Die Europäische Datenschutz-Grundverordnung

- ein Überblick -

Stand: 28.04.2016

Thilo Weichert
Waisenhofstr. 41, 24103 Kiel
0431 9719742
weichert@netzwerk-datenschutzexpertise
www.netzwerk-datenschutzexpertise.de

Inhalt

Inhalt 2
1. Entstehung der EU-DSGVO 3
2. Rechtlicher Rahmen 4
3. EuGH-Rechtsprechung 4
4. Zielsetzungen 6
5. Konfliktlinien 7
6. Struktur des EU-DSGVO 8
7. Anwendungsbereich 9
8. Grundprinzipien 10
9. Einwilligung 11
10. Besondere Datenkategorien 12
11. Betroffenenrechte 13
12. Verantwortlichkeit 14
13. Regulierte Selbstregulierung 16
14. Auslandsdatentransfer 17
15. Aufsichtsbehörden, Kooperation und Kohärenz 18
16. Rechtsschutz und Sanktionen 19
17. Sonderregelungen 20
18. Ausblick 21
Abkürzungen 23

1. Entstehung der EU-DSGVO

Am 08.04.2016 beschlossen der Rat der Europäischen Union (EU) und am 14.04.2016 das Parlament der EU[1] einen neuen Rechtsrahmen zum Schutz personenbezogener Daten in der Europäischen Union, auf die sich diese am 15.12.2015 mit der Kommission der EU im sog. Trilog geeinigt hatten.[2] Dieser Rechtsrahmen hat zwei Bestandteile, eine Richtlinie für den Datenschutz in den Bereichen Justiz und Polizei[3] sowie eine Europäische Datenschutz-Grundverordnung (EU-DSGVO).[4] Das Kernstück des neuen Rechtsrahmens ist die EU-DSGVO, mit der die Europäische Datenschutzrichtlinie (EG-DSRl) aus dem Jahr 1995[5] abgelöst wird.

Der Diskussion über die EU-DSGVO lag ursprünglich ein Vorschlag der EU-Kommission vom 25.01.2012 zugrunde.[6] Das EU-Parlament beschloss dann mit großer Mehrheit am 12.03.2014 eine Vielzahl von Änderungsvorschlägen.[7] Mit Datum vom 15.06.2015 hatte sich der EU-Rat auf seine Haltung zur EU-DSGVO verständigt.[8] Für die Erarbeitung und Aushandlung der EU-DSGVO war das informelle Trilog-Verfahren gewählt worden, mit dem die Einberufung eines komplexen und möglicherweise zeitlich nicht überschaubaren Vermittlungsverfahrens vermieden wurde.

Bevor die Kommission ihren Vorschlag vorgelegt hatte, waren in Bezug auf den geplanten Rechtsrahmen zwei Konsultationen durchgeführt worden und zwar die vom 09.07. bis 31.12.2009 „zum Rechtsrahmen für das Grundrecht auf Schutz personenbezogener Daten“ sowie vom 04.11.2010 bis 15.01.2011 „zum Gesamtkonzept der Kommission für den Datenschutz in der Europäischen Union“. Ihr „Gesamtkonzept“ hatte die EU-Kommission am 04.11.2010 vorgestellt.[9] Der EU-Rat hatte am 24.02.2011 Schlussfolgerungen angenommen, in denen er das Reformvorhaben der Kommission unterstützte. Mit einer Entschließung vom 06.07.2011 hatte das EU-Parlament einen Bericht angenommen, der das Kommissionskonzept für die Reform der Datenschutzregelungen guthieß.

---

1 PM Europäisches Parlament, Parlament verabschiedet EU-Datenschutzreform – EU fit fürs digitale Zeitalter, 14.04.2016, http://www.europarl.europa.eu/news/de/news-room/20160407IPR21776/Parlament-verabschiedet-EU-Datenschutzreform-%E2%80%93-EU-fit-f%C3%BCrs-digitale-Zeitalter.

2 PM EU-Kommission, Einigung über die EU-Datenschutzreform der Kommission wird digitalen Binnenmarkt voranbringen, 15.12.2015, http://europa.eu/rapid/press-release_IP-15-6321_de.htm.

3 Weichert DANA 1/2016, 8ff., http://www.netzwerk-datenschutzexpertise.de/dokument/eu-datenschutzrichtlinie-f%C3%Bcr-polizei-und-justiz.

