Die europäische Datenschutz-Grundverordnung – Der Anbruch einer neuen Ära

Constantin Herfurth / Stephan Schindler / Bernd Wagner, Kassel*

Nach ca. vier Jahren intensiver Diskussion wurde auf europäischer Ebene die Datenschutz-Grundverordnung verabschiedet, mit der die bislang geltende Datenschutzrichtlinie abgelöst wird. Durch sie wird das Datenschutzrecht innerhalb Europas weitestgehend vereinheitlicht. Datenverarbeitende Akteure stellt das vor das Problem, dass sie ihre Prozesse bis zum 25. Mai 2018 an das neue Recht anzupassen haben. Ab diesem Stichtag gilt die Datenschutz-Grundverordnung in all ihren Teilen verbindlich und unmittelbar in jedem Mitgliedsstaat der Europäischen Union. Der vorliegende Beitrag gibt einen Überblick über die wichtigsten Regelungen der Datenschutz-Grundverordnung.

A. Die europäische Datenschutzreform

Kern des Datenschutzes ist „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.[1] Der Einzelne soll die Verarbeitung ihn betreffender Daten kontrollieren können, um seine Privatsphäre und seine Persönlichkeitsrechte zu schützen.[2] Die Datenschutz-Grundverordnung[3] (im Folgenden DSGVO[4]) führt zu diesem Zweck einen europaweit weitestgehend vereinheitlichten Schutzstandard ein. Sie ist das Ergebnis eines Gesetzgebungsverfahrens, das im Jahr 2012 durch einen Vorschlag der EU-Kommission[5] eingeleitet wurde und durch die Arbeit des deutschen Berichterstatters des Europäischen Parlaments Jan Philipp Albrecht sowie massiven Lobbyismus geprägt war.[6] Am 24. Mai 2016 in Kraft getreten gilt sie nach einer zweijährigen Übergangszeit ab dem 25. Mai 2018.[7]

Die DSGVO ersetzt die aus den 1990er Jahren stammende Datenschutzrichtlinie 95/46/EG (im Folgenden DSRL),[8] auf deren Umsetzung bisher weite Teile des deutschen Datenschutzrechts, darunter auch das Bundesdatenschutzgesetz (BDSG), beruhen.[9] Als zentraler Bestandteil der europäischen Datenschutzreform verfolgt die DSGVO das Ziel, das europäische Datenschutzrecht an die Herausforderungen des 21. Jahrhunderts anzupassen.[10] Neue technische Entwicklungen, wie z.B. künstliche Intelligenz oder Big Data-Analysen, und die Zunahme datengetriebener Geschäftsmodelle erfordern ein modernes Datenschutzrecht, um den grundrechtlich verbürgten Schutz (vgl. Art. 8 GRCh, Art. 16 AEUV) personenbezogener Daten effektiv durchzusetzen. Ein unionsweit einheitlicher Datenschutzstandard soll die Grundrechte und Grundfreiheiten betroffener Personen bei der Verarbeitung personenbezogener Daten schützen und gleichzeitig den (digitalen) Binnenmarkt stärken.[11] Ergänzt wird die DSGVO durch eine Polizei-Richtlinie (im Folgenden JI-RL)[12] für die Datenverarbeitung zum Zweck der Verhütung und Verfolgung von Straftaten durch die zuständigen Behörden, die bis zum 06. Mai 2018 in innerstaatliches Recht umzusetzen ist.[13]

Die DSGVO bricht nicht mit den Prinzipien der alten DSRL, sondern lehnt sich vielfach an diese an. So fanden sich z.B. die Datenschutzgrundsätze (Art. 5) sowie die Erlaubnistatbestände (Art. 6 Abs. 1) schon weitgehend in der DSRL. Neu ist das Marktortprinzip (Art. 3 Abs. 2), welches in Fortführung des Google-Urteils des EuGH[14]

* Die Autoren sind wissenschaftliche Mitarbeiter an der Universität Kassel und dort sowohl am Fachgebiet für Öffentliches Recht, IT-Recht und Umweltrecht von Prof. Dr. Gerrit Hornung, LL.M. als auch am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) tätig.

1 Prägnant zur Volkszählung in Deutschland BVerfGE 65, 1 (43).

2 *Gola*, in: Gola (Hrsg.), DSGVO, 2017, Einl. Rn. 1 ff.

3 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119, 1.

4 Artikelangaben ohne Bezeichnung beziehen sich auf die DSGVO.

5 Vorschlag der *Kommission* für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11 endg.

6 Zum Gesetzgebungsverfahren z.B. *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, S. 40 ff.

7 Art. 99.

8 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31.

9 Zum Einfluss auf das BDSG *Simitis*, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, Einl. Rn. 89 ff.

10 S. die Mitteilung der *Kommission* zum Schutz der Privatsphäre in einer vernetzten Welt, KOM (2012) 9 endg.

11 Vgl. Art. 1; ausführlich zu den Zielen *Albrecht/Jotzo*, (Fn. 6), S. 37 ff.

12 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. 2016 L 119, 89.

