

Datenrichtigkeit*

Beitragsreihe „Input Control – Datenqualität und Datenvalidität als Grundlage rechtlicher Automatisierungsprozesse“,
Abschnitt „Allgemeines“

Prof. Dr. Moritz Hennemann | Inhaber des Lehrstuhls für Europäisches und Internationales Informations- und Datenrecht, Juristische Fakultät, Universität Passau | Affiliate am Berkman Klein Center for Internet & Society, Harvard University

5. Mai 2020

LR 2020, Seiten 77 bis 86 (insgesamt 10 Seiten)

Dieser Beitrag – ursprünglich als Auftakt zur Tagung „Input Control – Datenqualität und Datenvalidität als Grundlage rechtlicher Automatisierungsprozesse“ angedacht – soll einen kurzen Einblick in die Höhen und Tiefen, vielleicht auch Untiefen, der facettenreichen Datenrichtigkeit geben. 1

I. Eine „richtig“ kurze Einleitung...

Daten können nach landläufiger Auffassung *richtig* oder *unrichtig* sein. Daten im Sinne des Trägermediums sind natürlich nicht richtig oder unrichtig. Nur bestimmte Informationen, nämlich Tatsachen, können richtig oder unrichtig sein.¹ Zumindest im Lichte der Terminologie der Datenschutz-Grundverordnung (DS-GVO) will allerdings auch ich nachfolgend pauschal (und damit eigentlich *unrichtig*) von *Daten* sprechen. 2

* Gekürzte Schriftfassung meines für die Tagung „Input Control – Datenqualität und Datenvalidität als Grundlage rechtlicher Automatisierungsprozesse“ (19./20. März 2020, München) vorbereiteten Vortrags. Die Vortragsform wurde beibehalten. Stand des Beitrags ist März 2020.

¹ Zur Diskussion, ob und inwieweit Werturteile dem datenschutzrechtlichen Grundsatz der Datenrichtigkeit unterfallen, Herbst, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 60 und Art. 16 DS-GVO Rn. 8; Schantz, in: BeckOK Datenschutzrecht, 30. Ed. (1.2.2019), Art. 5 DS-GVO Rn. 27.

II. Von richtigen und unrichtigen Daten

Produktbezogen gesprochen steht mit der Datenrichtigkeit ein Aspekt der *Datenqualität* in Rede², die bislang aus rechtswissenschaftlicher Sicht wenig Aufmerksamkeit (und auch kaum Kritik) erfahren hat.³ Aus der Perspektive der Informatik sind damit Kriterien wie *availability*, *usability*, *reliability* und *relevance* angesprochen.⁴ Die Sicherstellung von Datenqualität aus rechtlicher Perspektive ist – wie *Hoeren* zutreffend betont – „primär eine Frage des allgemeinen Zivilrechts und nicht des Datenschutzrechts“⁵. Datenqualität wird zuvörderst vertraglich sichergestellt.⁶ Denn Datenrichtigkeit (zumindest im datenschutzrechtlichen Sinne) ist nicht mit Qualität im Sinne von Präzision oder Passgenauigkeit gleichzusetzen. Die Angabe eines Alters als „zwischen 30 und 35 Jahren“ oder als „34 Jahre 8 Monate und 5 Tage“ kann jeweils *richtig* sein⁷, ob *präzise* oder *zweckmäßig* hängt vom Verwendungs- bzw. Verarbeitungskontext bzw. der jeweiligen, oftmals vertraglich determinierten, Qualitätserwartung ab.

3

Die Unterscheidung zwischen *richtig* und *unrichtig*, die Zuschreibung anhand dieser binären Codierung⁸, kann nicht ohne eine Projektionsfläche erfolgen. Diese Projektionsfläche ist ein relevanter Ausschnitt der *Realität*.⁹ Etwas lapidar wird manchmal in datenschutzrechtlichen Kommentierungen von einem Nicht-Übereinstimmen mit der Realität¹⁰ oder mit der Wirklichkeit¹¹ gesprochen. *Frenzel* etwa weist genauer darauf hin, dass es um die Ermöglichung einer Rekonstruktion geht, um eine „Repräsentation der Realität“.¹² Im Zentrum der Unrichtigkeit soll also ein Abweichen der in dem Datum enthaltenen Information von dem jeweiligen rechtstatsächlichen Bezugspunkt stehen. Denn nur in diesem Sinne kann eine Richtigkeit im eigentlichen Sinne bestimmt werden. Im Übrigen heißt dies natürlich ebenso wenig, dass Daten bzw. Datenmengen die Realität *umfänglich abbilden*.¹³ Und umgekehrt, verarbeitet werden können Informationen nur, wenn und soweit diese

4

² Siehe etwa Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.), Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 136.