4 Rat der Europäischen Union v. 06.04.2016, Interinstitutionelles Dossier: 2012/0011 (COD) v. 06.04.2016, 5419/16, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE.

5 Richtlinie 95/46/EG.

6 KOM (2012) 11.

7 Dok. 7427/14.

8 Dok. 9565/15.

9 KOM(2010)699 endg.

2. Rechtlicher Rahmen

Die Vorschriften der nun verabschiedeten Grundverordnung zielen auf zweierlei ab: auf den Schutz des Grundrechts auf Datenschutz und die Garantie des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

In Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist der Grundsatz verankert, dass jede Person das Recht auf Schutz ihrer personenbezogenen Daten hat. Seit dem Vertrag von Lissabon verfügt die EU mit Art. 16 Abs. 2 AEUV über eine besondere Rechtsgrundlage für den Erlass von Datenschutzvorschriften.

Der europäische Rechtsrahmen zum Datenschutz in der EU hat zwei völkerrechtliche bzw. verfassungsrechtliche Grundlagen, nämlich Art. 8 der Europäischen Menschenrechtskonvention (EMRK) sowie die Art. 7 und 8 der Europäischen Grundrechtecharta (EuGRCh):

Art. 8 EMRK *– Recht auf Achtung des Privat- und Familienlebens*

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Art. 7 EuGRCh *– Achtung des Privat- und Familienlebens*

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Art. 8 EuGRCh *– Schutz personenbezogener Daten*

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

3. EuGH-Rechtsprechung

Mit der unter Ziffer 2 dargestellten, grundrechtlichen Absicherung des Datenschutzes besteht eine robuste rechtliche Grundlage für die Rechtsprechung des Europäischen Gerichtshofs (EuGH). Dieser

bekräftigte insbesondere durch folgende drei Entscheidungen den europäischen digitalen Grundrechtsschutz:

Im Urteil vom 08.04.2014 (C-293/12) hob der EuGH die Richtlinie zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten[10] wegen eines Verstoßes gegen Art. 7 und 8 EuGRCh auf. Das Fehlen einer inhaltlichen Begrenzung der anlasslosen Speicherung auf Vorrat und das Fehlen von verfahrensrechtlichen Sicherungen sind mit dem individuellen Grundrechtsschutz nicht vereinbar.

Während sich das vorgenannte Urteil gegen eine hoheitlich angeordnete Datenverarbeitung richtete, bestätigte das Urteil des EuGH vom 13.05.2015 (C-131/12) zum Fall Google vs. Gonzales die Anwendbarkeit des Datenschutzgrundrechts auf private Datenverarbeitung. Das Urteil zum „Anspruch auf Vergessen“ konkretisiert in diesem Bereich die Anwendbarkeit des Verhältnismäßigkeitsprinzips in jedem Einzelfall und stellt klar, dass bei Vorliegen einer Niederlassung in einem Mitgliedstaat dessen Datenschutzrecht anwendbar ist.

Im Urteil vom 06.10.2015 (C-362/14) auf Vorlage des Irish High Court anlässlich der Klage von Max Schrems gegen den irischen Datenschutzbeauftragten wegen Untätigkeit gegenüber Facebook konkretisierte der EuGH seine grundrechtlichen Anforderungen an Datenübermittlungen von Europa in Staaten, in denen kein angemessenes Datenschutzniveau besteht, und stellte klar, dass dabei das Verbot anlassloser Massenüberwachung relevant ist.

Der EuGH hat sich darüberhinaus in weiteren Urteilen zum Datenschutz und zur Anwendung der EG-DSRl geäußert, wovon hier einige wichtige aus der jüngeren Zeit aufgezählt werden sollen:

U. v. 01.10.2015 (C-201/14) Agentia Nationala de Administrare Fiscala (ANAF) – Rechtsgrundlage für Übermittlung von Steuerdaten

U. v. 01.10.2015 (C-230/14) Weltimmo s. r. o. – Ausführungen zum Begriff der Niederlassung und zum anwendbaren nationalen Recht

U. v. 11.12.2014 (C-212/13) Rynes – private Videoüberwachung im öffentlichen Raum

U. v. 13.10.2013 (C-291/12) Schwarz – biometrische Daten im Reisepass

U. v. 16.10.2012 (C-614/10) Österreichische Datenschutzkommission – unabhängige Datenschutzkontrolle

U. v. 24.11.2011 (C-468/10, C-469/10) ASNEF/FECEMD – Pflicht zur Interessenabwägung

U. v. 09.11.2010 (C-92, 93/10) Schecke – Veröffentlichung von Argarbeihilfeempfängern

U. v. 29.06.2010 (C-28/08P) Bavarian Lager – Veröffentlichung in Unionsorgan

U. v. 09.03.2010 (C-518/07) Deutsche Datenschutzaufsicht – unabhängige Datenschutzkontrolle

[10] 2006/24/EG.

