THOMAS HOEREN

Big Data und Datenqualität – ein Blick auf die DS-GVO

Annäherungen an Qualitätsstandards und deren Harmonisierung

Datenqualitätsstandards
Haftung
Datenrichtigkeit
Datenschutzprinzipien
Datenvalidität

■ Wenn eine neue Forschungsperspektive wie Big Data gerade darauf aufsetzt, irrelevante Daten ungefiltert auszuwerten, muss sich auch die Frage nach der Datenqualität stellen. Dafür spricht auch, dass die europäische Datenschutzgrundverordnung (DS-GVO) die Einhaltung von Datenqualitätsstandards zu einer bußgeldsanktionierten Forderung an Datenverarbeiter erhebt. Doch was bedeutet Datenqualität (vgl. hierzu erste Thesen von Hoeren, MMR 2016, 8 ff.)? Wie passt diese Forderung ins System des allgemeinen Zivilrechts und in die Struktur des Datenschutzrechts?
Lesedauer: 17 Minuten

■ If a new research perspective such as Big Data is based on assessing irrelevant data without filtering, then the question of data quality must also be regarded. This is also supported by the fact that the European General Data Protection Regulation (DS-GVO) makes the adherence of data quality standards a punishable administrative fine requirement for data processors. But what does data quality mean (see here the first theses of Hoeren, MMR 2016, 8 et seq.)? How does this demand fit into the system of general civil law and the structure of data protection law?

I. Einführung

Die Forderung nach Datenqualität ist alt.[1] Schon die europäische Datenschutzrichtlinie (DS-RL, vgl. näher zu den noch wesentlich älteren Regelungen und Guidelines unter II.) enthielt in Art. 6 unter der Rubrik „Datenschutzgrundsätze" ein Prinzip, wonach personenbezogene Daten „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein" müssten. Allerdings fehlte bei dieser Forderung jedwede Sanktion. Es kann daher nicht verwundern, dass der deutsche Gesetzgeber im BDSG die Grundsätze gar nicht umsetzt[2] (anders als Österreich[3] oder die Schweiz[4]). Umso geringer dürfte die Bedeutung in der datenverarbeitenden Wirtschaft zumindest in Deutschland eingeschätzt worden sein.

Das Schweigen des deutschen Rechts verblüfft allerdings, wenn man sich die aktuelle Bedeutung von Art. 6 DS-RL in der rechtspolitischen Diskussion ansieht. Nicht ohne Grund betont der *EuGH* im Google-Urteil[5] die Grundsätze der Datenqualität. Jede Verarbeitung personenbezogener Daten müsse den in Art. 6 DS-RL aufgestellten Grundsätzen in Bezug auf die Qualität der Daten genügen (Rdnr. 73).

Aus dem Grundsatz der Datenrichtigkeit ergebe sich auch, „dass auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten im Laufe der Zeit nicht mehr den Bestimmungen der Richtlinie entsprechen kann, wenn die Daten für die Zwecke, für die sie erhoben oder verarbeitet worden sind, nicht mehr erforderlich sind" (Rdnr. 93).

Die Verankerung dieses Prinzips im Datenschutzrecht war allerdings eher unglücklich und wenig durchdacht. Mit Datenschutz hat die Frage der Datenqualität wenig zu tun. Wer auf Grund überalterter Daten ein äußerst positives, aber leider mit Daten des reichen Onkels vermengtes Scorebild bei der Bonitätsauskunft bekommt, fühlt sich nicht betroffen. Umgekehrt ist nicht einzusehen, warum von der Frage der Datenrichtigkeit nur natürliche Personen betroffen sein sollen. Man denke nur an den Fall Kirch-Gruppe/Deutsche Bank und die fatalen Folgen nicht korrekter Hinweise auf die Zahlungsfähigkeit einer Unternehmensgruppe.[6] Insofern ist die Forderung der Datenqualität primär eine Frage des allgemeinen Zivilrechts und nicht des Datenschutzrechts.

Datenqualität ist zunächst einmal etwas, das im Interesse der verarbeitenden Industrie liegt. Das Ziel jedes Datenverarbeiters liegt darin, im eigenen Interesse möglichst viele valide, aktuelle und korrekte Daten zu verarbeiten. In besonders sicherheitsrelevanten Bereichen finden sich daher schon normative Fragmente einer Pflicht zur Gewährleistung der Datenqualität. So gilt für Flugorganisationen europaweit ein entsprechendes Gebot[7]; Ähnliches gilt für Statistikbehörden[8] oder Finanzdienstleister[9].