³ Grundlegend Hoeren, MMR 2016, 9; ders., ZD 2016, 459; Chen, EDPL 2018, 36.

⁴ Siehe hierzu und näher Hoeren, MMR 2016, 8 (11) m. w. N.

⁵ Hoeren, ZD 2016, 459 (459). Siehe auch ders., MMR 2016, 8 (10). Die Datenqualität (dagegen) aus rechtsvergleichender Perspektive als eines der Kernprinzipien des Datenschutzrechts einstuftend Bygrave, Data Privacy Law, 2014, S. 163 f.

⁶ Siehe im Übrigen Hoeren, MMR 2016, 8 (8 f.).

⁷ Beispiel in Anlehnung an Chen, EDPL 2018, 36 (40).

⁸ Hierzu näher Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.), Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 139.

⁹ Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.), Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 139.

¹⁰ Herbst, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 60; Worms, in: BeckOK Datenschutzrecht, 30. Ed. (Stand: 1.11.2019), Art. 16 Rn. 49.

¹¹ Worms, in: BeckOK Datenschutzrecht, 30. Ed. (Stand: 1.11.2019), Art. 16 Rn. 61.

¹² Frenzel, in: Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 39.

¹³ Siehe auch Chen, EDPL 2018, 36 (39).

maschinenlesbar *abgebildet werden können*.¹⁴ Jede Form der Sprache, auch Programmiersprache, ist (auch sprachphilosophisch) niemals eindeutig, sondern stets mehrdeutig – und in diesem Sinne *per se* unpräzise.

Wir nehmen traditioneller Weise eine weitere *Unterscheidung*, eine weitere Zuschreibung, vor. Wir überziehen den rechtstatsächlichen Bezugspunkt mit einer weiteren Schicht. Mit dem Faktor Zeit. Anders formuliert: wir bestimmen, im tieferen Sinne willkürlich, ob und inwieweit der Faktor Zeit *relevant* sein soll, ob und inwieweit – im wahrsten Sinne des Wortes – ein Datum mit dem Datum verknüpft werden soll. Die Richtigkeit von Daten kann ein *moving target* sein. So können Daten „zeitlos“ richtig oder unrichtig sein (wie das Geburtsdatum einer Person). Daten können sich auf einen bestimmten Zeitpunkt beziehen (wie ein Aufenthaltsort einer Person zu einem bestimmten Zeitpunkt) oder Daten können einem dynamischen Referenzpunkt (wie die Adresse einer Person) unterworfen sein (und deswegen veraltet sein). *Richtig* kann deswegen immer nur mehrfach *kontextual* bestimmt werden.¹⁵

5

Richtigkeit kann freilich auch in einer anderen Weise verstanden werden. *Richtigkeit* könnte auch als *Zweckmäßigkeit* für die bestimmte Verarbeitung verstanden werden. *Richtig* wären nur Daten, die für die – zumindest datenschutzrechtlich stets zu definierenden – Zwecke der Verarbeitung *relevant* sind. In diesem Sinne stellt etwa § 31 BDSG für das Scoring darauf ab, dass die jeweiligen „Daten (...) nachweisbar für die Berechnung des (...) Verhaltens *erheblich* sind“ (Hervorh. d. Verf.).¹⁶ Legt man ein solches Verständnis zugrunde, gelten veränderte, teils auch gegensätzliche Parameter für die Beurteilung. Der Maßstab der Datenrichtigkeit rückt hier allerdings an den Grundsatz der Zweckbindung heran – und verliert auf diese Weise an Kontur und Unterscheidungskraft.