4. Zielsetzungen

Zur Erreichung der Rechtsetzungsziele – einem hohen Datenschutzstandard und dem freien Fluss personenbezogener Daten im Binnenmarkt – schälten sich im Laufe der Diskussionen über die EU-DSGVO folgende Zwischenziele hieraus:

- Es werden *einheitliche verbindliche Regelungen* angestrebt, die europaweit gelten und direkt anwendbar sind.
- Für die Anwendbarkeit der EU-DSGVO soll das *Marktortprinzip* gelten; d. h. die europäischen Verbraucher und Betroffenen sollen durch das für sie vor Ort geltende europäische Recht geschützt werden, unabhängig davon, wo die Datenverarbeitung erfolgt und wo der Sitz der verarbeitenden Stelle liegt.
- Über den sog. *One-Stop-Shop* soll für ein Unternehmen vorrangig die örtliche Datenschutzbehörde zuständig sein, so dass eine Kommunikation in einer konkreten Frage zum Datenschutz ausschließlich mit dieser erfolgt. Die Abstimmung der Position dieser Aufsichtsbehörde mit den anderen Aufsichtsbehörden, in deren Zuständigkeit ein Unternehmen auf dem Markt agiert, hat innerhalb des administrativen Bereichs zu erfolgen.
- Die *Transparenz für die Betroffenen* soll verbessert und den modernen technischen Gegebenheiten angepasst werden.
- Der *technische Datenschutz* soll durch neue Instrumente verbessert werden, bei denen die Prinzipien des Privacy by Design und Privacy by Default sowie der Datensparsamkeit schon bei der Technikgestaltung berücksichtigt werden.
- Über eine *Risikofolgenabschätzung* soll zwischen risikoreichen Anwendungen und sonstigen Verfahren differenziert werden. Bei geringerem Risiko soll für die Unternehmen der bürokratische Aufwand reduziert werden, während bei komplexen Verfahren ein adäquater Schutz angestrebt wird.
- Nicht nur der Datenaustausch innerhalb der EU bzw. des Binnenmarktes soll gefördert werden, sondern auch mit Staaten, in denen ein angemessener Datenschutz besteht. Fehlt dieser, so sind verbindliche und rechtssichere *Instrumente für den Drittland-Datentransfer* vorgesehen.
- Durch Verbesserung der Rechte der Betroffenen und deren Möglichkeit, durch *administrative und gerichtliche Verfahren* Rechtsschutz zu erlangen, sollen die bestehenden Vollzugsdefizite abgebaut werden.
- Über präventiv wie auch repressiv wirkende angemessen hohe *Sanktionen* soll die Bereitschaft zur Umsetzung des Datenschutzes und zur Compliance bei den verantwortlichen Stellen gefördert werden.