Das Gebot stellt sich zivilrechtlich vor allem im Hinblick auf die allgemeinen Sanktionen bei der Verwendung falscher Daten. Negative Folgen für den Betroffenen wurden und werden häufig über Schadensersatzsanktionen aus dem allgemeinen Zivilrecht kompensiert, etwa über § 824 BGB oder die Verletzung vorvertraglicher Sorgfaltspflichten aus § 280 BGB. Eine klar konturierte Rechtsprechung zu einer solchen Informationshaftung gibt es allerdings nicht.

---

1 Fußnoten beziehen sich im Weiteren nur auf die zum Verständnis des Texts notwendigen Belege; vgl. ferner auch die Thesen zur Datenqualität, *Hoeren*, MMR 2016, 8 ff.

2 Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze v. 22.5.2001, BGBl. I, S. 904.

3 § 6 des österr. Bundesgesetzes über den Schutz personenbezogener Daten, österr. BGBl. I, Nr. 165/1999.

4 Art. 5 des schweizerischen DSG v. 19.6.1992, AS 1993, 1945.

5 *EuGH* ZD 2014, 350 m. Anm. *Karg* – Google Spain und Google; ferner *EuGH*, C-465/00, ECLI:EU:C:2003:294, Rdnr. 65 – Österreichischer Rundfunk u.a.; *EuGH* ZD 2012, 33, Rdnr. 26 – ASNEF/FECEMD und *EuGH* ZD 2013, 437, Rdnr. 33 – Worten.

6 Dazu u.a. *BGH*, U. v. 24.1.2006 – XI ZR 384/03 und *Derleder*, NJW 2013, 1786 ff.; *Höpfner/Seibl*, BB 2006, 673 ff.

7 Art. 6 der Luftfahrtdaten-Qualitätsanforderungen-Verordnung.

8 Art. 12 VO (EG) Nr. 223/2009 v. 11.3.2009, ABl. 2009, Nr. L 87/169.

9 § 17 Solvabilitätsverordnung v. 14.12.2009, BGBl. I, S. 2926 und § 4 der Versicherungsmeldeverordnung v. 18.4.2016, BGBl. I, S. 793.

Dementsprechend blieb die Regelung zur Datenqualität ein mit wenig Leben gefülltes Relikt. Zu Recht betonte daher eine *Expertenkomission der US-Regierung* bereits 1977: „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".[10]

Der Markt und damit auch das allgemeine Zivilrecht sollten demnach über das Versagen der Unternehmen bei der Verwendung veralteter oder unrichtiger Daten entscheiden.

II. Vorgeschichte zur Datenqualität

Spätestens hier zeigt sich, dass es ein wichtiges Desiderat der Rechtsgeschichte bleibt, die Geschichte des Datenschutzrechts aufzuarbeiten.[11]

1. Grundsatz der Datenqualität – Mutterland: USA

Erstaunlicherweise stammt der Grundsatz der Datenqualität aus den USA, eigentlich einem der Länder, dem ein europäischer Datenschützer das wohl eher nicht zugetraut hätte. Der noch heute geltende US Privacy Act 1974[12] enthält zahlreiche Anforderungen an eine Datenverarbeitung im Hinblick auf die „accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness"[13].

Die Regelung bezieht sich allerdings nur auf die Verarbeitung personenbezogener Daten durch den Staat (agencies) und sicherte dem Betroffenen über die Gewährleistung der Datenqualität einen fairen Entscheidungsprozess der Behörde.

In den USA wurde ferner 2001 als Bestandteil des Consolidated Appropriations Act der Data Quality Act (DQA) – auch Information Quality Act (IQA) genannt – verabschiedet. Er ermächtigt das *Office of Management and Budget* dazu, Richtlinien zu erlassen, die die Qualität und Integrität von Informationen sicherstellen und erhöhen sollen, die durch staatliche Einrichtungen veröffentlicht werden (Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies[14]).[15] Darüber hinaus sollen Mechanismen geschaffen werden, die es den von der Verbreitung fehlerhafter Informationen Betroffenen ermöglichen, dies anzuzeigen und korrigieren zu lassen.[16]