6

Hilfreich ist es insoweit, sich die englischsprachige Version der DS-GVO vor Augen zu führen. Diese spricht nicht etwa von *correctness*, sondern von *accuracy*. Darin spiegelt sich ein Relevanz-orientiertes Verständnis. Ein solches Verständnis ist bereits früh (etwa im Zuge der Diskussionen zu den OECD-Leitlinien 1980) unter Bezug auf das Vorverständnis in der Informatik zugrunde gelegt worden; es wurde verwiesen auf den „degree of accuracy or reliability“, also ein relatives Verständnis von Datenqualität, sowie das Eigeninteresse von Verarbeitern.¹⁷

Eine weitere Dimension der *Richtigkeit* eröffnet sich, wenn wir unterstellen, dass Daten Grundlage zur Erkennung von erkenntnisfördernden *Mustern* sind.¹⁸ Denn die Qualität

7

¹⁴ Siehe auch Chen, EDPL 2018, 36 (44).

¹⁵ Siehe auch Datenethikkommission, Gutachten der Datenethikkommission (Oktober 2019), https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=F9D0EDB93EB4995F6F48A9A89EB41665.1_cid373?__blob=publicationFile&v=6, S. 52 f.

¹⁶ Zum Kriterium der Nachweisbarkeit auch bereits Hoeren, MMR 2016, 8 (9 f.).

¹⁷ Hierzu Hoeren, ZD 2016, 459 (460 f.) m. w. N.

¹⁸ Grundlegend aus soziologischer Perspektive Nassehi, Muster, 2019.

entsprechender Muster hängt maßgeblich von der Qualität des Inputs ab. Es kommt also nicht allein auf die Richtigkeit von Daten im engeren Sinne und die Zweckmäßigkeit der verarbeiteten Daten an. Entscheidend wird in aller Regel auch die *Vollständigkeit* der Daten sein.¹⁹ Eine solche *Vollständigkeit* ist freilich ebenso ohne einen Zweckbezug nicht zu definieren.²⁰

III. Wozu Datenrichtigkeit?

Die Idee einer *Datenrichtigkeit* verfolgt Ziele auf unterschiedlichen Ebenen. Zunächst sind hiermit gesellschaftliche bzw. zivilgesellschaftliche Ziele angesprochen, die auch und gerade unter dem Begriff der *Datenethik* diskutiert werden. Aus diesem Blickwinkel sollte eine Verarbeitung von Daten, insbesondere als Grundlage für Entscheidungen, anhand der Parameter *Gerechtigkeit*, *Fairness* und *Transparenz* erfolgen. Der Datenrichtigkeit kommt hierfür eine befördernde Funktion zu. Verabsolutieren darf man diese Funktion allerdings nicht, sonst gerät man auf eine *slippery slope*. Denn konsequenter Weise müsste man immer mehr Daten sammeln, um unrichtige Daten nach und nach zu marginalisieren.²¹

8

Aus genuin staatlicher Perspektive wird mit der Datenrichtigkeit zunächst in Bezug auf öffentliche Aufgaben eine Präzision der eigenen Aufgabenerfüllung angestrebt. Die Eckpunkte der Bundesregierung für eine Datenstrategie sprechen darüber hinaus und allgemeiner von der „Bereitstellung hochwertiger Daten“²². Es besteht das Interesse an einem innovationsfreundlichen und gefährdungsadäquaten Rechtsrahmen für die Datenwirtschaft bzw. Daten-gestützte Geschäftsmodelle.²³ Die Datenethikkommission der Bundesregierung führt ergänzend in ihrem Gutachten zur Datenqualität aus:

9

„Ein verantwortungsvoller Umgang mit Daten in der Datengesellschaft setzt (...) im Interesse aller auch das Bemühen um eine dem Einsatzzweck angemessene Datenqualität voraus (...). Die Bestimmung dessen, was jeweils eine „angemessene“ Datenqualität bedeutet, muss jedoch stets kontextspezifisch erfolgen.“²⁴

Die Datenrichtigkeit beugt auch (so mag man unter dem Gesichtspunkt der Nachhaltigkeit argumentieren) einer zunehmenden *Data Pollution*²⁵ vor.

10

¹⁹ Schantz, in: BeckOK Datenschutzrecht, 30. Ed. (Stand: 1.2.2019), Art. 5 Rn. 29 stuft die Unvollständigkeit als Unterfall der Unrichtigkeit ein.

²⁰ Worms, in: BeckOK Datenschutzrecht, 30. Ed. (Stand: 1.11.2019), Art. 16 Rn. 58.