13 Art. 63 JI-RL.

14 EuGH, 13.05.2014, Rs. C-131/12 – Google Spain.

den räumlichen Anwendungsbereich der DSGVO von der Niederlassung des Verantwortlichen[15] emanzipiert. Die Betroffenenrechte wurden u.a. um ein „Recht auf Vergessenwerden" (Art. 17)[16] und ein Recht auf Datenübertragbarkeit (Art. 20) ergänzt. Es finden sich neue Regelungen zum Datenschutz durch Technikgestaltung (Art. 25) und zur Datenschutz-Folgenabschätzung (Art. 35). Als wichtige Änderung im Sinne eines effektiven Datenschutzes gelten die Regelungen zu den Aufsichtsbehörden und deren europaweiter Zusammenarbeit (Art. 51 ff.).[17] Schließlich wurden die Bußgelder nach Art. 83 auf bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes drastisch erhöht. Aufgrund des technologieneutralen Ansatzes (EwG 15) wurde auf die Regelung spezifischer technischer Verfahren, z.B. Videoüberwachung, verzichtet.

Regelungstechnisch bringt der Wandel von der Richtlinie zur Verordnung mit sich, dass die Vorgaben der DSGVO unmittelbar geltendes Recht werden.[18] Entgegenstehendes nationalstaatliches Recht wird aufgrund des Anwendungsvorranges des EU-Rechts verdrängt.[19] Allerdings sieht die DSGVO in Gestalt sog. Öffnungsklauseln einen Gestaltungsspielraum der Mitgliedsstaaten vor.[20] Dies betrifft z.B. die Datenverarbeitung für den öffentlichen Bereich (Art. 6 Abs. 2) oder den Beschäftigtendatenschutz (Art. 88). Diese Spielräume können die Mitgliedsstaaten mit nationalstaatlichen Regelungen ausfüllen, weshalb die DSGVO zum Teil als „atypischer Hybrid"[21] aus Verordnung und Richtlinie bezeichnet wird. Allerdings ist eine derartige Vorgehensweise europarechtlich weder unzulässig noch ungewöhnlich.[22] In Deutschland wurde zur Ausfüllung der Öffnungsklauseln der DSGVO (sowie zur Umsetzung der JI-RL) das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU[23] verabschiedet, das v.a. eine Neufassung des Bundesdatenschutzgesetzes (BDSG 2018) beinhaltet. Daneben ist eine Überarbeitung der verschiedenen Landesdatenschutzgesetze in Arbeit.

Die DSGVO wird unterschiedlich bewertet; zum Teil wird sie als „Meilenstein" und „Gold-Standard"[24] gefeiert, zum Teil als „größte Katastrophe des 21. Jahrhunderts"[25] verdammt. Kritisiert wird ihre Anlehnung an die DSRL, d.h. ein „Verharren auf überholten Regelungen", sowie ihre „Unterkomplexität", die „die Breite, Tiefe und Komplexität der Aufgabe" verkenne und künftige Herausforderungen unter dem Vorwand der Technikneutralität nicht ausreichend spezifisch adressiere.[26] Durch die zahlreichen Öffnungsklauseln drohe trotz aller Harmonisierungsbestrebungen ein „Datenschutz-Flickenteppich"[27] zu entstehen.

Ob sich die DSGVO insofern in der Zukunft bewährt, hängt maßgeblich davon ab, wie die im Folgenden vorgestellten Regelungen in der Rechtspraxis ausgelegt und umgesetzt werden.

B. Anwendungsbereich der DSGVO

Die DSGVO gilt nur in den Fällen, in denen sie sachlich (Art. 2) und räumlich (Art. 3) anwendbar ist.

I. Sachlicher Anwendungsbereich

Die DSGVO gilt gem. Art. 2 Abs. 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem (Art. 4 Nr. 6) gespeichert sind oder gespeichert werden sollen.[28] Die Absätze 2 und 3 enthalten demgegenüber Ausnahmen, etwa bei der Datenverarbeitung zu ausschließlich persönlich familiärer Tätigkeit.

Während unter Verarbeitung (Art. 4 Nr. 2) im Ergebnis jeder Umgang mit personenbezogenen Daten zu verstehen ist,[29] werden mit personenbezogenen Daten nach Art. 4 Nr. 1 alle Informationen bezeichnet, die sich auf eine identifizierte oder identifizierbare natürliche Person (sog. „betroffene Person") beziehen. Der Begriff der Information ist weit zu verstehen und kann Angaben jeglicher Art, z.B. zu Aussehen, Meinungen etc., umfassen. Es existiert „kein belangloses Datum",[30] da abhängig vom Verwendungszusammenhang jeglicher Information datenschutzrechtliche Relevanz zukommen kann. Allerdings muss die Information Bezug zu einer identifizierten, jedenfalls aber identifizierbaren natürlichen Person aufweisen.[31] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollen nach EwG 26 „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden". Nach Ansicht des EuGH werden dabei alle rechtlich zulässigen Mittel erfasst, die von dem Verantwortlichen – auch unter Zuhilfenahme Dritter, z.B. im Rahmen von

15 Zum Begriff des Verantwortlichen unter E.

16 Welches aber mehr verspricht als es hält, s. *Kühling/Martini*, EuZW 2016, 448 (450): „Scheinriese".

17 *Albrecht/Jotzo*, (Fn. 6), S. 113.