Eine Differenzierung zwischen personenbezogenen und nichtpersonenbezogenen Daten wird hierbei allerdings nicht vorgenommen. Hinzu kommt, dass sich der Anwendungsbereich des DQA in der Verbreitung von Informationen durch staatliche Behörden gegenüber der Öffentlichkeit erschöpft.[17]

Darüber hinaus gibt es kein bundeseinheitliches Gesetz, das Vorgaben für die Datenqualität von personenbezogenen Daten für den nicht-staatlichen Bereich aufstellt. Da das US-amerikanische Datenschutzrecht durch zahlreiche Gesetze und Leitlinien auf Bundes- und Staatenebene geregelt ist, gibt es vereinzelt bereichsspezifische Gesetze, die Regelungen zur Datenqualität enthalten (z.B. der Fair Credit Reporting Act oder der Health Insurance Portability and Accountability Act of 1996). Der Fair Credit Reporting Act verpflichtet z.B. Nutzer von Verbraucherberichten, Verbraucher über ihr Recht aufzuklären, die Richtigkeit der sie betreffenden Berichte zu bestreiten. Ein weiteres Beispiel ist die HIPAA Security Rule, wonach betroffene Einrichtungen (z.B. Gesundheitsprogramme, Abrechnungsstellen für Gesundheitsversorgung oder Gesundheitsversorgungsunternehmen) die Integrität von elektronisch geschützten Gesundheitsdaten sicherstellen müssen.[18]

2. OECD-Guidelines 1980

Die US-Grundsätze wurden übernommen und ausgeweitet in den OECD-Guidelines 1980[19]. Dabei gilt es zu beachten, dass die Richtlinien von vornherein als nicht verbindliche Empfehlungen konzipiert waren.[20] Guideline 8 enthält den allgemeinen Hinweis auf das Gebot der „accuracy" der Daten. Zur Erläuterung wurde darauf hingewiesen: „Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept"[21].

Noch detaillierter geregelt war die Frage der Datenqualität in einer zweiten OECD-Empfehlung aus dem Jahre 1980, den „15 Principles on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters."[22] Principle Nr. 5 enthielt detaillierte Ausführungen zur Datenqualität, die weit über den heutigen Stand hinausgingen: „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."

Schon damals gab es Zweifel innerhalb der *OECD-Expertengruppe*, ob Datenqualität eine Kategorie des Datenschutzes ist: „In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection."[23]

So stritten sich auch externe Experten[24] um die Sinnhaftigkeit eines solchen Konzepts: „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."[25]

Zu Recht wurde immer wieder betont, dass es sich um ein allgemeines Fachkonzept der Informatik handele: „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. Organisations 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

---

10 S. unter: https://epic.org/privacy/ppsc1977report/c1.htm.

11 Ansätze dazu bei *Büllesbach/Garstka*, CR 2005, 720 ff.; *v. Lewinski*, in: Arndt u.a., Freiheit – Sicherheit – Öffentlichkeit, 2009, S. 196 ff.

12 Vgl. unter: http://www.archives.gov/about/laws/privacy-act-1974.html.

13 552 a (4) US Privacy Act 1974 betreffend die Datenverarbeitung staatlicher „agencies".

14 Vgl. unter: https://www.whitehouse.gov/omb/fedreg_final_information_quality_guidelines/.

15 Vgl. unter: https://www.whitehouse.gov/omb/fedreg_reproducible.

16 Subsection (2) (B) of the DQA.

17 *Dallas Wait/Maney*, Regulatory Science and the Data Quality Act, in: Environmental Claims Journal, S. 148.

18 *Jay*, Data Protection & Privacy 2015, London 2015, S. 210 f.

19 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, abrufbar unter: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; dazu *Patrick*, Privacy Restrictions, in: Jurimetrics Vol. 21, No. 4 (Summer 1981), 405 ff.

20 Abrufbar unter: http://idpl.oxfordjournals.org/content/1/1/6.full.pdf, dort auf S. 11.

21 Abrufbar unter: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#comments.

22 Abrufbar unter: http://www.statewatch.org/news/2007/may/oecd-1980s-data-protection-principles.pdf.

23 So steht es ausdrücklich in den Erläuterungen zu den Guidelines.

24 Zur *Expertengruppe der OECD* s. *Fuster*, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, S. 78 f.

25 *Roger Clarke*, The OCED Guidelines: A template, Paper 1989, abrufbar unter: http://www.rogerclarke.com/DV/PaperOECD.html.

people concerned, but to ensure that their own decision-making is based on data of adequate quality."[26]