²¹ Siehe Chen, EDPL 2018, 36 (39); siehe auch ebd. (51): „[T]he appropriate degree of accuracy of personal data is a matter of ethics decided by the community as well as individuals, not simply a question of technical or economic feasibility.“

²² Bundesregierung, Eckpunkte einer Datenstrategie der Bundesregierung (18.11.2019), S. 3.

²³ Bundesregierung, Eckpunkte einer Datenstrategie der Bundesregierung (18.11.2019), S. 4.

²⁴ Datenethikkommission, Gutachten der Datenethikkommission (Oktober 2019), S. 83 (ohne Hervorhebungen).

²⁵ Siehe Ben-Shahar, Journal of Legal Analysis 2019, 104.

Datenschutzrechtlich angesprochen ist hiermit das Zusammenspiel von Datenrichtigkeit, Aktualisierungsgebot, Datenminimierung und Zweckbindung.²⁶ So sei nur beispielhaft darauf verwiesen, dass unrichtige Daten in aller Regel nicht erheblich bzw. nicht für die jeweiligen Zwecke erforderlich sind.²⁷

Datenrichtigkeit ist allerdings auch und gerade ein genuin ökonomisches Ziel – sei es auf dem Primärmarkt oder auf dem Sekundärmarkt für Daten.²⁸ Die Aggregation von Daten und das Erkennen von *richtigen* Mustern hat enormen ökonomischen Wert. *Richtige* Daten können – wie bei einer Navigationsdienstleistung – elementare Grundlage der Dienstleistung sein. Richtige Daten können der Optimierung des eigenen Angebots dienen. Richtige Daten unterstützen bei der Analyse und Bewertung von Innovationen. Richtige Daten können höhere Preise im Datenhandel²⁹ erzielen. Richtige Daten können zur Abschöpfung der Konsumentenrente genutzt werden, etwa durch die Personalisierung von Werbung bzw. von Preisen.³⁰

11

Schließlich stehen auch individuelle Ziele in Rede. Neben der Idee einer Vollständigkeit der Daten bzw. der Datenbasis steht dabei das Wissen um den Grad³¹ und die Grundlage informationeller Fremdbestimmung (*v. Lewinski*)³² im Fokus – trotz *privacy paradox* dürfte die geneigte betroffene Person bei omnipräsenten Verarbeitungen immer noch auf ein „wenigstens mit den richtigen Daten“ hoffen. Datenrichtigkeit stärkt – so die Grundannahme – das Vertrauen in und damit die Akzeptanz von Datenverarbeitungen und darauf basierenden Entscheidungen. Ein besonders starkes Interesse hieran besteht wohl überwiegend allerdings nur dann, wenn *belastende* Entscheidungen im Raume stehen. Das heißt natürlich in keiner Weise, dass Datenrichtigkeit immer gewünscht sein muss. Die Literatur verweist etwa auf teilweise höhere Preise für iPhone-Nutzer (da durchschnittlich wohl zahlungskräftiger)³³ sowie – sicherlich mit einem Schmunzeln – auf die korrekte Angabe des Beziehungsstatus oder des Alters in Dating-Apps³⁴. Die Frage, ob sich ein Nutzer bei einer unrichtigen Angabe vertragswidrig verhält, kann hier nicht vertieft werden. Hinweisen möchte ich zumindest auf eine SPIEGEL ONLINE-Meldung zu einem Niederländer, der gerichtlich die Änderung seines Geburtsdatums um 20 Jahre erreichen wollte, im Ergebnis allerdings erfolglos

12

²⁶ Siehe zu diesem Zusammenspiel auch Chen, EDPL 2018, 36 (47) sowie Kramer, in: Auernhammer DSGVO BDSG, 6. Aufl. 2018, Art. 5 DSGVO Rn. 32, der zu Recht auf Friktionen zwischen Aktualisierung und Datenminimierung hinweist.

²⁷ Spindler/Dalby, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, Art. 5 DS-GVO Rn. 13.

²⁸ Siehe hierzu etwa Schweitzer/Peitz, NJW 2018, 275.

²⁹ Hierzu etwa Specht, Konsequenzen der Ökonomisierung informeller Selbstbestimmung, 2012.

³⁰ Hierzu aus rechtlicher Sicht ausführlich Hennemann, AcP 219 (2019), 818.

³¹ Hierzu Chen, EDPL 2018, 36 (49).