18 Vgl. Art. 288 Abs. 2 AEUV.

19 Grundlegend zum Vorrang des Europarechts EuGH, 15.07.1964, Rs. 6/64 – Costa/ENEL.

20 Überblick zu den verschiedenen Öffnungsklauseln z.B. *Gola*, (Fn. 2), Einl. Rn. 45 ff.

21 *Kühling/Martini*, (Fn. 16), 449.

22 *Albrecht/Jotzo*, (Fn. 6), S. 133 f.

23 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017, BGBl. 2017 I, 2097.

24 *Albrecht*, CR 2016, 88 (97 u. 98).

25 *Hoeren*, nach heise-online, http://heise.de/-3190299, Abruf v. 13.03.2018.

26 *Roßnagel*, DuD 2016, 561 (564 f.).

27 *Gola*, (Fn. 2), Einl. Rn. 45.

28 Daher dürften z.B. unstrukturiert aufbewahrte Akten aus dem sachlichen Anwendungsbereich fallen; vgl. EwG 15.

29 *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO, 2017, Art. 4 Nr. 2 Rn. 4.

30 So bereits BVerfGE 65, 1 (45); ähnlich EuGH, 20.12.2017, Rs.C-434/16 – Nowak, Rn. 34.

31 Dazu *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DSGVO, 2017, Art. 4 Nr. 1 Rn. 17 ff.

Auskunftsansprüchen – vernünftigerweise eingesetzt werden können.[32]

II. Räumlicher Anwendungsbereich

In räumlicher Hinsicht ist die DSGVO nach Art. 3 Abs. 1 anwendbar, soweit die Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters[33] in der EU erfolgt. Nach dem neuen Marktortprinzip (Art. 3 Abs. 2) gilt sie überdies bei Fehlen einer Niederlassung in der EU, wenn die Datenverarbeitung im Zusammenhang damit steht, dass Personen, die sich in der EU befinden, Waren oder Dienstleistungen angeboten werden (lit. a) oder ihr Verhalten beobachtet wird (lit. b). Verarbeitet dementsprechend ein in den USA ansässiger Onlinehändler die Daten europäischer Kunden, ist die DSGVO auch für den Fall anwendbar, dass er keine Niederlassung in der EU hat.

C. Grundsätze der Datenverarbeitung

Art. 5 normiert die allgemeinen Datenschutzgrundsätze. Diese haben einen Doppelcharakter – sie sind Programmsätze und verbindliche Regelungen zugleich.[34] An vielen Stellen der DSGVO werden sie wieder aufgegriffen und durch detaillierte Regelungen konkretisiert.

I. Rechtmäßigkeit der Datenverarbeitung

Art. 5 Abs. 1 lit. a fordert eine rechtmäßige Datenverarbeitung, d.h. eine Einwilligung der betroffenen Person oder eine sonstige Rechtsgrundlage. Andernfalls ist sie verboten (sog. Verbotsprinzip). Rechtsgrundlagen können der DSGVO oder, wenn sich die DSGVO darauf bezieht, dem sonstigen Unionsrecht oder dem Recht der Mitgliedsstaaten entnommen werden.[35]
Art. 6 Abs. 1 ist die zentrale Vorschrift zur Rechtmäßigkeit der Datenverarbeitung. Für besondere Kategorien personenbezogener Daten, d.h. besonders sensible Daten, wie z.B. Angaben zur Sexualität oder Gesundheitsdaten, gelten die Anforderungen des Art. 9. Die in der Praxis wichtigsten Erlaubnistatbestände des Art. 6 Abs. 1, die Einwilligung (lit. a) und die Interessenabwägung (lit. f), sollen im Folgenden kurz erläutert werden.