3. Art. 6 DS-RL und die Auswirkungen in Kanada

Die damals schon weltweit anerkannten OECD-Standards wurden später in die DS-RL aufgenommen.[27] Im ersten Entwurf der Richtlinie[28] findet sich nur eine allgemeine Beschreibung der Erlaubnistatbestände für eine Datenverarbeitung der öffentlichen Hand.[29] Erst in Art. 16 findet sich die Pflicht, „accurate" personenbezogene Daten zu verarbeiten – ohne Bezug zur Frage der Zulässigkeit der Datenverarbeitung. In der zweiten Version von Oktober 1992[30] wurde diese Regelung dann zu Art. 6 des Texts und damit in die Nähe der Zulässigkeit der Verarbeitung gerückt. Sanktionen waren nicht vorgesehen. Auch jetzt noch war die Verbindung der Datengrundsätze zur Zulässigkeit der Verarbeitung ungeklärt. Die Datengrundsätze behielten ihren Charakter als Programmsätze mit Empfehlungscharakter.

Länder wie Kanada schlossen sich unter dem Druck der EU mit dem PIDEDA Act im Jahre 2000 den dortigen Grundsätzen der Datenqualität an: „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 sog. Guidelines wurde in Kanada der Grundsatz der „accuracy" noch konkretisiert: „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]

Von den EU-Ländern erwies sich bei der Umsetzung der EU-Datengrundsätze vor allem Großbritannien als Pionier. In Großbritannien wurde die DS-RL mit dem Data Protection Act 1998 umgesetzt. Während der Data Protection Act 1998 die Grundzüge des britischen Datenschutzrechts regelt, erfolgt eine Konkretisierung dieser Vorschriften i.R.v. Verordnungen (statutory instruments) und Rechtsvorschriften (regulations).[33] Der Data Protection Act 1998 stellt insgesamt acht Datenschutzprinzipien auf. Die Qualitätsregel des Art. 6 Abs. 1 lit. d DS-RL wurde i.R.d. vierten Datenschutzprinzips umgesetzt, welches vorschreibt, dass personenbezogene Daten aktuell und sachlich richtig sein müssen.[34]

Aus Gründen der Praktikabilität trifft der Data Protection Act Sonderregelungen für die Fälle, in denen Personen Informationen über sich selbst bereitstellen oder personenbezogene Daten von Dritten erlangt werden. Auch wenn in diesen Fällen personenbezogene Daten sachlich falsch sind, wird dies nicht als Verstoß gegen das vierte Datenschutzprinzip angesehen, wenn beim Betroffenen oder einem Dritten falsche Informationen korrekt erfasst wurden, der Verantwortliche angemessene Maßnahmen (reasonable steps) zur Sicherung der Datenqualität getroffen hat und die Daten erkennen lassen, dass der Betroffene den Verantwortlichen auf die Ungenauigkeiten hingewiesen hat.[35]

Was genau unter angemessenen Maßnahmen zu verstehen ist, richtet sich nach der Art der personenbezogenen Daten und danach, welche Bedeutung die Korrektheit im Einzelfall hat.[36]

Im Jahr 2013 hob der *UK Court of Appeal* im Fall „Smeaton v. Equifax Plc" hervor, dass der Data Protection Act 1998 keine absolute Verpflichtung zur Gewährleistung der Richtigkeit personenbezogener Daten begründe, sondern nur die Vornahme angemessener Maßnahmen verlange, welche die Datenqualität sicherstellen sollen. Die Angemessenheit ist nach dem jeweiligen Einzelfall zu beurteilen. Auch ergebe sich aus dem vierten Datenschutzprinzip keine parallele Verpflichtung auf dem Gebiet des Deliktsrechts.[37]

Trotz dieser internationalen Welle kurz vor der Jahrtausendwende blieb das Prinzip der Datenqualität allerdings nahezu unbeachtet, als „the most forgotten of all of the internationally recognized privacy principles"[38].

III. Datenqualität in der Datenschutzgrundverordnung

Die Rechtsnatur der Datengrundsätze änderte sich erst mit der DS-GVO.

