 30. 3. 2012 ist der Entwurf erstmals im Bundestag und -rat beraten worden. Anhand des Hintergrunds dieser Verordnung wird sowohl ein Einblick in die bisherige Rechtslage gewährt als auch die uneinheitliche Umsetzung der Datenschutzbestimmungen, die zu dem neuen Entwurf geführt hat, dargestellt. Die Analyse des Verordnungsentwurfs soll dann die wesentlichen geplanten Neuerungen des europäischen Datenschutzes verdeutlichen und abschließend entsprechende Schlussfolgerungen ermöglichen.

WE http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf

Inhaltsübersicht

I. Einführung

Dem Entwurf ging Anfang Dezember ein Proposal for a Regulation 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 (Version 56 vom 29. 11. 2011, COM 56/2011) voraus. Der neue Gesetzesrahmen für den Datenschutz soll sich aus zwei Rechtsakten zusammensetzen, bestehend aus einer Verordnung und einer Datenschutz-Richtlinie für polizeiliche und strafrechtliche Zusammenarbeit (KOM(2012) 11 endg.).

Vorschlag soll Vertrauen in Online-Geschäftsumfeld und Datenschutz stärken

Die technischen Entwicklungen haben den Datenschutz vor neue Herausforderungen gestellt. Infolgedessen war die Europäische Kommission der Ansicht, dass das Vertrauen in die Online-Umgebung gestärkt werden müsse und dass die EU eine umfassende und konsequente Strategie zur Gewährleistung des Grundrechts auf Schutz personenbezogener Daten brauche. Die aktuellen Regelungen müssten geändert werden, weil die europäische Rechtsgrundlage fragmentiert ist. So würden die betreffenden Regelungen nicht nur Rechtsunsicherheit verursachen, sondern auch die öffent-

* Universitätsprofessor Dr. Thomas Hoeren lehrt an der Juristischen Fakultät der Westfälischen Wilhelms-Universität Münster am Institut für Informations-, Telekommunikations- und Medienrecht; Andra Giurgiu ist wissenschaftliche Mitarbeiterin an diesem Lehrstuhl und Rechtsanwältin in Sibiu (Rumänien).

liche Wahrnehmung dahingehend bestimmen, dass Online-Aktivitäten eine hohes Risiko mit sich brächten (Begründung KOM(2012)11).

Wirtschaftsfreundliche Regelungen

Nach dem Willen der Kommissarin Viviane Reding soll ein wirtschaftsfreundlicherer Datenschutz die Kostenbelastung für die Wirtschaft der Mitgliedstaaten mindern. Außerdem soll das Vertrauen der Bürger in neue Dienstleistungen und Technologien gestärkt werden, um die digitale Gesellschaft zu fördern.

Zwei Jahre Vorlauf und Verhandlungen

Der jetzige Entwurf ist das Ergebnis sich über zwei Jahre erstreckender, ausführlicher Konsultationen, Konferenzen, Workshops, Seminaren, Umfragen und Studien.

II. Hintergrund des Entwurfs

Trotz einheitlicher Grundlagen unterschiedlicher nationaler Rechtsinhalt

Bereits im siebten Erwägungsgrund des Entwurfs wird anerkannt, dass die Ziele und die allgemeinen Grundsätze der bisherigen Datenschutzrichtlinie (RL 95/46/EG vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) erhalten bleiben. Die Fragmentierung bei der Umsetzung dieser Richtlinie hatte jedoch ein unterschiedliches Schutzniveau der Rechte und Freiheiten in den verschiedenen Mitgliedstaaten zur Folge. Diese Unterschiede stellen ein Hemmnis für den grenzüberschreitenden Fluss personenbezogener Daten in der Union und damit auch für die Wirtschaftstätigkeiten und den freien Wettbewerb dar, so die EU-Kommission.

Seit seiner Einführung 1995 wurde die Datenschutzrichtlinie von den Mitgliedstaaten uneinheitlich umgesetzt. Daraus ergaben sich verschiedene Konfliktsituationen zwischen der Kommission und den jeweiligen Staaten. Bereits 2009 wurde das Vereinigte Königreich von der Kommission beim Europäischen Gerichtshof verklagt, weil es die EU-Vorschriften zum Datenschutz nicht befolgt habe. Es habe die Datenschutzvorschriften bezüglich der Vertraulichkeit der elektronischen Kommunikation missachtet und das Abfangen von Nachrichten ohne eine entsprechende Einwilligung gestattet.

Vertragsverletzungsverfahren der Kommission gegen Deutschland

Die Umsetzung der Datenschutzrichtlinie wurde auch in Deutschland thematisiert. Die Kommission leitete im November 2007 ein Vertragsverletzungsverfahren gegen die Bundesrepublik mit der Begründung ein, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nicht öffentlichen Bereich zuständigen Kontrollstellen in den Bundesländern der staatlichen Aufsicht unterworfen seien, so dass das Erfordernis der „völligen Unabhängigkeit" dieser Stellen nicht gewahrt sei. Im anschließenden Urteil stellte der EuGH einen Verstoß Deutschlands gegen seine Verpflichtungen aus der Richtlinie 95/46/EG fest (EuGH, Urteil vom 9. 3. 2010 - Rs. C-518/07).