1. Einwilligung

Die Einwilligung ist primärrechtlich in Art. 8 Abs. 2 GRCh verankert und Ausdruck der Privatautonomie des Einzelnen. Ihre Voraussetzungen sind in den Art. 4 Nr. 11 und Art. 7 geregelt. Spezielle Vorgaben finden sich für Kinder in Art. 8 und für sensible Daten in Art. 9 Abs. 2 lit. a. Eine wirksam erteilte Einwilligung kann nach Art. 7 Abs. 3 „jederzeit" mit ex nunc-Wirkung widerrufen werden.
In formaler Hinsicht bedarf es – anders als nach dem bisherigen deutschen Recht – keiner besonderen Form. Jedoch ist aufgrund der Beweislast des Verantwortlichen gem. Art. 7 Abs. 1 DSGVO eine textliche Manifestation sinnvoll.[36] Überdies muss die Einwilligung „unmissverständlich" abgegeben werden. Dies ist auch konkludent – z.B. durch Kopfnicken – möglich,[37] nicht aber durch Untätigkeit oder Stillschweigen.[38] Bei einer Einwilligung durch eine schriftliche Erklärung,[39] die noch weitere Sachverhalte betrifft, ist die Einwilligung so zu gestalten, dass sie von den anderen Sachverhalten klar unterschieden werden kann (Art. 7 Abs. 2). Diese Hervorhebung soll verhindern, dass der Einwilligende – z.B. durch Kleingedrucktes in den AGB – überrumpelt wird.[40]
Inhaltlich muss die Einwilligung freiwillig und in informierter Weise für einen bestimmten Fall erteilt werden. Freiwilligkeit setzt voraus, dass die betroffene Person eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.[41] Problematisch sind Fälle, in denen zwischen der betroffenen Person und dem Verantwortlichen „ein klares Ungleichgewicht"[42] vorliegt, was z.B. im Rahmen eines Arbeitsverhältnisses oder auch bei einer Monopolstellung des Anbieters eines sozialen Netzwerkes der Fall sein kann. Das sog. Koppelungsverbot sieht insofern in Art. 7 Abs. 4 vor, dass bei der Beurteilung der Freiwilligkeit in Rechnung zu stellen ist, ob eine Vertragserfüllung von der Einwilligung in dafür nicht erforderliche Datenverarbeitungsvorgänge abhängig gemacht wird. Ist das der Fall, führt dies zwar nicht zwingend zur Unfreiwilligkeit der Einwilligung, die Koppelung ist jedoch als gewichtiges Kriterium in die umfassende Beurteilung der Freiwilligkeit miteinzustellen.[43]
Eine Einwilligung genügt den Bestimmtheitsanforderungen, wenn erkennbar ist „unter welchen Bedingungen sich die Betroffenen mit der Verarbeitung welcher Daten einverstanden erklärt haben".[44] Hierzu muss der Betroffene

---

32 EuGH, 19.10.2016, Rs. C-582/14 – Breyer, Rn. 46 ff.

33 Mit Auftragsverarbeiter wird nach Art. 4 Nr. 8 eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle bezeichnet, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

34 *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO, 2017, Art. 5 Rn. 1.

35 EwG 40.

36 *Buchner/Kühling*, DuD 2017, 544 (546).

37 *Krohm*, ZD 2016, 368 (371).

38 EwG 32.

39 Mit Schriftform ist dabei keine deutsche Schriftform (§§ 126, 126a BGB) gemeint, sondern eine „europäische", die deutlich weiter ist und i.Erg. allein die mündliche Form ausschließen dürfte; s. hierzu ausführlich *Isik*, Die Schriftform im EU-Recht, 2013, S. 201 ff.

40 Vgl. *Liedke*, Die Einwilligung im Datenschutzrecht, 2012, S. 24.

41 EwG 42.

42 EwG 43.

43 So beispielweise auch *Ernst*, ZD 2017, 110 (112).

44 Bereits m.w.N. zum BDSG *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 4a Rn. 77.

„übersehen können, auf welche Daten sich seine Einwilligung erstreckt".[45] Dies deckt sich insofern mit der Informiertheit der betroffenen Person.

2. Interessenabwägung

Art. 6 Abs. 1 lit. f. erlaubt die Datenverarbeitung, die zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Es handelt sich um eine Generalklausel, die flexibel auf eine Vielzahl von Fällen anwendbar ist, aufgrund ihrer Unbestimmtheit und dehnbaren Kriterien aber zu Rechtsunsicherheit führen kann.[46]
Zunächst muss ein berechtigtes Interesse, d.h. ein Interesse rechtlicher, wirtschaftlicher oder ideeller Art, das im Einklang mit dem Unionsrecht sowie dem Recht des jeweiligen Mitgliedsstaats steht, vorliegen.[47] Des Weiteren muss die Datenverarbeitung zur Wahrung der berechtigten Interessen erforderlich sein. Das ist der Fall, wenn sie zur Wahrung berechtigter Interessen geeignet ist und keine mildere – also datenschutzschonendere – Alternative besteht, die dem Verantwortlichen zumutbar ist.[48]
Schließlich dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person die berechtigten Interessen des Verantwortlichen oder Dritter nicht überwiegen.[49] Die konkret widerstreitenden Positionen sind zu gewichten und gegeneinander abzuwägen, wobei die Bedeutung der berechtigten Interessen zuvorderst davon abhängt, ob sie auf Grundrechte (z.B. Meinungs-, Presse- oder Berufsfreiheit) gestützt werden können. Das Gewicht der entgegenstehenden Interessen der betroffenen Person ergibt sich u.a. auch aus ihrer grundrechtlichen Anerkennung, v.a. durch Art. 7 und 8 GRCh. In Rechnung zu stellen ist dabei die drohende Belastung. Zu berücksichtigen ist z.B. die Art und Menge der Daten, die Art der Verarbeitung oder die Dauer der Speicherung.[50]