1. Erstaunlich: Art. 5 als Grundlage von Bußgeldern

Am Anfang hatte die Verordnung noch das Ziel, die Grundsätze aus der DS-RL als Empfehlungen ohne Sanktionen nahezu wörtlich zu übernehmen.[39]

Irgendwann während der Trilog-Gespräche änderte sich jedoch offensichtlich die Haltung, ohne dass man die Akteure aus den ohnehin nicht veröffentlichten Trilog-Papieren identifizieren könnte. Jedenfalls tauchte im Trilog-Kompromisspapier von Dezember 2015[40] auf einmal der Hinweis auf, dass auch die Datenschutzgrundsätze mit dem höchsten Level der Bußgeldsanktionen versehen werden (Art. 83 Abs. 5 lit. a). Seitdem ist auch der Grundsatz der Datenqualität seinem Status als reiner Programmsatz entronnen und gilt nunmehr auch als ein ordnungswidrigkeitsrechtlicher Bußgeldtatbestand. Diese von der Öffentlichkeit kaum beachtete Veränderung ist fatal und schwierig, wie im Weiteren zu zeigen sein wird.

Fraglich ist z.B., ob tatsächlich ein Bußgeld i.H.v. maximal 4% des Jahresumsatzes bei Verletzung der Qualitätsregel verhängt werden könnte. Denn das Kriterium der „sachlichen Richtig-

---

26 *Clarke* (o. Fußn. 25).
27 Dazu allg. *Cate*, EU Data Protection Directive, Information Privacy, and the Public Interest, 80 Iowa L. Rev. 431 (1994-95).
28 Abrufbar unter: http://aei.pitt.edu/3768/1/3768.pdf.
29 S. KOM (90)314 endg. SYN 287, S. 53.
30 Vgl. unter: http://a[LI]ei.pitt.edu/10375/.
31 Personal Information Protection and Electronic Documents Act (PIPEDA), (S.C. 2000, c. 5); dazu *Austin*, Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA, University of Toronto Law Journal 56.2 (2006) 181-215.
32 Sect. 4.6. der Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96; s. dazu auch *Scassa* u.a. (Hrsg.), Electronic commerce and Internet Law in Canada, 2. Aufl. 2012, S. 135 ff.
33 Abrufbar unter: http://united-kingdom.taylorwessing.com/uploads/tx_sirupla wyermanagement/NB_000168_Overview_UK[LI]_data_protection_law_WEB.pdf.
34 Sch. 1 Pt. 1 Para. 4 Data Protection Act 1998; ausf. Informationen zum vierten Datenschutzprinzip, abrufbar unter: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/.
35 Sch. 1 Pt. 2 Para. 7 Data Protection Act 1998.
36 Abrufbar unter: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/.
37 Smeaton v Equifax Plc [2013] ECWA Civ 108, abrufbar unter: http://www.bailii.org/ew/cases/EWCA/Civ/2013/108.html.
38 Cline Data Quality, Computerworld v. 18.9.2007, abrufbar unter: http://www.computerworld.com/article/2541015/security0/data-quality----the-forgotten-privacy-principle.html.
39 S. Art. 5 Abs. 1 lit. d i.d.F. v. 11.6.2015: „Personenbezogene Daten müssen (d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein".
40 Interinstitual File 2012/0011 (COD) Nr. 15039/15 v. 15.12.2015.

keit" ist unklar. Was bedeutet „sachlich"? Dem Begriff liegt eine duale Kategorisierung mit „richtig" und „unrichtig" zu Grunde. Sie basiert auch auf der alten, schon bei § 35 BDSG diskutierten Abgrenzung zwischen Tatsachen und Meinungen.[41] Tatsachenbehauptungen können „richtig" oder „unrichtig" sein, nicht aber Werturteile. Ist „richtig" identisch mit „wahr"? Der englische Text der Verordnung spricht nicht von „richtig", sondern von „accurate".

Dieser Terminus ist vielschichtiger als die deutsche Übersetzung. Er umfasst die Zielgerichtetheit, Genauigkeit, Exaktheit i.S.d. Mathematik. Er stammt aus den Ingenieurwissenschaften und der frühen Informatik und findet sich aus dieser Wurzel heraus als Zentraldefinition in modernen ISO-Normen.[42] Er findet sich in diesem Sinne auch in den o.g. Spezialregelungen für Statstikbehörden oder Luftfahrtorganisationen. Der Terminus war insofern auch nie im ontologischen Sinne gemeint und damit auch nicht auf die bipolare Beziehung von „richtig" und „unrichtig" bezogen. Für den Ordnungswidrigkeitentatbestand ist der Begriff nach Art. 103 Abs. 2 GG eindeutig zu unbestimmt.[43] Zugleich besteht die Gefahr, dass die Datenschutzaufsicht zur „Megabehörde für richtige Daten" mutiert, vor allem im Lichte des weiten Begriffs des Personenbezugs in Art. 4 Abs. 1 DS-GVO. Die Datenschutzaufsichtsbehörde ist gar nicht in der Lage, die mathematisch-statistische Validität von Daten zu beurteilen. Dies war bislang auch nicht ihre Aufgabe und ihre Kernkompetenz. Die Datenschutzaufsichtsbehörde müsste dann selbstständig mit Hilfe von Mathematikern die Validität überprüfen.