Vielfache nationale Umsetzung und Einpassung in den bestehenden Ordnungsrahmen

Diskussionen gab es in Deutschland auch bezüglich der Änderungen (RL 2009/136/EG vom 25. 11. 2009 zur Änderung der RL 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung [EG] Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl EG L 337 vom 18. 12. 2009 S. 11), der Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG vom 12. 7. 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [Datenschutzrichtlinie für elektronische Kommunikation]), die sog. E-Privacy-Richtlinie bezüglich der Opt-in-Pflicht für Cookies.

III. Natur und Inhalte des Verordnungsentwurfs

1. Verordnung statt Richtlinie

Verordnungstext soll EU-weite Einheitlichkeit des Rechts sicherstellen

Zur Stärkung des Datenschutzes hat sich die EU diesmal für eine Verordnung entschieden, die an die Stelle der Richtlinie 95/46/EG treten soll. Zum einen hat eine Verordnung in den EU-Mitgliedstaaten direkte Wirkung, so dass sich sowohl eine

rechtliche Fragmen
Darüber hinaus sol
soll zur Verringeru
gleiches Schutznive
die für die Verarbeit
soll Rechtssicherhei
und Verarbeitung, d
wirksame Zusamme
Erwägungsgrund 1

2. Erweiterter Anw
Der Schutz der EU-B
soll, wenn der Veran
betroffene Person in
oder Dienstleistung
betroffenen Persone
sich zukünftig auch
troffene wenden, wi

3. Ausnahme nur fü
Ausgenommen vom
arbeitung sein, die
schließlich persönlicl
KOM(2012) 11).

4. Begriffsbestimmu
„Personenbezogene
Standortdaten, Onlin
Bestimmbarkeit eine
zwangsläufig und ur
werden (KOM(2012)
Neue Begriffe sol
vor diesem Hintergru
Verantwortlichen wir
folglich der Ort, an
Vorhandensein und d
nicht entscheidend.
Hauptverwaltung in
Erwägungsgrund 27).
die Verarbeitung von
dessen stellt sich die
denen die Entscheidu
Lösung wäre die Bestir
raum. Ein Unternehm
Anweisungen der Aus
Hauptniederlassung b

5. Zusätzliche Anford
Neuerungen gibt es au
eigenen Daten. Diese
sowie „explizit" erteilt

rechtliche Fragmentierung als auch andere Umsetzungsstreitigkeiten vermeiden lassen. Darüber hinaus soll sie aber weitere Vorteile schaffen: Das Instrument der Verordnung soll zur Verringerung des Verwaltungsaufwands beitragen. Außerdem soll sie ein gleiches Schutzniveau der Rechte der Bürger aller Mitgliedstaaten sicherstellen und für die für die Verarbeitung Verantwortlichen gleiche Pflichten begründen. Eine Verordnung soll Rechtssicherheit für die Wirtschaftsbeteiligten durch eine einheitliche Überwachung und Verarbeitung, durch äquivalente Sanktionen in allen Mitgliedstaaten und durch eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden schaffen (s. KOM(2012) 11, Erwägungsgrund 11).

2. Erweiterter Anwendungsbereich

Wohnsitz in EU-Mitgliedstaat und Betroffenheit sollen für Anwendbarkeit ausreichen

Der Schutz der EU-Bürger wird insoweit erweitert, als die Verordnung auch dann gelten soll, wenn der Verantwortliche nicht in der EU ansässig ist. Dabei soll es genügen, dass die betroffene Person in der EU wohnhaft ist und die Verarbeitung dem Angebot von Waren oder Dienstleistungen „in der Union" oder der Beobachtung des Verhaltens der betroffenen Personen dient (Art. 3 Abs. 2 KOM(2012) 11 endg.). Infolgedessen werden sich zukünftig auch Unternehmen außerhalb Europas, die sich an EU-ansässige Betroffene wenden, wie Google und Facebook, an die EU-Vorschriften halten müssen.

3. Ausnahme nur für rein persönliche oder häusliche Tätigkeiten

Rein persönliche Datenerhebungen fallen nicht in den Anwendungsbereich

Ausgenommen vom Anwendungsbereich der Verordnung soll weiterhin die Datenverarbeitung sein, die natürliche Personen ohne jede Gewinnerzielungsabsicht zu ausschließlich persönlichen oder familiären Zwecken vornehmen (Art. 2 Abs. 2 Buchst. d KOM(2012) 11).

4. Begriffsbestimmungen

Alle Informationen, die sich auf eine Person beziehen, sind personenbezogene Daten

„Personenbezogene Daten" sind alle Informationen, die sich auf eine Person beziehen. Standortdaten, Online-Kennungen oder genetische Elemente werden zu den Mitteln der Bestimmbarkeit einer Person hinzugefügt. IP-Adressen sollen laut Entwurf „nicht zwangsläufig und unter allen Umständen als personenbezogene Daten" betrachtet werden (KOM(2012) 11, Erwägungsgrund 24).