5. Konfliktlinien

Die bestehenden Regelungen in der EU und die Rechtsprechung des EuGH zum europäischen Datenschutz heben sich von der Gesetzeslage und der Rechtsprechung zum *Datenschutz in den USA* ab. Dort bestehen keine einheitlichen und umfassenden Regelungen. Vielmehr ist der Schutz des allgemeinen Persönlichkeitsrechts und sonstiger Grundrechte bei digitaler Datenverarbeitung nur fragmentarisch in unterschiedlichen Gesetzen auf nationaler und Bundesstaats-Ebene geregelt und betrifft jeweils nur spezifische Sektoren. Hinsichtlich der international äußerst relevanten Internetdatenverarbeitung durch US-Unternehmen gibt es in den USA nur wenige zwingende Vorgaben. Diese entsprechen den europäischen Datenschutzstandards nicht einmal im Ansatz. Der US-Supreme Court erkennt allenfalls Betroffenenrechte hinsichtlich „reasonable expectations of privacy" an, was keinen umfassenden Grundrechtsschutz zur Folge hat. Einen Grundrechtsschutz von Nicht-US-Bürgerinnen und -Bürgern kennen die USA bisher nicht. Grundrechte sind grundsätzlich nur für US-Bürger und nur gegenüber dem Staat wirksam. Sind Daten an Dritte gelangt, so können Betroffene keinen spezifischen Schutz erwarten (Third-Party-Doctrine).[11] Demnach bestehen zwischen Europa und den USA, obwohl ein intensiver Datenaustausch gepflegt wird, gewaltige Unterschiede hinsichtlich des Schutzes personenbezogener Daten. Wegen der Präsenz von US-Unternehmen auf dem europäischen Markt und der Unwilligkeit von global agierenden Firmen, europaspezifische Schutzvorkehrungen vorzusehen, versuchten die US-Regierung und US-Unternehmen in starkem Maße auf die Diskussionen zur EU-DSGVO Einfluss zu nehmen.

Deutschland war eines der EU-Mitgliedsländer, das sich inhaltlich am stärksten gegen die Verabschiedung einer einheitlichen Datenschutzregelung in Form einer direkt anwendbaren Verordnung zur Wehr setzte. Dabei wurde argumentiert, es dürfe keine Absenkung gegenüber dem bisher erreichten deutschen Standard geben. Einer einheitlichen direkt anwendbaren Regelung bedürfe es nicht. Der Bundesrat erhob demgemäß eine Subsidiaritätsrüge.[12] Dem *Subsidiaritätsprinzip* nach Art. 5 Abs. 3 EUV zufolge darf die Union nur tätig werden, sofern und soweit die verfolgten Ziele von den Mitgliedstaaten allein nicht ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs oder ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind. Die Rüge wurde von der EU mit dem Hinweis darauf zurückgewiesen, dass bei Wirtschaft und Verwaltung innerhalb der EU ein die Grenzen überschreitender Datenaustausch immer wichtiger werde. Nur über harmonisierte kohärente Regelungen könnten bürokratische Hürden abgebaut werden. Daher wurden die Versuche der deutschen Seite zurückgewiesen, an Stelle einer direkt anwendbaren Verordnung wieder eine Richtlinie zu erlassen.

Von deutscher Seite, der Verwaltung sowohl des Bundes wie auch einiger Länder, wurde zudem befürchtet, die ausdifferenzierten nationalen bereichsspezifischen Regelungen, die es insbesondere *im öffentlichen Bereich* gibt, müssten zugunsten der allgemeineren europäischen Regelungen vollständig aufgegeben werden. Dem hat die Verordnung nun in der Form Rechnung getragen, dass an vielen Stellen Öffnungsklauseln und Konkretisierungsmöglichkeiten für die nationalen Gesetzgeber aufgenommen wurden.

---

11 Weichert RDV 2012, 113 ff.

12 Nguyen DuD 2013, 662.

Ein zentraler Konfliktpunkt bei der Debatte über die Verordnung war, welche *Rolle die Einwilligung* spielen soll und wann eine Einwilligung angenommen werden kann. Kurz bevor der Kommissionsvorschlag Anfang 2012 von der Kommission vorgestellt wurde, kursierte noch eine Formulierung, die eine Datennutzung für Zwecke der Werbung und des Adresshandels grds. nur auf der Grundlage einer Einwilligung zulassen wollte. Streitig war, ab wann Kinder als einwilligungsfähig angesehen werden können. Diskutiert wurden zudem der Grad der Konkretisierung, die Art der Erklärung und die Abgabe in Abhängigkeitsverhältnissen. Während bisher z. B. in Großbritannien Information über die Verarbeitung mit einer Opt-out-Möglichkeit für eine Einwilligung als ausreichend angesehen wird, bestehen in anderen EU-Mitgliedstaaten höhere Anforderungen an die Bestimmtheit und die Freiwilligkeit.

Von Seiten der Wirtschaft wurde vielstimmig vorgetragen, eine strenge *Zweckbindung* und der Grundsatz der *Datensparsamkeit* würden Big-Data-Geschäftsmodelle zunichtemachen. Insbesondere die deutsche Bundesregierung machte sich mit diesem Argument für einen Verzicht auf den Grundsatz der Datensparsamkeit und eine möglichst vage Formulierung zur Zweckbindung stark.[13] Diese Positionen konnten sich letztlich nicht durchsetzen.