2. Verhältnis zu den Betroffenenrechten

Zu beachten ist auch, dass die DS-GVO selbst eigene Verfahrensinstrumente zu Gunsten des Betroffenen und der Sicherung der in seinem Sinne richtigen Daten vorsieht. Nach Art. 16 DS- GVO hat der Betroffene einen Anspruch auf Richtigstellung (rectification) bei „inaccurate personal data". Art. 18 DS-GVO ergänzt den Schutz des Betroffenen durch das Recht auf Beschränkung der Verarbeitung in Fällen, in denen die Richtigkeit der Daten vom Betroffenen bestritten wird; auf einen solchen Widerspruch hat der Datenverarbeiter die Möglichkeit, die Richtigkeit der Daten zu überprüfen. Art. 16 und Art. 18 DS-DVO greifen mit „inaccurate" bzw. „accuracy" die Formulierung aus Art. 5 DS-GVO bewusst auf und korrespondieren insofern mit dem Gebot der Datenrichtigkeit. Die Vorschriften zeigen auch, dass sich Art. 5 DS-GVO nicht daran erschöpft, i.S.d. Betroffenen die zu seinen Gunsten richtigen Daten zu sichern. Art. 83 Abs. 5 lit. b DS-GVO sanktioniert die Einhaltung der Betroffenenrechte ebenfalls mit der höchsten Bußgeldstufe. Allerdings meint „accuracy" hier „Richtigkeit" im o.g. Sinne. Es gilt, eine Vermengung zweier Konzepte in der Verordnung interpretatorisch zu vermeiden: den technologisch-relationalen Begriff der „accuracy" mit der ontologisch-bipolaren Thematik der „Richtigkeit" von Behauptungen über den Betroffenen. Das Richtigkeitskonzept der Art. 12, 16 DS-GVO hat nichts mit dem „accuracy"-Modell von Art. 5 DS-GVO zu tun. Deshalb ist es auch gefährlich, die Begriffe in Art. 5 und Art. 12, 16 DS-GVO identisch zu interpretieren.

3. Verhältnis Datenqualität und Zulässigkeit der Datenverarbeitung

Auch ist unklar, wie sich die Beziehung von Art. 5 und Art. 6 DS-GVO gestaltet. Zunächst einmal stellt sich die Frage, ob nicht das Gebot der Datenrichtigkeit zu einem Erlaubnistatbestand i.S.v. Art. 6 lit. f DS-GVO genutzt werden kann. Ein legitimes Interesse für die Datenverarbeitung wäre dann die Tatsache, dass die Daten nach Art. 5 DS-GVO immer „up-to-date" gehalten werden müssen.

4. Art. 5 DS-GVO als abstraktes Gefährdungsdelikt

Denkbar wäre eine restriktive Auslegung von Art. 5 oder die Einordnung als abstraktes Gefährdungsdelikt.[44] Die o.g. Einstiegsfrage stellt sich hier erneut: Müsste man nicht Art. 5 DS-GVO teleologisch reduzieren und darauf beschränken, die Datenrichtigkeit nur dann einzufordern, wenn die Nichteinhaltung zu Lasten des Betroffenen geht? In diesem Sinne hat eine *australische Juristenkommission*[45] entsprechende Regelungen im australischen Datenschutzrecht verstanden: „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."

Ähnliche Korrekturansätze finden sich bereits in der o.g. britischen Rechtsprechung. Allerdings sprechen die allgemeine Gefahrenquelle und die erhöhten Risiken, die von großen Datenpools im Zeitalter von Big Data ausgehen, für das Vorliegen eines Gefährdungstatbestands. Auf solche Gefahrenlagen weisen auch ausländische Gerichte hin, darunter der kanadische *Federal Court Ottawa,* also ein Gericht aus dem Staat, der sich am weitesten in Sachen Datenqualität im Datenschutzrecht nach vorne gewagt hat. So hat der *Federal Court* in der Entscheidung „Nammo"[46] betont: „An organization's obligation 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."