Räumlicher Bezugsort als Anknüpfungspunkt für Verordnung kann Probleme bereiten

Neue Begriffe sollen miteinbezogen und rechtlich bestimmt werden. Interessant ist vor diesem Hintergrund die Definition des Begriffs „Hauptniederlassung". Im Falle des Verantwortlichen wird damit die Zentralverwaltung eines Unternehmens bezeichnet, folglich der Ort, an dem die Management-Entscheidungen getroffen werden. Das Vorhandensein und die Nutzung der technischen Mittel sind dabei für die Verarbeitung nicht entscheidend. Für den Auftragsverarbeiter ist das der Ort, an dem sich seine Hauptverwaltung in der Union befindet (Art. 4 Abs. 13 KOM(2012) 11, s. auch Erwägungsgrund 27). Diese Definition wirft das Problem auf, dass heutzutage sowohl die Verarbeitung von Daten als auch das Management dezentralisiert sind. Infolgedessen stellt sich die Frage der Bestimmung der Hauptniederlassung in Situationen, in denen die Entscheidungen in einem „virtuellen" Raum getroffen werden. Eine mögliche Lösung wäre die Bestimmung nach dem Serverstandort für den virtuellen Besprechungsraum. Ein Unternehmen mit mehreren Niederlassungen in der EU soll sich zukünftig den Anweisungen der Ausfichtsbehörde des Mitgliedstaats fügen müssen, in dem sich seine Hauptniederlassung befindet (Art. 51 Abs. 2 KOM(2012).

WP Schröder, EU: Neue Details zur EU-Datenschutzreform, unter http://www.2b-advice.com/no_cache/service/meldungen/2b/news/2011/12/09/eu-neue-details-zur-eu-datenschutzreform.html

5. Zusätzliche Anforderungen an eine gültige Einwilligungserklärung

Jede Nutzung soll der ausdrücklichen Einwilligung bedürfen

Neuerungen gibt es auch bezüglich der Einwilligung in die Nutzung und Verarbeitung der eigenen Daten. Diese soll in Zukunft für den konkreten Fall und in Kenntnis der Sache sowie „explizit" erteilt werden (Art. 4 Abs. 8 KOM(2012) 11).

Hinweis Die Kommission hat damit der Diskussion über die Form, in der die Einwilligung erteilt werden soll, ein Ende gesetzt. Ein allgemeines Schrifterfordernis besteht nicht.

Nutzer der fremden Daten trägt die Beweislast für freie Einwilligung

Wenn aber die Verarbeitung aufgrund der Einwilligung der betroffenen Person stattfindet, liegt die Beweislast bei dem für die Verarbeitung Verantwortlichen. Er muss nachweisen, dass die betroffene Person ihre Einwilligung für die Verarbeitung erteilt hat (Art. 7 Abs. 1 KOM(2012) 11).

Nur Opt-in-Lösungen sollen zulässig sein

Diesbezüglich hat die Kommission deutlich gemacht, dass nur die Opt-in-Möglichkeit berücksichtigt werden darf. Die Einwilligung muss in Form einer Erklärung oder einer eindeutigen Handlung abgegeben werden, die es ermöglicht, dass der Betroffene in vollem Bewusstsein über seine Zustimmung entscheidet, wie z. B durch das Anklicken eines Kästchens beim Besuch einer Internetseite (KOM(2012) 11, Erwägungsgrund 25). Dies hat zur Folge, dass Untätigkeit für die erforderliche bewusste Einwilligung nicht ausreichen wird.

Eine wesentliche Neuerung betrifft das Verbot einer auf Einwilligung basierenden Verarbeitung, „wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht" (Art. 7 Abs. 4 KOM(2012) 11). Die Einwilligung muss ohne Zwang erteilt werden, was zur Folge hat, dass sie dann nicht als Grundlage der Verarbeitung dienen kann, wenn die einwilligende Person keine wirkliche und freie Wahl hat und wenn sie ihre Zustimmung nicht nachträglich ohne Schaden zurücknehmen kann (KOM(2012) 11, Erwägungsgrund 33). Diese neue Vorschrift erinnert an das Problem der gestörten Vertragsparität, welches vom BVerfG bei Bürgschaftsverträgen aufgegriffen wurde. Für die grundrechtliche Gewährleistung der Privatautonomie soll bei einer strukturellen Unterlegenheit des einen Vertragsteils, wenn die Folgen des Vertrags für den unterlegenen Vertragsteil ungewöhnlich belastend sind, die Zivilrechtsordnung eingreifen können und Korrekturen ermöglichen. Darüber steht der Gedanke, dass Verträge nicht als Mittel der Fremdbestimmung dienen sollen, wenn ihr Inhalt ungewöhnlich belastend und als Interessenausgleich offensichtlich unangemessen ist (BVerfG, Beschluss vom 5. 8. 1994 - 1 BvR 1402/89, NJW 1994 S. 2749).

Werden wertende Korrekturen zugunsten schwächerer Vertragspartner möglich?