II. Weitere Grundsätze

Art. 5 Abs. 1 lit. a normiert den Transparenzgrundsatz, wonach die Datenverarbeitung für die betroffene Person nachvollziehbar sein muss. Dies ist von zentraler Bedeutung, da zahlreiche Betroffenenrechte (Art. 12 ff.) nur bei Kenntnis der Verarbeitung wahrgenommen werden können (Transparenzdreiklang: See – Check – Act).
Gem. Art. 5 Abs. 1 lit. b müssen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Zweckbindung). Eine spätere Veränderung des Verarbeitungszwecks ist nur unter engen Voraussetzungen zulässig (vgl. Art. 6 Abs. 4). Der Grundsatz der Zweckbindung soll Daten- und Informationsströme eingrenzen.[51] Die Eingrenzung erfolgt im Verbund mit den Grundsätzen der Datenminimierung und der Speicherbegrenzung.[52] So müssen nach Art. 5 Abs. 1 lit. c personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung). Dies wird in zeitlicher Hinsicht durch den Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e ergänzt. Danach müssen Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Im Anschluss sind die Daten zu löschen oder zu anonymisieren.
Gem. Art. 5 Abs. 1 lit. d müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein (Richtigkeit), um die Realität zutreffend abzubilden und zu verhindern, dass der Betroffene durch die Verwendung fehlerhafter Daten Nachteile erleidet.[53]
Art. 5 Abs. 1 lit. f fordert die Gewährleistung angemessener Datensicherheit durch geeignete technische und organisatorische Maßnahmen, so dass die personenbezogenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung sowie Verlust und Zerstörung geschützt sind (Integrität und Vertraulichkeit).
Für die Einhaltung dieser Grundsätze ist gem. Art. 5 Abs. 2 der Verantwortliche verantwortlich. Er muss deren Einhaltung nachweisen können (Rechenschaftspflicht). Derjenige, der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, soll auch für das Pflichtenprogramm zum Schutz der betroffenen Person zuständig sein. Die DSGVO stellt hierfür u.a. in den Art. 24 ff. verschiedene Instrumente bereit.

D. Betroffenenrechte

Mit der Datenschutzreform sollen die individuellen Rechte der betroffenen Personen gestärkt werden.[54] Diese sind – nicht abschließend – in den Art. 12 bis 23 geregelt.
Die Rechte in den Art. 12 bis 15 können als Konkretisierung des Transparenzgebotes (Art. 5 Abs. 1 lit. a) verstanden werden. Gem. Art. 12 ist der Verantwortliche gegenüber betroffenen Personen zu einer transparenten Bereitstellung von Informationen und zur Erleichterung der Rechtsausübung verpflichtet. Die Art. 13 und 14 verlangen von dem Verantwortlichen die aktive Mitteilung bestimmter Informationen (z.B. Kontaktdaten, Verarbeitungszweck). Dies gilt allerdings nicht, wenn die betroffene Person z.B.

45 So bereits zum BDSG BGH, NJW 2003, 1237 (1241).
46 *Buchner*, DuD 2016, 155 (159).
47 *Schulz*, in: Gola (Hrsg.), DSGVO, 2017, Art. 6 Rn. 51.
48 S. z.B. *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DSGVO, 2017, Art. 6 Rn. 45.
49 Zur Abwägung *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 649 ff.
50 Vgl. Art. 29-Datenschutzgruppe (Hrsg.), WP 217, 2014, S. 47 ff.
51 *Frenzel*, (Fn. 34), Art. 5 Rn. 23.
52 Vgl. Art. 29-Datenschutzgruppe (Hrsg.), WP 203, 2013, S. 4.
53 *Frenzel*, (Fn. 34), Art. 5 Rn. 39.
54 *Albrecht/Jotzo*, (Fn. 6), S. 83.

bereits über diese Informationen verfügt.[55] Zudem kommt betroffenen Personen gem. Art. 15 ein Auskunftsanspruch gegen den Verantwortlichen zu, der sich auf die wesentlichen Umstände der Datenverarbeitung bezieht. Der Auskunftsanspruch ist eine wichtige Voraussetzung für die Geltendmachung weiterer Ansprüche, da er es betroffenen Personen ermöglicht, „sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können."[56] Seine Bedeutung wird durch die explizite Erwähnung in Art. 8 Abs. 2 S. 2 GRCh unterstrichen.

Im Zusammenhang mit dem Grundsatz der Datenrichtigkeit steht das in Art. 16 verankerte Recht auf Berichtigung unrichtiger Daten (z.B. Angaben zu Namen oder Geburtsdatum), das auch ein Recht auf Vervollständigung unvollständiger Daten beinhaltet.