Und die *Datenschutzaufsicht in Ottawa* betont in ihrem Tätigkeitsbericht 2011:[47] „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."

Man sollte diese beiden Gedanken verbinden. Art. 5 lit. d DS-GVO ist die Grundlage eines abstrakten Gefährdungsdelikts und gerade deshalb restriktiv auszulegen. Dies gilt umso mehr, als Art 5 lit. d DS-GVO nunmehr nach Art. 83 Abs. 5 lit. a DS-GVO auch Grundlage eines Ordnungswidrigkeitenverfahrens mit massiven Bußgeldern sein kann. Allerdings kann und darf die restriktive Auslegung nicht dazu führen, dass aus einem abstrakten Gefährdungsdelikt ein konkretes wird. Dies würde den Wortlaut von Art. 5 lit. d DS-GVO konterkarieren. Eine Auslegung, die weitreichende Auslegungseingriffe bei einem gerade verabschiedeten Verordnungstext vornimmt, ist vorläufig erst einmal zu vermeiden. Insofern ist Art. 5 lit. d DS-GVO i.E. als abstrakter Gefährdungstatbestand und damit weit auszulegen. Die korrespondierende Regelung im neuen Bußgeldtatbestand gilt es jedoch eng und behutsam einzusetzen.

---

41 S. dazu *Mallmann*, in: Simitis, BDSG, 8. Aufl. 2014, § 20 Rdnr. 17 ff.; *Dix*, in: Simitis, BDSG, 8. Aufl. 2014, § 35 Rdnr. 13.

42 ISO 5725-1:1994.

43 BVerfGE 75, 329, 341.

44 *Anastasopoulou*, Delikstypen zum Schutz kollektiver Rechtsgüter, 2005, S. 63 ff.; *Graul*, Abstrakte Gefährdungsdelikte und Präsumptionen im Strafrecht, 1989, S. 144 ff.; *Gallas*, Abstrakte und konkrete Gefährdung, in: FS Heinitz, 1972, S. 171.

45 Australian Law Reform Commission For Your Information: Australian Privacy Law and Practice (ALRC Report 108), abrufbar unter: http://www.alr[LI]c.gov.au/publications/27.%20Data%20Quality/balancing-data-quality-and-other-privacy-interests.

46 Nammo v. TransUnion of Canada Inc., 2010 FC 1284, abrufbar unter: http://www.fasken.com/files/upload/Nammo-v-Transunion-2010-FC-12[LI]84.pdf.

47 PIPEDA Report of Findings Nr. 2011-009 Credit Bureau Purges Loan History from Individual's Credit; ähnl. bereits PIPEDA Case Summary Nr. 2003-224 Bank failed to correct credit rating discrepancy and to provide access to financial records; PIPEDA Case Summary Nr. 2003-163 Bank fails to maintain up to date, accurate personal information Report without his Knowledge.

IV. Fazit und Ausblick

Das Beispiel der ausländischen Regelungen etwa in den USA und Kanada sowie der Weg von der DS-RL zur DS-GVO zeigen, dass die steigende Relevanz des Themas Datenqualität immer mehr erkannt wird. Allerdings kann „veracity"[48] bzw. „accuracy" von Daten nur dann erreicht werden, wenn wirksame Instrumentarien geschaffen werden, die Qualitätsstandards für Daten gewährleisten können. Sowohl die DS-RL als auch der Data Quality Act stellen einen Weg in die richtige Richtung dar. Allerdings wird der bloße Verweis auf die Einhaltung von Qualitätsstandards nicht per se ausreichen, um Art. 5 DS-GVO einzuhalten. Erinnert sei an den o.g. kanadischen Nammo-Fall:[49] „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."

Diese Warnung ist besonders deshalb wichtig, weil es im Bereich der Datenqualität keine weltweit gültigen und anerkannten Industriestandards gibt. Wie an anderer Stelle beschrieben,[50] gibt es zwar einige nationale Forschungsansätze in dieser Frage. Aber von einer Harmonisierung und echten Standardisierung sind wir noch weit entfernt. Insofern sollten die Datenschutzaufsichtsbehörden den neu beschrittenen Weg der strafrechtlichen Sanktionierung von Datenqualität sehr behutsam und mit Augenmaß beschreiten.