EU-Verordnung könnte deutschen Beschäftigtendatenschutz „überholen"

Hinweis Diese europäische Vorschrift hat als Folge, dass im Beschäftigungsverhältnis sowie im Falle behördlicher Subordinationsverhältnisse, die Einwilligung des Betroffenen keine rechtliche Grundlage für die Verarbeitung darstellen soll (KOM(2012) 11, Erwägungsgrund 34).

6. Erweiterte Auskunfts- und Informationsrechte

Detailliertes Informationsrecht der Personen, deren Daten verarbeitet werden

Datenverarbeitende Unternehmen müssen sicherstellen, dass die Informationen bezüglich der Datenverarbeitung leicht zugänglich, verständlich sowie klar und einfach abgefasst sind (Art. 11 KOM(2012) 11). Die erweiterte Transparenz setzt voraus, dass der betroffenen Person zumindest die Informationen bezüglich der Existenz einer Verarbeitung und ihrer Ziele, der Speicherdauer der Daten, des Bestehens des Rechts auf Zugang, zur Berichtigung und Löschung und ein Beschwerderecht zur Verfügung gestellt werden (Art. 14 KOM(2012) 11).

7. Recht auf Vergessenwerden

Recht auf Vergessenwerden als bloße Informationspflicht

Neu ist die Einführung des sog. Rechts auf Vergessen. Abgesehen von dem schon bekannten Recht auf Löschung führt der Verordnungsentwurf im Falle der Veröffentlichung der Daten die Pflicht des Verantwortlichen ein, „alle vertretbaren Schritte, auch technischer Art" zu unternehmen, „um Dritte, die die Daten verarbeiten, darüber zu

informieren, dass
diese personenb
verlangt." (Art. 17
Das in der ei
Vergessenwerden
aus allen öffentl
Informationspflicl

Hinweis Tr
setzen. Dabei soll
Geldbuße von bis
Buße für Verstöße
KOM(2012) 11).

8. Recht auf Datei
Wenn die Daten „e
verarbeitet werder
personenbezogene
damit die eigenen
sozialen Netzwerk
überträgt (Art. 18 k

9. Beschränkung v
Eine Profilerstellun
automatisierte Ver
Lage, des Standorts
der Zuverlässigkeit
Beschränkung soll g
Erfüllung eines Verti
auf der Einwilligung

Hinweis Dies
die Profilbildungs- u

10. Pflicht zur Einha
Jeder für die Verarb
soll alle Verarbeitung
entsprechenden Auf
die Überwachung d
KOM(2012) 11).

11. Verpflichtung zu
Um eine vertraulich
Verantwortlichen ur
vacy by Design) und
KOM(2012) 11). Ents
sowohl bei der Aus
Verarbeitungsprozes
Art. 23 enthält keine
gebunden sein soll.
wortung, einen solch

informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt." (Art. 17 Abs. 2 KOM(2012) 11).

Das in der ersten Fassung des Entwurfs (COM 56/2011) angekündigte Recht auf Vergessenwerden, wonach der Betroffene einen Anspruch auf umfassende Löschung aus allen öffentlich-zugänglichen Verzeichnissen hatte, ist somit durch eine bloße Informationspflicht ersetzt worden, was auf jeden Fall viel realitätsnäher ist.

Abschreckend hohe Bußgelder

Hinweis Trotzdem ist dieses neu eingeführte Recht praktisch schwer umzusetzen. Dabei soll die bewusste oder auch nur fahrlässige Nichtbeachtung mit einer Geldbuße von bis zu 500.000 € geahndet werden können – für Unternehmen soll die Buße für Verstöße bis zu 1 % ihres Jahresumsatzes betragen (Art. 79 Abs. 5 Buchst. c KOM(2012) 11).

8. Recht auf Datenübertragbarkeit

Anspruch auf elektronische Kopie der eigenen Daten

Wenn die Daten „elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet werden", soll die betroffene Person Anspruch darauf haben, eine Kopie ihrer personenbezogenen Daten in einem elektronischen Format zu erhalten. Sie könnte damit die eigenen Daten vereinfacht weiterverwenden, indem sie diese z. B. von einem sozialen Netzwerk wie StudiVZ auf ein anderes soziales Netzwerk wie Facebook überträgt (Art. 18 KOM(2012) 11).

9. Beschränkung von Profilerstellungen

Größere Hürden für Profilbildung und Scorings

Eine Profilerstellung soll grds. untersagt sein (Art. 20 KOM(2012) 11). Damit sollen automatisierte Verarbeitungen zur Auswertung der Arbeitsleistung, der finanziellen Lage, des Standorts der Person, des Gesundheitszustands, der persönlichen Vorlieben, der Zuverlässigkeit oder des Verhaltens untersagt werden. Eine Ausnahme von dieser Beschränkung soll gelten, wenn die Verarbeitung im Rahmen des Abschlusses oder der Erfüllung eines Vertrags erfolgt, wenn sie durch eine Rechtsvorschrift zugelassen ist oder auf der Einwilligung der betroffenen Person beruht (Art. 20 Abs. 2 KOM(2012) 11).

Hinweis Diese Vorschrift wird in dieser Form viele Unternehmen beeinträchtigen, die Profilbildungs- und Scoringmethoden einsetzen.