³² v. Lewinski, Die Matrix des Datenschutzes, 2014, S. 40 ff.

³³ Siehe zur öffentlichen Diskussion etwa <https://www.computerbild.de/artikel/cb-News-Internet-Individualisierte-Preise-Online-Shop-22720415.html>.

³⁴ Beispiel von Chen, EDPL 2018, 36 (48).

blieb.³⁵ Der Kläger verwies SPIEGEL ONLINE zufolge unter anderem auf seine Chancen auf Tinder, aber auch bei einer Kreditvergabe.³⁶

Es ist an dieser Stelle kurz innezuhalten. Denn abgesehen von solchen Sonderfällen scheinen die meisten relevanten Akteure (Staat, private Verarbeiter und betroffene Personen) selten Interesse an der Verarbeitung unrichtiger Daten zu haben. Etwas, was von allen ganz überwiegend gewollt wird, wird regelmäßig allerdings auch ohne rechtliche Vorgaben eingehalten. Ist eine Regulierung der Datenrichtigkeit daher überhaupt erforderlich? Ökonomisch gesprochen ist die Frage aufgeworfen, ob ein besonderes Marktversagen droht, dem mit einer Regulierung vorgebeugt werden muss. Mit Blick auf das ureigene Interesse von Verarbeitern an Datenqualität³⁷ ist zumindest aus ökonomischer Perspektive ein rein marktbasierter Ansatz unter Rückgriff auf das allgemeine Zivilrecht nicht völlig fernliegend.³⁸ Aus technischer Perspektive mag mancher ergänzen: Algorithmen könnten im Einzelfall bereits ausreichend „trainiert“ sein, unrichtige Daten zu identifizieren und diese bei einer Auswertung außer Acht zu lassen; sollten wir gar darauf vertrauen, Algorithmen würden alsbald schon lernen, diese Unterscheidung vorzunehmen?³⁹

13

Einigkeit dürfte demgegenüber zumindest dahingehend bestehen, dass – im Datenschutzrecht – der betroffenen Person ausgewählte Betroffenenrechte für allfällige Korrekturen und Aktualisierungen (oder auch Löschungen) zustehen müssen, auch wenn unter Umständen auch Anreize auf Seiten der Verarbeiter bestehen, die eigenen Datenbestände jeweils *up-to-date* zu halten. Aus ökonomischer Perspektive ist damit auch ganz allgemein die Allokation von Risiken betreffend die Datenrichtigkeit angesprochen, die eine datenrechtliche Regulierung vornehmen muss. So ist zu fragen, ob und inwieweit für die Angabe oder die Verwendung von unrichtigen Daten gehaftet werden muss bzw. welche Sanktionen drohen.⁴⁰

14

IV. Der (Rechts-)Rahmen der Datenrichtigkeit

Die Datenrichtigkeit hat bislang vor allem genuin vertragsrechtliche Beachtung gefunden.⁴¹ Allgemein ist für die rechtliche Perspektive zentrale Weichenstellung, ob und inwieweit personenbezogene oder nicht-personenbezogene Daten in Rede stehen

15

³⁵ Rechtbank Gelderland, 3.12.2018, C/05/335902, ECLI:NL:RBGEL:2018:5102.

³⁶ Siehe <https://www.spiegel.de/panorama/emile-ratelband-niederlaender-will-sein-alter-per-klage-um-20-jahre-senken-a-1237344.html>.

³⁷ Hoeren, ZD 2016, 459 (459): „Datenqualität ist zunächst einmal etwas, das im Interesse der verarbeitenden Industrie liegt.“

³⁸ Siehe Hoeren, ZD 2016, 459 (460): „Der Markt und damit auch das allgemeine Zivilrecht sollten (...) über das Versagen der Unternehmen bei der Verwendung veralteter und unrichtiger Daten entscheiden.“

³⁹ Siehe Chen, EDPL 2018, 36 (39).

⁴⁰ Siehe auch Hoeren, ZD 2016, 459 (459), der zutreffend darauf verweist, dass eine Informationshaftung für Datenunrichtigkeit bisher nicht ausgeformt ist. Vgl. auch dens., MMR 2016, 8 (9).

⁴¹ Daten fungieren bereits bzw. werden spätestens nach Umsetzung der Digitale Inhalte-RL (EU) 2019/770 als „Gegenleistung“ im vertrags- bzw. schuldrechtlichen Sinne fungieren.