Prof. Dr. Thomas Hoeren
ist Direktor der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster und Mitherausgeber der ZD.

48 Anknüpfend an *Douglas'* "Four V's of Big Data" (Volume, Variety, Velocity und Veracity).
49 Nammo v. TransUnion of Canada Inc., 2010 FC 1284.
50 *Hoeren*, MMR 2016, 8 ff.

PHILIP LAUE

Öffnungsklauseln in der DS-GVO – Öffnung wohin?

Geltungsbereich einzelstaatlicher (Sonder-)Regelungen

Räumlicher Anwendungsbereich
Sitzlandprinzip
Territorialitätsprinzip
Rom I-VO

■ Zentrales Ziel der Datenschutzgrundverordnung (DS-GVO) ist ein einheitlicher Rechtsrahmen zum Datenschutz in der Europäischen Union. Dennoch sieht die DS-GVO an vielen Stellen Öffnungsklauseln vor, die den Mitgliedstaaten Spielraum für nationale (Sonder-)Regelungen geben. Auch in Zukunft kann es daher erforderlich sein, den Geltungsbereich einzelstaatlicher Datenschutzvorschriften zu bestimmen. Im Gegensatz zur bisherigen Rechtslage enthält die DS-GVO dabei jedoch keine allgemeine Kollisionsnorm. Anhand verschiedener Kategorien von Öffnungsklauseln und im Zusammenhang mit den Rahmenbedingungen von Einwilligungen von Kindern sowie Einwilligungsbeschränkungen bei besonderen Kategorien von Daten lässt sich das jeweils anwendbare Recht eines Mitgliedstaats aber nach dem Sitzlandprinzip, dem Territorialitätsprinzip bzw. nach den Grundsätzen des internationalen Privatrechts ermitteln.
Lesedauer: 19 Minuten

■ The central goal of the General Data Protection Regulation (DS-GVO) is a uniform legal framework for data protection in the European Union. Nevertheless, the General Data Protection Regulation has many opening clauses, which give the Member States leeway for national (special) arrangements. Thus, it can also be necessary in the future to determine the area of application of data protection provisions of individual states. In contrast to the hitherto legal situation, the General Data Protection Regulation does not contain any general conflict of law rule. Based on the various categories of opening clauses and in connection with the framework conditions of consent of children, as well as the limitation of consent in special categories of data, the respective applicable law of a Member State can be determined by way of the domicile principle, the territorial principle, or, as the case may be, the principles of international private law.

I. Einleitung

Nach einem mehrjährigen Marathon von Gesprächen, Diskussionen und Verhandlungen trat am 24.5.2016 die Datenschutzgrundverordnung (DS-GVO) in Kraft. Ab dem 25.5.2018 wird sie dann auch gem. Art. 99 Abs. 2 DS-GVO in jedem EU-Mitgliedstaat als geltendes Recht unmittelbare Anwendung finden.[1] Zum gleichen Zeitpunkt tritt gem. Art. 94 Abs. 1 DS-GVO die EU-Datenschutzrichtlinie (DS-RL)[2] aus dem Jahr 1995 außer Kraft. Deren Umsetzung in einzelstaatliches Recht hatte zu einem Flickenteppich unterschiedlicher mitgliedstaatlicher Regelungen und einem i.E. uneinheitlichen Datenschutzniveau in Europa geführt. Erklärtes Ziel der DS-GVO ist es, „einen soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union" zu schaffen, um insbesondere das Binnenmarktwachstum zu fördern (Erwägungsgrund 7 DS-GVO). Ein gleichwertiges Schutzniveau bei der Verarbeitung in sämtlichen EU-Mitgliedstaaten soll dabei „ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen ... gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union ... beseitigen" (Erwägungsgrund 10 DS-GVO).

Tatsächlich wurde die angestrebte Vollharmonisierung des europäischen Datenschutzrechts jedoch nicht erreicht. Vielmehr ent-

1 Die Vertragsstaaten des Europäischen Wirtschaftsraums (EWR), d.h. Island, Liechtenstein und Norwegen, sind vom Anwendungsbereich der DS-GVO nicht unmittelbar erfasst, da sich diese nur an die Mitgliedstaaten der EU richtet. Auf Grund des Vertrags über den EWR sind sie allerdings verpflichtet, die Anforderungen des Europäischen Binnenmarkts ebenso umzusetzen wie EU-Mitgliedstaaten, darunter fällt auch die DS-GVO.
2 RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.