10. Pflicht zur Einhaltung einer Dokumentation

Umfassende Dokumentation bleibt notwendig

Jeder für die Verarbeitung Verantwortliche, Auftragsdatenverarbeiter sowie Vertreter soll alle Verarbeitungsvorgänge, für die er zuständig ist, dokumentieren müssen, mit der entsprechenden Aufsichtsbehörde zusammenarbeiten und ihr die Dokumentation für die Überwachung der Verarbeitungsprozesse zur Verfügung stellen (Art. 28 und 29 KOM(2012) 11).

11. Verpflichtung zur datenschutzfreundlichen Grundeinstellung

Weitreichende organisatorische Pflichten bei der Verarbeitung sollen verpflichtend werden

Um eine vertrauliche Verarbeitung sicherzustellen, soll die Verpflichtung für jeden Verantwortlichen und Auftragsverarbeiter bestehen, Datenschutz „automatisch" (Privacy by Design) und „standardmäßig" (Privacy by Default) zu implementieren (Art. 23 KOM(2012) 11). Entsprechende technische und organisatorische Vorkehrungen sollen sowohl bei der Ausgestaltung der Verarbeitung als auch während des gesamten Verarbeitungsprozesses getroffen werden (KOM(2012) 11, Erwägungsgrund 61). Der Art. 23 enthält keine Hinweise darauf, inwieweit ein Verarbeiter an diese Grundsätze gebunden sein soll. Ein Unternehmen, das Daten verarbeitet, trägt aber die Verantwortung, einen solchen Auftragsverarbeiter zu wählen, der hinreichende Garantien für

die Sicherheit der Verarbeitung und die Einhaltung der Rechte der Betroffenen bietet. Zu diesem Zweck ist darauf zu achten, dass der gewählte Auftragsverarbeiter „geeignete technische Sicherheitsvorkehrungen und organisatorische Maßnahmen" trifft (Art. 23 Abs. 1 KOM(2012) 11).

12. Ernennung eines Vertreters

Wenn ein Unternehmen nicht in der EU ansässig ist, soll es einen Vertreter in dem Mitgliedstaat ernennen müssen, in dem die betroffene Person wohnhaft ist. Ausnahmen von dieser Pflicht gelten für Unternehmen aus Drittstaaten, die einen angemessenen Schutz bieten, für Unternehmen mit weniger als 250 Mitarbeitern bzw. für Unternehmen, die Personen (Betroffenen) in der Union nur „gelegentlich" Waren oder Dienstleistungen anbieten. Dieser Vertreter unterliegt den Vorschriften dieser Verordnung, seine Ernennung beseitigt jedoch nicht die Möglichkeit des rechtlichen Vorgehens gegen den für die Verarbeitung konkret Verantwortlichen – auch, wenn er seinen Sitz außerhalb der EU hat (Art. 25 KOM(2012) 11).

Geltung nicht nur für EU-Unternehmen

13. Strengere Anforderungen an Auftragsverarbeiter

Der Verordnungsentwurf stellt mehrere Pflichten für die Auftragsverarbeitung auf. Der Auftragsverarbeiter muss die Vertraulichkeit bei der Einstellung der Mitarbeiter und die Sicherheit der Verarbeitung gewährleisten. Das Anwerben weiterer Auftragsverarbeiter darf nur nach vorheriger Einwilligung des für die Verarbeitung Verantwortlichen stattfinden.

Pflicht zur Folgenabschätzung

Die Pflicht der Gewährleistung der Sicherheit der Datenverarbeitung betrifft jetzt auch den Auftragsverarbeiter ungeachtet seines Verhältnisses zu dem Verantwortlichen. Er soll außerdem den Verantwortlichen bei der Einhaltung seiner Pflichten bezüglich der Sicherheit der Verarbeitung, der Benachrichtigung bei Verletzungen des Schutzes personenbezogener Daten und der Durchführung der Datenschutz-Folgenabschätzung unterstützen. Er soll die Ergebnisse nach Abschluss der Verarbeitung übergeben und die Daten nicht weiterverarbeiten. Der Auftragsverarbeiter soll außerdem dem Verantwortlichen und der Kontrollstelle alle Informationen bereitstellen, die für die Kontrolle der Einhaltung seiner Pflichten notwendig sind. Die Pflicht der Dokumentation besteht auch für den Auftragsverarbeiter. Die Grundlage des Auftrags bildet entweder ein Vertrag oder ein anderer Rechtsakt, der diese Pflichten konkretisiert. Bei Nichtbeachtung der vom Verantwortlichen erteilten Anweisungen gilt der Auftragsverarbeiter als Verantwortlicher und haftet entsprechend (Art. 26 KOM(2012) 11).

14. Benachrichtigungspflicht im Falle eines Datenschutzvorfalls

Bei Gefahr der Verletzung persönlicher Daten Meldepflicht binnen 24 Stunden

Bei Verletzung personenbezogener Daten soll der Verantwortliche die Aufsichtsbehörde binnen 24 Stunden benachrichtigen müssen. Diese Pflicht soll unabhängig von der Schwere des Verstoßes oder der Art der betroffenen personenbezogenen Daten bestehen. Bei möglichen negativen Auswirkungen der Verletzung soll außerdem die betroffene Person informiert werden. Diese muss dann nicht benachrichtigt werden, wenn der für die Verarbeitung Verantwortliche nachweist, dass er geeignete technische Schutzmaßnahmen getroffen hat (Art. 32 KOM(2012) 11). Ein solcher Schutz kann beispielsweise durch Verschlüsselungsmechanismen errichtet werden.