Art. 17 Abs. 1 („Recht auf Vergessenwerden") enthält einen Löschungsanspruch des Betroffenen bei Vorliegen der dort genannten Gründe (z.B. bei unrechtmäßiger Verarbeitung oder Widerruf der Einwilligung). Zusätzlich normiert Art. 17 Abs. 1 eine unabhängig von der Geltendmachung des Löschungsanspruchs bestehende Löschpflicht des Verantwortlichen. Hat der Verantwortliche Daten öffentlich gemacht, so hat er gem. Art. 17 Abs. 2 angemessene Maßnahmen zu ergreifen, um andere für die Datenverarbeitung Verantwortliche darüber zu informieren, dass eine betroffene Person von ihnen die Löschung von Kopien bzw. aller Links zu diesen personenbezogenen Daten verlangt hat. Hierdurch soll dem „Recht auf Vergessenwerden" v.a. im Internet Geltung verschafft werden.[57] Dies betrifft z.B. Webseiten- und Suchmaschinenbetreiber, die im Falle eines Löschverlangens Dritte, die die Daten ebenfalls verarbeiten, über das Verlangen informieren müssen, soweit dies möglich und zumutbar ist.

Das in Art. 21 geregelte Widerspruchsrecht erlaubt es betroffenen Personen bei Verarbeitungssituationen nach Art. 6 Abs. 1 lit. e oder f (Abs. 1) sowie in Werbesituationen (Abs. 2 u. 3) eine an sich rechtmäßige, sie betreffende Datenverarbeitung zu unterbinden. Im Falle eines berechtigten Widerspruchs dürfen die Daten (für die betreffenden Zwecke) nicht mehr verarbeitet werden und sind gegebenenfalls zu löschen.[58]

Art. 20 regelt das Recht auf Datenübertragbarkeit, welches der alten DSRL fremd war. Betroffene Personen können von dem Verantwortlichen verlangen, dass dieser ihnen Daten, die sie ihm bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format bereitstellt. Dies soll eine bessere Kontrolle über eigene Daten gewährleisten und z.B. den Wechsel zwischen Anbietern sozialer Netzwerke erleichtern, indem Lock-in-Effekte aufgebrochen werden.[59]

Art. 22 Abs. 1 gesteht betroffenen Personen das Recht zu, keiner Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Datenverarbeitung beruht, wenn diese ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. EwG 71 nennt beispielhaft die „automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliches Eingreifen". Damit möchte der Gesetzgeber erreichen, dass die „Letztentscheidungsbefugnis" einer natürlichen Person obliegt.[60] Hiervon sieht Art. 22 Abs. 2 allerdings Ausnahmen vor, wenn die betroffene Person bspw. eingewilligt hat (lit. c) oder die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages erforderlich ist (lit. a). Für letzteres kann als (Haupt-)anwendungsfall wohl die automatisierte Entscheidung über die Kreditvergabe nach einem Bonitätsscoring angeführt werden.[61]

Abschließend enthält Art. 23 einen Katalog an Öffnungsklauseln zur Beschränkung der in den Art. 12 bis 22 genannten Betroffenenrechte durch Rechtsvorschriften der Europäischen Union oder der Mitgliedsstaaten. Beschränkungen können z.B. im Interesse nationaler oder öffentlicher Sicherheit sowie im Interesse der Strafverfolgung erlassen werden.

E. Pflichten des Verantwortlichen

Die Art. 24 ff. regeln die Pflichten des Verantwortlichen. Der Verantwortliche der Datenverarbeitung ist der maßgebliche Normadressat der DSGVO. Nach der Legaldefinition des Art. 4 Nr. 7 handelt es sich dabei um diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Art. 24 Abs. 1 greift die Rechenschaftspflicht (Art. 5 Abs. 2) auf und verpflichtet den Verantwortlichen zu geeigneten technischen und organisatorischen Maßnahmen, um eine datenschutzkonforme Datenverarbeitung sicherzustellen und nachzuweisen. Die nachfolgenden Artikel stellen hierfür verschiedene, teils verpflichtende Instrumente wie Datenschutz durch Technik (Art. 25), Datensicherheit (Art. 32), Datenschutz-Folgenabschätzung (Art. 35) sowie Verhaltensregeln (Art. 40) und Zertifizierungen (Art. 42) bereit. Zu erwähnen ist schließlich der aus dem bisherigen deutschen Recht bereits bekannte Datenschutzbeauftragte als ein Instrument behördlicher bzw. betrieblicher Selbstkontrolle, der über Art. 37 ff. erstmalig europaweit verpflichtend wird. Drei der genannten Instrumente sollen im Folgenden kurz beleuchtet werden.

Art. 25 verpflichtet den Verantwortlichen zum Datenschutz durch Technikgestaltung (Privacy by Design) sowie zu datenschutzfreundlichen Voreinstellungen (Privacy by Default). Der Vorteil solcher technischer Lösungen besteht darin, dass der Schutz personenbezogener Daten nicht von der Einhaltung von Regelungen abhängt, sondern bereits „eingebaut" ist.[62] Beispielhaft nennt Art. 25 Abs. 1 die

55 Art. 13 Abs. 4, Art. 14 Abs. 5 lit. a.

56 EwG 63.

57 EwG 66.

58 Art. 17 Abs. 1 lit. c.

59 *Albrecht/Jotzo*, (Fn. 6), S. 87.