Streitig waren zudem die *Sanktionen*. Zwar waren sich alle Beteiligten darüber einig, dass der niedrige Sanktionsrahmen in vielen EU-Mitgliedstaaten völlig unzureichend ist, um der Androhung von Bußgeldern eine abschreckende Wirkung zukommen zu lassen. Während die Kommission und vor allem der Rat zur Mäßigung mahnten, wollte das Parlament einen weiten Rahmen. Da der Rahmen nicht ausgeschöpft werden muss, setzte sich schließlich ein relativ weitgehendes Sanktionsregime durch.

6. Struktur des EU-DSGVO

Die Grundverordnung ist in 11 Kapitel gegliedert, deren Struktur sich weitgehend an den bestehenden Datenschutzgesetzen und der EG-DSRl orientiert. Einen Schwerpunkt und Innovationen setzt die Verordnung weniger im materiell-rechtlichen Bereich als im administrativen, im technisch-organisatorischen sowie im prozeduralen Bereich. Die verbindlich geltende EU-DSGVO soll künftig an der Spitze einer hierarchischen Regelungsstruktur stehen, in der nationale Gesetze oder andere nachgeordnete Normen und Festlegungen spezielle Präzisierungen vornehmen können.

Die Zählweise der Artikel orientierte sich während der Diskussion in den EU-Gremien an den Vorgaben der EU-Kommission. Da jedoch ganze Artikel und Absätze gestrichen und andere hinzugefügt wurden, erfolgte vor der Beschlussfassung eine neue Durchnummerierung. Im folgenden Text werden die Artikel gemäß der endgültigen Beschlussfassung nummeriert.

[13] Netzwerk Datenschutzexpertise, Wirtschaft 4.0, Big Data und der Datenschutz, http://www.netzwerk-datenschutzexpertise.de/big-data.

Gliederung EU-DSGVO (Ziffern vor dem Schrägstrich Beschlussfassung/dahinter in der Entwurfsfassung)

Kap. 1 Allgemeine Bestimmungen (1-4)

Kap. 2 Grundsätze (5-11/5-10)

Kap. 3 Rechte der Betroffenen Person (13-23/11-21)

Kap. 4 Für Verarbeitung Verantwortlicher und Auftragsdatenverarbeiter (24-43/22-39a)

Kap. 5 Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen (44-50/40-45)

Kap. 6 Unabhängigkeit der Aufsichtsbehörden (51-59/46-54)

Kap. 7 Zusammenarbeit und Kohärenz (60-76/54a-72)

Kap. 8 Rechtsbehelfe, Haftung und Sanktionen (77-84/73-79b)

Kap.9 Besondere Datenverarbeitungssituationen (85-91/80-85)

Kap. 10 Delegierte Rechtsakte und Durchführungsrechtsakte (92, 93/86, 87)

Kap. 11 Schlussbestimmungen (94-99/88-91)

7. Anwendungsbereich

Die EU-DSGVO wird die zentrale Datenschutzregelung in der EU, ist aber nicht in allen Bereichen in der EU anwendbar. Dort, wo Unionsrecht keine Gültigkeit hat, gilt auch die EU-DSGVO nicht. Entsprechendes gilt für Tätigkeiten nach Titel V Kapitel 2 EUV, also die gemeinsame Außen- und Sicherheitspolitik. Für Tätigkeiten zum Zweck der polizeilichen und justiziellen Verhütung und Verfolgung von Straftaten gilt die zeitgleich konsentierte EU-Datenschutzrichtlinie für Justiz und Polizei.[14] Weitere Ausnahmen sind die personenbezogene Verarbeitung von Daten in ungeordneten Akten sowie, wenn sich die Datenverarbeitung ausschließlich auf den persönlichen oder familiären Bereich bezieht (sog. Haushaltsausnahme). Soweit Organe der EU tätig werden, gilt weiterhin die Verordnung EG Nr. 45/2001. Unberührt bleibt weiterhin die Datenschutzrichtlinie für den Telekommunikationsbereich, welche die Verarbeitung von Bestands- und Verkehrsdaten von Netzdiensteanbietern regelt (Art. 2).