Kritik an den sehr vagen Tatbeständen

Der Entwurf wurde insoweit schon kritisiert, weil er weder die Kriterien und die Anforderungen zur Feststellung einer Verletzung noch die genauen Umstände der Benachrichtigung festlegt. Allerdings wird die Benachrichtigungspflicht für deutsche Unternehmen keine wesentlichen Änderungen der anzeigepflichtigen Sachverhalte bringen. Gleichwohl ist festzustellen, dass der Zeitraum, in dem der Verstoß gemeldet werden muss, verkürzt würde. Die Benachrichtigung soll „unverzüglich" erfolgen, was

„ohne schuldhafte
Verletzung in 24 Stu
begründet werden.

15. Folgenabschätz
Neu hinzu käme au
bestimmten Daten
erweitern. Eine Folg
die Verarbeitung be
darstellen kann. De
matisch und umfa
wirtschaftliche Lage
abschätzung zum
KOM(2012) 11). Was

16. Verpflichtung zu
Neu wäre auch die E
seiner Aufgaben una
alle Fälle betreffen, i
erfolgt oder durch ei
alle Fälle, in dener
Verarbeitungsvorgän
mäßige und systema

Laut Entwurf wä
samen Datenschutzb
der Unternehmensgr
(Art. 35 KOM(2012) 1

Hinweis Im Ve
pflicht eines Beauftr
privaten Stellen ab ei
EU-Verordnung eine
BDSG).

Übrigens können nacl
Datenpannen trotzd
interne Selbstkontro
stelltenzahl könnte
Einhaltung der Dater
hörden zu verhinderr

17. Vereinfachte Übe
Die Datenübermittlu
interne Datenschutz
sichtsbehörde angen
sichtsbehörde geneh
der nationalen Aufsic
- wenn sie rechtsve
- den Betroffenen d
- die in Art. 43 Abs.

„ohne schuldhaftes Zögern" (§ 121 BGB) bedeutet, wobei laut dem Entwurf eine Verletzung in 24 Stunden gemeldet werden soll. Eine verzögerte Benachrichtigung muss begründet werden.

15. Folgenabschätzung statt Vorabkontrolle

Folgenabschätzung für risikoreiche Verarbeitungsvorgänge

Neu hinzu käme auch die Pflicht zur Prüfung der Auswirkungen für den Datenschutz bei bestimmten Datenverarbeitungsverfahren; dies soll die bisher bekannte Vorabkontrolle erweitern. Eine Folgenabschätzung müsste in den Fällen durchgeführt werden, in denen die Verarbeitung besondere Risiken für die Rechte und Freiheiten der betroffenen Person darstellen kann. Der Verordnungsentwurf nennt beispielhaft Unternehmen, die systematisch und umfassend persönliche Aspekte einer Person auswerten, etwa deren wirtschaftliche Lage oder Daten zum Gesundheitszustand. Hier würde eine Folgenabschätzung zum Schutz der Rechte der Betroffenen verpflichtend (Art. 33 Abs. 2 KOM(2012) 11). Was das etwa für Finanzdaten bedeutet, ist noch völlig unklar.

16. Verpflichtung zur Bestellung eines Datenschutzbeauftragten

Datenschutzbeauftragte in Unternehmen grds. erst ab 250 Mitarbeitern

Neu wäre auch die EU-weite Verpflichtung der Verantwortlichen, einen in der Ausübung seiner Aufgaben unabhängigen Datenschutzbeauftragten zu ernennen. Diese Pflicht soll alle Fälle betreffen, in denen die Verarbeitung durch eine Behörde oder öffentliche Stelle erfolgt oder durch ein Unternehmen, das über 250 Mitarbeiter hat. Hinzu kommen sollen alle Fälle, in denen die Haupttätigkeit des Unternehmens im Wesentlichen aus Verarbeitungsvorgängen besteht, die nach Art, Umfang und/oder Zweck eine regelmäßige und systematische Überwachung erfordern.

Laut Entwurf wäre es für eine Gruppe von Unternehmen zulässig, einen gemeinsamen Datenschutzbeauftragten zu benennen. Dieser soll beim Unternehmen bzw. bei der Unternehmensgruppe beschäftigt sein können, aber auch extern beauftragt sein (Art. 35 KOM(2012) 11).

Aus deutscher Perspektive weniger Datenschutzbeauftragte und mehr Unternehmensferne

Hinweis Im Vergleich zum deutschen Bundesdatenschutzgesetz, das die Bestellpflicht eines Beauftragten für Datenschutz im Falle herkömmlicher Verarbeitung von privaten Stellen ab einer Zahl von 20 Beschäftigten festlegt, würden die Vorschriften der EU-Verordnung eine Herabsetzung des Datenschutzniveaus darstellen (s. § 4f Abs. 1 BDSG).