60 *Gola*, (Fn.2) , Art. 22 Rn. 1.

61 *Gola*, (Fn. 2), Art. 22 Rn. 30.

62 *Hornung*, ZD 2011, 51 (51 f.).

Pseudonymisierung personenbezogener Daten. Verarbeitet der Verantwortliche ausschließlich pseudonyme Daten, senkt dies die Risiken für die betroffene Person erheblich, da unbefugte Personen diese Daten ohne Kenntnis der spezifischen Zuordnungsregel keiner bestimmten Person zuordnen können.

Der Verantwortliche ist zudem gem. Art. 32 verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Datensicherheitsniveau zu gewährleisten. Die DSGVO enthält selbst keinen Katalog mit geeigneten Datensicherheitsmaßnahmen. Der Verantwortliche kann sich jedoch an bewährten Katalogen der IT-Sicherheit orientieren. Dies betrifft auf internationaler Ebene den internationalen Standard ISO 27002 und auf nationaler Ebene den IT-Grundschutz-Katalog des Bundesamts für Sicherheit in der Informationstechnik.[63]

Die DSGVO führt ferner in Art. 35 die Datenschutz-Folgenabschätzung ein. Dadurch sollen bei besonders risikobehafteten Verarbeitungsvorgängen die Risiken für die Rechte und Freiheiten betroffener Personen systematisch identifiziert, bewertet, bewältigt und überwacht werden, um geeignete Abhilfemaßnahmen zu planen und zu implementieren. Somit kann die Datenschutz-Folgenabschätzung nicht nur für solche Verarbeitungsvorgänge mit einem hohen Risiko, sondern auch als allgemeines Compliance-Tool eingesetzt werden.

F. Aufsicht, Zusammenarbeit und Kohärenz

Da europäisches Recht in erster Linie durch die Mitgliedsstaaten vollzogen wird, üben deren Behörden auch die Aufsicht über die Anwendung der DSGVO aus. Wichtig sind daher die Regelungen über die Aufsichtsbehörden (Art. 51 ff.) und deren Zusammenarbeit (Art. 60 ff.).[64]

Gem. Art. 51 Abs. 1 sehen die Mitgliedsstaaten vor, dass eine oder mehrere Aufsichtsbehörden für die Überwachung und Anwendung der DSGVO zuständig sind. In Deutschland bestehen aufgrund der föderalen Struktur Aufsichtsbehörden auf Bundes- und Landesebene, woran sich auch mit Geltung der DSGVO nichts ändern wird.

Ein zentrales Merkmal der Aufsichtsbehörden ist ihre Unabhängigkeit, die primärrechtlich in Art. 16 Abs. 2 S. 2 AEUV, Art. 8 Abs. 3 GRCh verankert ist. Unabhängigkeit bedeutet v.a., dass die Mitglieder ihre Tätigkeit frei von direkter und indirekter Beeinflussung von außen und frei von Weisungen wahrnehmen können.[65] Weitere Vorgaben zur Errichtung und Ausgestaltung der Aufsichtsbehörden durch die Mitgliedsstaaten finden sich in Art. 54.

Aufgabe der Aufsichtsbehörden ist es, die Anwendung der DSGVO zu überwachen und durchzusetzen.[66] Des Weiteren sollen sie sich mit Beschwerden betroffener Personen befassen, europaweit mit anderen Aufsichtsbehörden zusammenarbeiten und im Europäischen Datenschutzausschuss mitwirken.[67] Zur Aufgabenerfüllung verleiht ihnen Art. 58 Abs. 1 bis 3 Untersuchungs-, Abhilfe- sowie Genehmigungs- und Beratungsbefugnisse. Dies betrifft u.a. die Befugnis, den Verantwortlichen anzuweisen, die Datenverarbeitung in Einklang mit der DSGVO zu bringen, die Verarbeitung zu untersagen sowie gem. Art. 83 Geldbußen zu verhängen.[68]

Im Allgemeinen verpflichtet Art. 51 Abs. 2 die Aufsichtsbehörden zur Zusammenarbeit, um eine unionsweit einheitliche Anwendung der DSGVO zu gewährleisten. Die Zusammenarbeit konkretisiert sich v.a. in den sog. One-Stop-Shop-Fällen (Art. 56 und 60) sowie im Kohärenzverfahren (Art. 63 ff.). Im Sinne einer einheitlichen Anwendung der DSGVO wurde überdies der Europäische Datenschutzausschuss als Nachfolger der Art. 29-Datenschutzgruppe geschaffen.[69] Dieser Ausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedsstaates sowie dem Europäischen Datenschutzbeauftragten.[70] Er handelt unabhängig und soll gemäß Art. 70 Abs. 1 S. 1 die einheitliche Anwendung der DSGVO sicherstellen. Anders als die in erster Linie beratende Art. 29-Datenschutzgruppe kann er auch verbindliche Entscheidungen treffen, z.B. zur Streitbeilegung im Kohärenzverfahren in den One-Stop-Shop-Fällen.[71]