Es gilt das Marktortprinzip. Danach kommt es nicht darauf an, wo physisch die Datenverarbeitung erfolgt. Relevant ist vielmehr, dass die Verarbeitung einer verantwortlichen Stelle oder eines Auftragsdatenverarbeiters auf eine Person abzielt, die sich in der EU aufhält (Art. 3).

Die Begriffsbestimmungen bringen im Vergleich zur EG-DSRl keine wesentlichen inhaltlichen Änderungen, wohl aber Erweiterungen: Neu definiert werden z. B. Begriffe wie „Profiling“, „Pseudonymisierung“, „genetische Daten“, „biometrische Daten“, „Hauptniederlassung“, „Vertreter“,

[14] Weichert DANA 1/2016, 8.

„Unternehmen“, „Unternehmensgruppe“ oder „verbindliche unternehmensinterne Datenschutzvorschriften“, was bisher mit dem englischen Begriff „Binding Corporate Rules“ (BCRs) bezeichnet worden ist (Art. 4).

8. Grundprinzipien

Im deutschen Datenschutzrecht war es bisher nicht üblich, Gesetzen *Grundprinzipien* voranzustellen, anders nun in Europa in Art. 5. Dies ist systematisch zu begrüßen. Bei der Auslegung der weiteren Regelungen sollte und kann immer hierauf zurückgegriffen werden. Außerdem wird dem mit dem Datenschutzrecht nicht vertrauten Menschen kurz und bündig klargestellt, welche generellen Erwägungen die EU-DSGVO prägen. Diese sind für erfahrene Anwender alle keine Unbekannten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz,
- Zweckbindung,
- Richtigkeit,
- Erforderlichkeit, die etwas sperrig „Speicherbegrenzung“ genannt wird,
- Integrität und Vertraulichkeit,
- Verantwortlichkeit, die unter dem Begriff „Rechenschaftspflicht“ geführt wird.

Hervorzuheben ist, dass als weiterer Grundsatz die „*Datenminimierung*“ erwähnt wird. Wirtschaftsvertreter wie auch die deutsche Bundesregierung hatten noch kurz vor Abschluss des Trilogs dafür gekämpft, das Prinzip der Datensparsamkeit aus der EU-DSGVO zu verbannen, weil damit die Chancen der europäischen Wirtschaft bei der Entwicklung zukunftsweisender und lukrativer Big-Data-Konzepten beschnitten würden.[15] Davon unbeeindruckt findet sich dieser Grundsatz nicht nur eingangs prominent, sondern an vielen weiteren Stellen, so insbesondere in Art. 25, wo als Instrumente der Datenminimierung die Pseudonymisierung und „Privacy by Default“ genannt werden, im Rahmen von Zertifizierungen (Art. 25 Abs. 3), als Sicherheitsmaßnahme (Art. 32 Abs. 1 lit. a) sowie als Kriterium für Verhaltensregeln (Art. 40 Abs. 2 lit. d). In Art. 11 wird explizit klargestellt, dass aus einer pseudonymen oder sonstwie datensparsamen Verarbeitung keine Pflicht besteht, allein zum Zweck der Einhaltung der Verordnung zusätzliche Daten einzuholen.

Das schon bisher in der EG-DSRl geltende Verbot mit Erlaubnisvorbehalt ergibt sich aus Art. 6, der die „*Rechtmäßigkeit der Verarbeitung*“ regelt. Übersichtlicher und systematischer als z. B. in den §§ 28 ff. BDSG werden die Legitimationsmöglichkeiten für die Verarbeitung aufgezählt:

- Einwilligung,
- Vertragserfüllung,

[15] Weichert/Schuler, Datenschutz contra Wirtschaft und Big Data, 12/2015, http://www.netzwerk-datenschutzexpertise.de/big-data.

- Erfüllung einer rechtlichen Verpflichtung
- Schutz lebenswichtiger Interessen,
- Erfüllung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt,
- Wahrnehmung berechtigter Interessen, sofern die schutzwürdigen Interessen nicht überwiegen.

Der letztgenannte Punkt war umstritten. Während Datenschützer für eine Eingrenzung der *berechtigten Interessen* plädierten, setzten sich vor allem der Rat und die Wirtschaftslobby für eine Ausweitung ein. Letztendlich kam es insofern zu keiner Änderung des bisherigen Rechtszustands, der eine offene Abwägungsformel enthält (z. B. § 28 Abs. 1 S. 1 Nr. 2 BDSG).