– unterliegen doch erstere mindestens auch dem strengen Datenschutzrecht. Für nicht-personenbezogene Daten steht ein umfassender unionaler (oder nationaler) Ordnungsrahmen noch aus. Insbesondere der DS-GVO vergleichbare Vorgaben zur Datenrichtigkeit bestehen nicht bzw. noch nicht. Der Austausch nicht-personenbezogener Daten erfolgt weitestgehend auf vertraglicher bzw. vertragsrechtlicher Basis – und unterliegt dem rechtspolitischen Grundsatz eines freien Datenflusses.⁴²

Für die Verarbeitung personenbezogener Daten benennt die DS-GVO unter anderem den Grundsatz der Richtigkeit, der ausgefüllt bzw. ergänzt wird durch verschiedene Regelungen – insbesondere durch das Betroffenenrecht auf Berichtigung. Art. 5 Abs. 1 lit. d DS-GVO führt aus: „Personenbezogene Daten müssen (...) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)^{43,44} Die Verwendung des Wortes „müssen“ wirkt freilich ein wenig apodiktisch. In der Sache soll der Verantwortliche durch diesen datenschutzrechtlichen Grundsatz auf eine Richtigkeit der Daten verpflichtet werden, womit ausweislich des Verweises „auf den neusten Stand“ auch eine jeweils aktuelle Richtigkeit gemeint sein soll. Der Passus „erforderlichenfalls“ stellt dabei eine Verbindung zum konkreten Verwendungskontext her.⁴⁵ Liest man den datenschutzrechtlichen Grundsatz der Richtigkeit unbefangen, scheint jedes unrichtige personenbezogene Datum für den Verantwortlichen ein veritables Problem zu sein. Weit verstanden führt die Verarbeitung eines unrichtigen Datums zu einem Verstoß gegen Art. 5 Abs. 1 lit. d DS-GVO – was in Ansehung der Bußgeldbewehrung des Art. 5 DS-GVO nach Art. 83 Abs. 5 DS-GVO (und auch unbeschadet des damit einhergehenden offenkundigen Bestimmtheitsproblems) einschneidende Konsequenzen nach sich zieht. Hat beispielsweise ein Kunde ein falsches Geburtsdatum angegeben, würde dies bereits die Gefahr eines Bußgeldes auslösen – der Verantwortliche könnte sich nur noch auf mangelnde Kenntnis bzw. mangelndes Verschulden berufen.

16

Zugrunde liegt einem solchen Zugriff freilich die Annahme, dass der Grundsatz der Richtigkeit einen „absoluten“ Richtigkeitsbegriff verwendet, der pauschal auf die Unrichtigkeit personenbezogener Daten abstellt. Von einem solchen Verständnis der

17

⁴² EU-Kommission, Mitteilung „Aufbau einer europäischen Datenwirtschaft“, COM(2017) 9 final. Siehe zu Märkten für nicht-personenbezogenen Daten etwa Fries/Scheufen, MMR 2019, 721. Kleinere Vorgaben für nicht-personenbezogenen Daten bestehen seit 2018 teilweise betreffend die Datenlokalisierung und den Datenhandel (Verordnung (EU) 2018/1807). Auf die Richtigkeit oder die Qualität von nichtpersonenbezogenen Daten geht die Verordnung nicht explizit ein, scheint diese allerdings vorauszusetzen. Ebenso geht die EU-Kommission (diese Fn.) nicht explizit auf die Datenrichtigkeit oder -qualität ein.

⁴³ Vgl. auch § 47 Nr. 4 BDSG für den Bereich der Verarbeitung im Bereich Justiz und Inneres.

⁴⁴ Siehe auch bereits EuGH, EuZW 2009, 183 (185) – Huber sowie EuGH, Urt. v. 13.5.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – Google Spain.

⁴⁵ Frenzel, in: Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 40; Heberlein, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 24.