Das Prinzip des One-Stop-Shops stellt eine wichtige Innovation der DSGVO dar.[72] Grundsätzlich bestimmt Art. 55 Abs. 1, dass jede Aufsichtsbehörde für die Wahrnehmung der Aufgaben und Befugnisse im Hoheitsgebiet ihres Mitgliedsstaates zuständig ist. Ist aber eine grenzüberschreitende Verarbeitung im Sinne von Art. 4 Nr. 23 gegeben, sieht Art. 56 Abs. 1 vor, dass die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters als sog. federführende Aufsichtsbehörde gem. dem Verfahren nach Art. 60 fungiert. Die federführende Aufsichtsbehörde ist die einzige Ansprechpartnerin für den Verantwortlichen oder den Auftragsverarbeiter.[73] Dadurch soll verhindert werden, dass sich Unternehmen bei grenzüberschreitender Verarbeitung mit den zuständigen Aufsichtsbehörden mehrerer Mitgliedsstaaten auseinandersetzen müssen, was ihre Tätigkeit im Binnenmarkt behindern könnte.[74] Der federführenden Aufsichtsbehörde wiederum fällt es anheim, mit den anderen betroffenen Aufsichtsbehörden im Einklang mit Art. 60 zusammenzuarbeiten.[75] Dazu kann sie gem. Art. 60 Abs. 2 um Amtshilfe ersuchen oder gemeinsame Maßnahmen mit anderen Aufsichtsbehörden durchführen. Zuvorderst aber obliegt ihr die Ausarbeitung eines Beschlussentwurfes, über den im Streitfall im Kohärenz-

63 Vgl. *Kramer/Meints*, in: Auernhammer, DSGVO/BDSG, 5. Aufl. 2017, Art. 32 Rn. 47 f.

64 *Albrecht/Jotzo*, (Fn. 6), S. 113.

65 Art. 52 Abs. 2.

66 Art. 57 Abs. 1 lit. a.

67 Vgl. Art. 57 Abs. 1 lit. f, g und t.

68 Vgl. Art. 58 Abs. 2 lit. d, f und i.

69 Art. 68 ff.

70 Art. 68 Abs. 3.

71 Vgl. Art. 65.

72 *Gola*, (Fn. 2), Art. 56 Rn. 1.

73 Art. 56 Abs. 6.

74 *Albrecht/Jotzo*, (Fn. 6), S. 117 f.

75 Art. 60 Abs. 1.

verfahren durch den Europäischen Datenschutzausschuss entschieden wird.[76] Der endgültige Beschluss ergeht dann nach Art. 60 Abs. 7 bis 9. Ausnahmen vom One-Stop-Shop finden sich in Art. 55 Abs. 2 und 56 Abs. 2.

G. Ausblick

Mit Schaffung der DSGVO wurde zwar eine neue Ära des Datenschutzrechts, nicht aber dessen goldenes Zeitalter eingeläutet. Ihre zahlreichen Öffnungsklauseln werden auch in Zukunft für eine gewisse datenschutzrechtliche Heterogenität in Europa sorgen und einige Inkonsistenzen harren der Novellierung.

Nichtsdestotrotz darf die Datenschutzreform als Fortschritt gewertet werden. So werden innovative Instrumente, wie die Datenschutz-Folgenabschätzung oder Privacy by Design, (erstmalig) normiert. Auf Unternehmensseite dürften die Änderungen der DSGVO – insbesondere der weite Anwendungsbereich und die signifikante Anhebung möglicher Bußgelder – zudem zu mehr datenschutzrechtlicher Sensibilität führen.

Ob die DSGVO die anfangs beschriebenen Herausforderungen in der Praxis bewältigen kann, wird jedoch auch davon abhängen, wie sie künftig auf europäischer und mitgliedsstaatlicher Ebene mit Leben gefüllt wird. Das gilt in besonderem Maße für die datenschutzrechtliche Einhegung der schnelllebigen und disruptiven Entwicklungen der Informationstechnologie. Gerade mit Blick auf diese sind aus den abstrakten Vorgaben und Grundsätzen der DSGVO konkrete Anforderungen und Maßnahmen zu entwickeln, die einen angemessenen Ausgleich zwischen dem Schutz der betroffenen Personen und den Interessen der datenverarbeitenden Akteure herstellen. Die europäische Datenschutzreform stellt daher einen Meilenstein, aber gewiss nicht den Endpunkt der datenschutzrechtlichen Entwicklung in Europa dar.

[76] Vgl. Art. 60 Abs. 3 u. 4 sowie Art. 65 Abs. 1 lit. a.