Übrigens können nach dem Verordnungsentwurf bei mangelndem Datenschutz oder bei Datenpannen trotzdem hohe Bußgelder gegen Unternehmen verhängt werden. Eine interne Selbstkontrolle durch einen Beauftragten auch bei einer niedrigeren Angestelltenzahl könnte für Unternehmen zukünftig also eine Option sein, um für die Einhaltung der Datenschutzvorschriften zu sorgen und ein Eingreifen der Aufsichtsbehörden zu verhindern.

17. Vereinfachte Übermittlung von Daten an Drittstaaten

Vereinfachte Datenübermittlung in Drittstaaten durch verbindliche unternehmensinterne Datenschutzvorschriften und angenommene Standarddatenschutzklauseln

Die Datenübermittlung an Drittländer soll in Zukunft durch verbindliche unternehmensinterne Datenschutzvorschriften (BCR), durch von der EU-Kommission oder eine Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder durch von einer Aufsichtsbehörde genehmigte Vertragsklauseln vereinfacht werden. Solche BCR sollen von der nationalen Aufsichtsbehörde mittels des Kohärenzverfahrens genehmigt werden,

- wenn sie rechtsverbindlich sind,
- den Betroffenen durchsetzbare Rechte einräumen und
- die in Art. 43 Abs. 2 des Entwurfs genannten Mindestinformationen beinhalten.

Alternativ sollen Datenübermittlungen anhand der schon in Art. 26 Abs. 4 der Richlinie 95/46/EG erwähnten Standardvertragsklauseln stattfinden können. Diese sollen aber zukünftig nicht nur von der EU-Kommission, sondern auch von der nationalen Aufsichtsbehörde festgelegt werden können.

18. Beschwerderechte und Anspruch auf Schadensersatz

Datenschutzorganisationen sollen das Recht zur Beschwerde bei einer nationalen Kontrollstelle sowohl im Namen einer oder mehrerer Personen als auch im eigenen Namen erhalten (Art. 73 Abs. 2 KOM(2012) 11).

Rechtsbehelfe gegen eine Aufsichtsbehörde

Außerdem sollen Entscheidungen der Kontrollstellen anfechtbar sein (Art. 74 KOM(2012) 11). Auch gegen gegen die Verantwortlichen der Verarbeitung sowie deren Auftragsverarbeiter sollen Personen, die sich in ihren Rechten verletzt sehen, direkt gerichtlich vorgehen können (Art. 75 KOM(2012) 11).

Haftung der Verarbeiter von persönlichen Daten

Bei einer rechtswidrigen Verarbeitung geht aus Art. 77 ein Anspruch auf Schadensersatz sowohl gegenüber dem Verantwortlichen als auch gegen den Auftragsverarbeiter hervor. Bei mehreren Verantwortlichen soll jeder gesamtschuldnerisch haften. Der Verordnungsentwurf vermutet bei Verstößen ein Verschulden des Verantwortlichen oder des Auftragsverarbeiters (Art. 77 Abs. 3 KOM(2012) 11). Die Sanktionen für Verstöße gegen die Vorschriften der Verordnung sollen von den Mitgliedstaaten selbst festgelegt werden. Die Höchstsumme der Geldbußen reicht aber bei schweren Verstößen bis zu 1.000.000 € und im Fall eines Unternehmens bis zu 2 % seines weltweiten Jahresumsatzes (Art. 79 Abs. 6 KOM(2012) 11).

Verschuldensvermutung zulasten der Verarbeiter

19. Einführung von Regeln für die Verarbeitung bestimmter Kategorien von Daten

Die Verordnung soll speziellen innerstaatlichen Bestimmungen für die Verarbeitung von Daten zu Gesundheitszwecken sowie für Beschäftigungsverhältnisse nicht im Wege stehen (Art. 81–82 KOM(2012) 11). Die Anforderungen der Verordnung müssen dabei aber gewahrt bleiben.

20. Reaktionen auf den Entwurf

Bundestag: Entwurf verstößt gegen Grundsatz der Subsidiarität und ist zu abstrakt

Der deutsche Bundestag hat sich bereits kritisch zur geplanten Datenschutzgrundverordnung geäußert. Der Haupteinwand bezieht sich auf die Tatsache, dass der Entwurf die Prinzipien der Subsidiarität und der Verhältnismäßigkeit nicht berücksichtige. Der Entwurf verdränge ausdifferenzierte Datenschutzregelungen der Mitgliedstaaten zugunsten eines durch ein hohes Abstraktionsniveau geprägten Rechtsakts vollständig.

Bundesrat kritisiert Zersplitterung des Datenschutzrechts

Auch unstreitige Bereiche des deutschen Datenschutzrechts würden infrage gestellt. Der Bundesrat sieht in der Fortentwicklung der geltenden Datenschutzrichtlinie eine viel bessere Lösung zum Datenschutz als die geplante Zersplitterung durch drei verschiedene Rechtsakte mit unterschiedlicher Bindungswirkung für die Mitgliedstaaten, nämlich der Datenschutzgrundverordnung, der vorgeschlagenen Richtlinie zum Datenschutz bei Polizei und Justiz und der bestehenden Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG).