Richtigkeit scheint zumindest die überwiegende datenschutzrechtliche Literatur auszugehen.⁴⁶ Hoeren hat bereits 2016 ein alternatives Verständnis vorgestellt und dafür auch und gerade auf den der englischen Sprachfassung zugrundeliegenden Begriff der *accuracy* verwiesen. Der Grundsatz der Datenrichtigkeit beziehe sich nicht auf die Richtigkeit im jeweiligen Einzelfall. Dies sei nur die Perspektive der einzelnen Betroffenenrechte. Für den (bußgeldbewehrten) Grundsatz der Datenrichtigkeit solle der „technologisch-relational[e] Begriff der „accuracy““ zugrunde gelegt werden.⁴⁷ Die identischen Begriffe seien unterschiedlich auszulegen.⁴⁸ Art. 5 Abs. 1 lit. d DS-GVO bezieht sich dann vor allem auf die Sicherstellung der *jeweils angemessenen* Datenqualität.⁴⁹ Erwägungsgrund 39 DS-GVO kann mit gutem Willen (vielleicht auch *nur* mit gutem Willen) in einem solchen Sinne verstanden werden, wenn dort dem Verantwortlichen „alle *vertretbaren Schritte*“ auferlegt werden.⁵⁰

Zentrales Betroffenenrecht, um eine möglichst *akkurate* Verarbeitung zu erreichen, ist das Recht auf Berichtigung nach Art. 16 DS-GVO.⁵¹ Die Norm statuiert zweierlei. Zum einen hat „[d]ie betroffene Person (...) das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen“ (Art. 16 Satz 1 DS-GVO). Zusätzlich ist vorgesehen, dass die betroffene Person „[u]nter Berücksichtigung der Zwecke der Verarbeitung (...) das Recht [hat], die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen“ (Art. 16 Satz 2 DS-GVO).⁵² Ergänzend tritt das Recht auf Löschung nach Art. 17 DS-GVO hinzu, wodurch ebenso gewährleistet wird, dass bestimmte unrichtige Daten nicht mehr für eine Datenverarbeitung herangezogen werden können. Allgemein hat der Verantwortliche im Übrigen Daten nicht nur auf Antrag zu berichtigen oder zu löschen. Vielmehr besteht eine damit korrespondierende, laufende und antragsunabhängige Pflicht, als unrichtig identifizierte Daten zu berichtigen oder unter Umständen zu löschen.⁵³ Zudem sei noch darauf verwiesen, dass nach Art. 18 Abs. 1 lit. a DS-GVO die betroffene Person die Einschränkung der Verarbeitung verlangen kann, falls die Richtigkeit der personenbezogenen Daten von ihr bestritten wird⁵⁴ – und zwar, um dem Verantwortlichen eine Überprüfung der Richtigkeit zu ermöglichen. Wurden Daten anderen Empfängern offengelegt, ist diesen Berichtigung oder Einschränkung der Verarbeitung grundsätzlich mitzuteilen. Für eine

18

⁴⁶ Siehe Herbst, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, 2. Aufl. 2018, Art. 16 DS-GVO Rn. 8 sowie Art. 5 DS-GVO Rn. 60 und 62: „Die Richtigkeit muss im Hinblick auf die Zwecke der Verarbeitung gegeben sein.“; Spindler/Dalby, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, Art. 5 DS-GVO Rn. 13; Wolff, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 441 ff.

⁴⁷ Hoeren, ZD 2016, 459 (462).

⁴⁸ Hoeren, ZD 2016, 459 (462).

⁴⁹ Siehe im Übrigen zu technisch-organisatorischen Maßnahmen auch Art. 24 f. DS-GVO.

⁵⁰ Hervorh. d. Verf.

⁵¹ Es bestehen freilich verschiedene Einschränkungen, siehe etwa § 28 Abs. 3 BDSG und § 23 Abs. 1 Nr. 2 BDSG sowie § 57 Abs. 2 Satz 3 RStV und (für den Bereich Justiz und Inneres) §§ 74 Abs. 1, 75 Abs. 1 BDSG.

⁵² Siehe auch Erwägungsgrund 59 und 65 DS-GVO.

⁵³ Siehe Worms, in: BeckOK Datenschutzrecht, 30. Ed. (Stand: 1.11.2019), Art. 16 Rn. 6 f.; betreffend Art. 17 DS-GVO siehe Hennemann, PinG 2016, 176 (177).

⁵⁴ Zum Tatbestandsmerkmal des Bestreitens siehe VG Stade, NVwZ 2019, 251.

automatisierte Entscheidungsfindung bzw. das Profiling verweist Erwägungsgrund 71 DS-GVO ebenfalls darauf, dass „technische und organisatorische Maßnahmen [getroffen werden] (...), mit denen in geeigneter Weise (...) sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden“.⁵⁵

V. Vom Wollen und Sollen der Datenrichtigkeit

Eine grundlegende Frage beantworten die datenschutzrechtlichen Regeln nicht: Ob und inwieweit wir Datenrichtigkeit eigentlich „wollen sollen“...?⁵⁶ Anders gefragt: Welchen Grad der Datenrichtigkeit streben wir jeweils an? Noch anders gefragt: Besteht je nach Kontext ein Anspruch auf einen bestimmten Grad von Datenrichtigkeit?⁵⁷ Hier ist freilich zu unterscheiden. In vielfältigen Konstellationen, etwa bei der Erhebung von Geo- oder Wetterdaten, streben wir nachvollziehbarer Weise eine umfassende *accuracy* an. Schon bei der Erhebung allerdings von Standortdaten eines Nutzers im Zuge einer Navigations-App springt ins Auge, dass mit höchster Präzision allfällige Vor- und Nachteile einhergehen. Mit dem Grad der Datenrichtigkeit sind zudem Konstellationen angesprochen, in denen aus rechtlichen Gründen explizit keine umfassende (Daten-)Richtigkeit zugrunde gelegt werden darf (etwa bei Versicherungsverträgen, bei denen unter Umständen das Geschlecht kein zulässiges Differenzierungskriterium ist⁵⁸) oder in Situationen, in denen sogar ein „Recht auf Lüge“ besteht (etwa arbeitsrechtlich in Bezug auf die Nichtangabe einer Schwangerschaft im Bewerbungsgespräch)^{59, 60}

19

Darüber hinaus wurde in jüngerer Zeit hervorgehoben, dass eine umfassende „Korrektheit“, insbesondere personenbezogener Daten, zu einem „Verlust des [individuellen] Manövrierraums“ für den Prozess der Selbstkonstruktion führe.⁶¹ Eine sehr hohe Präzision von personenbezogenen Daten eröffnet zudem den Raum für eine perfekte, vielleicht zu perfekte, Diskriminierung⁶² – auch wenn damit zunächst nur eine *Unterscheidung* zwischen verschiedenen Individuen angesprochen ist, an dieser Stelle

20

⁵⁵ Siehe hierzu auch Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP251rev.01, S. 12 f.

⁵⁶ Zu den Gefahren der *accuracy* siehe allgemein Chen, EDPL 2018, 36.

⁵⁷ Siehe hierzu ausführlich Chen, EDPL 2018, 36, insbesondere ebd. (49 ff.): „The restriction on the accuracy of personal data is an essential component of informational self-determination, but it is not properly translated into EU data protection principles.“

⁵⁸ EuGH, Urt. v. 1.3.2011, C-236/09 – *Association belge des Consommateurs Test-Achats ASBL u. a./ Conseil des ministres*.

⁵⁹ Siehe hierzu allgemein(er) Armbrüster, in: Münchener Kommentar BGB, Bd. 1, 8. Aufl. 2018, § 123 Rn. 46 ff.

⁶⁰ Hierzu näher Chen, EDPL 2018, 36 (50 ff.).

⁶¹ Chen, EDPL 2018, 36 (42 f.) [Übersetzung des Verf.]; siehe ebd. (43): „[E]fforts in improving correctness and precision could end up depriving individuals of their limited space in which they manoeuvre forward in the course of self-construction. (...) „[T]he higher accuracy of personal data could actually mean a lower level of autonomy.“

⁶² Chen, EDPL 2018, 36 (40 f.).

sei insofern wiederum nur auf die umfassenden Diskussionen zur personalisierten Preisbildung bzw. zur Preisdiskriminierung verwiesen.⁶³

Konzeptionell noch weitergehender ist natürlich der Ansatz in anderem Zusammenhang, bewusst unrichtige Daten „beizumischen“ (etwa zugunsten des Datenschutzes im Zuge von Anonymisierungstechniken⁶⁴) – ein gewisser Grad der Unrichtigkeit ist hier positiv gewollt.

21

⁶³ Siehe ausführlich Hennemann, AcP 219 (2019), 818.

⁶⁴ Siehe hierzu Art. 29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP216 sowie Chen, EDPL 2018, 36 (46) m. w. N.