Datenschutzbeauftragte befürchten mehr staatliches Hineinwirken in die Unternehmen

Auch der deutsche Berufsverband der Datenschutzbeauftragten (BvD) sieht in dem Entwurf einen Rückschritt für den Datenschutz in Deutschland. Besonders kritisch äußert er sich gegenüber der Pflicht zur Bestellung eines Datenschutzbeauftragten in Unternehmen erst ab 250 Mitarbeiter. Darin sieht der BvD eine mögliche Gefährdung des Datenschutzes in der Wirtschaft, insbesondere durch die Verarbeitung personenbezogener Daten durch Niederlassungen von Nicht-EU-Unternehmen oder durch Auftragsverarbeiter mit weniger als 250 Mitarbeitern. Der Bürokratieabbau ist laut BvD mit dieser Verordnung ausgeschlossen – im Gegenteil sei ein Bürokratiewachstum „unvermeidlich."

FAZIT

Nach Studien s Verwendung il überhaupt, nu Datenschutzes digitalen Raur soll die 15 Jahr Unternehmen barkeit, die Be: Erweiterung de lobenswerten \ scheint in den (Unternehmen l stelle –, und zw Einführung der risikoreichen Ve Aktivität der Ur Schutz der Rech Bestellung eine ohne dass Art u beschränkt sich zu beschreiben, Mitwirkungsbef der EU-Kommiss wird vielfach kri nommen werde neuen Regelung

AUTOREN

Professor Dr. Thoma ist Dekan der Rechtsw zivilrechtlichen Abteilu Autor und Mitherausge Düsseldorf.

Andra Giurgiu ist Doktorandin und Re Rechtswissenschaften u 2011 arbeitet sie als W Universität Münster.

NWB 19/2012

FAZIT

Nach Studien sorgen sich mehr als zwei Drittel der Bürger der EU-Mitgliedstaaten um die Verwendung ihrer Daten durch Unternehmen. Sie waren der Auffassung, dass sie, wenn überhaupt, nur allzu wenig Kontrolle über ihre Daten hätten. Die Verstärkung des Datenschutzes ist schon aufgrund immer größerer Verlagerung von Daten in den digitalen Raum ein begründetes Anliegen. Die geplante Datenschutz-Grundverordnung soll die 15 Jahre alte Richtlinie 95/46/EG ersetzen und den betroffenen Personen und Unternehmen zusätzliche Rechte verleihen, namentlich das Recht der Datenübertragbarkeit, die Beschränkung der Profilbildung und zusätzliche Auskunftsansprüche. Die Erweiterung des Anwendungsbereichs des europäischen Datenschutzrechts stellt einen lobenswerten Versuch dar, Umgehungen entgegenzuwirken. Auch die Wirtschaft scheint in den Genuss eines industriefreundlicheren Datenschutzes zu kommen. Die Unternehmen brauchen insbesondere einen „One-Stop-Shop" – eine einzige Kontrollstelle –, und zwar in dem Mitgliedstaat, in dem sie ihren Hauptsitz haben. Die Einführung der Folgenabschätzung soll den Schutz der betroffenen Personen bei risikoreichen Verarbeitungen verbessern. Zwar mag die Pflicht zur Dokumentation die Aktivität der Unternehmen erschweren, sie schafft aber Transparenz und trägt zum Schutz der Rechte der betroffenen Personen bei. Umstritten ist aber die Pflicht zur Bestellung eines Datenschutzbeauftragten, die an die Mitarbeiteranzahl geknüpft ist, ohne dass Art und Umfang der Datenverarbeitung berücksichtigt werden. Der Entwurf beschränkt sich leider auch darauf, Konzernstrukturen wie die „Unternehmensgruppe" zu beschreiben, ohne weitere Regelungen für Konzernunternehmen zu schaffen. Die Mitwirkungsbefugnisse der Mitgliedstaaten soll zugunsten von Einwirkungsrechten der EU-Kommission beschränkt werden; deren Recht zum Erlass delegierter Rechtsakte wird vielfach kritisiert. Der Verordnungsentwurf muss noch verhandelt und angenommen werden. Erst zwei Jahre darauf – frühestens ab Mitte 2014 – könnten die neuen Regelungen die aktuellen ersetzen.

AUTOREN

Professor Dr. Thomas Hoeren
ist Dekan der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster, Direktor der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) und vielfacher Autor und Mitherausgeber kommunikationsrechtlicher Veröffentlichungen; 1996 bis Ende 2011 war er Richter am OLG Düsseldorf.

Andra Giurgiu
ist Doktorandin und Rechtsanwältin in der Rechtsanwaltskammer Sibiu (Rumänien). Sie studierte in Sibiu und Marburg Rechtswissenschaften und schloss ein Masterstudium zur Mediation in Rechtskonflikten in Bukarest an. Seit November 2011 arbeitet sie als Wissenschaftliche Mitarbeiterin am ITM an der Juristischen Fakultät der Westfälischen Wilhelms-Universität Münster.