Den Mitgliedstaaten wird in Art. 6 Abs. 3 und 4 insbesondere für die *Verarbeitung öffentlicher Stellen* und zur Erfüllung rechtlicher Pflichten ein sehr weitgehendes Konkretisierungsrecht zugesprochen. Dabei sind aber Regeln zu beachten: So muss eine klare Zweckbestimmung erkennbar sein. Eine Präzisierung kann hinsichtlich der Datenarten, der Verarbeitungsbedingungen, der Betroffenen, der verarbeitenden Stellen und der Speicherfristen erfolgen. Zu beachten ist, dass immer ein im öffentlichen Interesse liegendes Ziel in verhältnismäßiger Weise verfolgt wird.

Damit können die meisten in Deutschland geltenden *bereichsspezifischen Datenschutzregelungen* beibehalten werden. Die in der Verordnung genannten Anforderungen an solche bereichsspezifischen Regelungen entsprechen denen des deutschen Bundesverfassungsgerichts (BVerfG) an die Verfassungsmäßigkeit gesetzlicher Regelungen zur personenbezogenen Datenverarbeitung. Dies hat zur Folge, dass materiell verfassungswidrige Gesetze auch der EU-DSGVO widersprechen und umgekehrt. Enthalten die bereichsspezifischen nationalen Regelungen aber prozedurale oder organisatorische Normen, insbesondere hinsichtlich des Datenschutzmanagements bei den Verantwortlichen, der Selbstregulierung und der staatlichen Aufsicht, so kann insofern doch eine Anpassung an die EU-DSGVO erforderlich sein. Jedenfalls ist die Befürchtung, dass nach Inkrafttreten der Verordnung alle bereichsspezifischen Gesetze in Deutschland zur Randnotiz in der Datenschutzgeschichte würden, unbegründet.

Äußerst umstritten war Art. 6 Abs. 4, der die Voraussetzungen für *Zweckänderungen* regelt. Die Norm muss im Zusammenhang mit den Absätzen 1 und 2 gelesen werden, in denen allgemeine Voraussetzungen für rechtmäßige Datenverarbeitungen definiert werden. Zusätzlich werden Kriterien benannt, die bei einer Zweckänderung berücksichtigt werden müssen: a) die Verbindung des neuen mit dem ursprünglichen Zweck, b) der Erhebungszusammenhang, c) die Sensibilität der Daten, d) die möglichen Folgen der Weiterverarbeitung für die Betroffenen und e) angemessene Schutzmaßnahmen wie z. B. Verschlüsselung oder Pseudonymisierung.

9. Einwilligung

Die *Einwilligung* ist und bleibt eine zentrale Legitimation für die Datenverarbeitung (Art. 7). Die Diskussion über die Bedeutung, die Voraussetzungen und die Rahmenbedingungen von datenschutzrechtlichen Einwilligungen wird seit Jahren engagiert geführt. Diese Debatte findet mit der

EU-DSGVO kein Ende, wohl erfolgen aber einige Konkretisierungen. Die allgemeinen Anforderungen an die Einwilligung ändern sich jedoch nicht: inhaltliche Bestimmtheit, Hervorhebungspflicht, Widerrufsmöglichkeit, Freiwilligkeit.

Konkretisierungen hinsichtlich der Einwilligungserfordernisse bestehen insofern, als die Einwilligung bzw. das Ersuchen danach „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu erfolgen hat. Beim Widerruf dürfen keine formellen Hürden errichtet werden. In Art. 7 Abs. 4 wird unter dem Stichwort Freiwilligkeit ein eingegrenztes *Koppelungsverbot* normiert: Wird für einen Vertrag oder eine Dienstleistung eine Einwilligung abverlangt, „die für die Erfüllung des Vertrags nicht erforderlich ist“, so ist sie im Zweifel nicht freiwillig. Unklar sind die Rechtsfolgen einer unzulässigen Koppelung. Diese dürfte die Unzulässigkeit der gesamten Einwilligung zur Folge haben. In jedem Fall kann ein Widerruf der Einwilligung deren Wirkung für die Zukunft aufheben. Bei der Anwendung der Regelung kann es letztlich auch nicht darauf ankommen, ob eine Einwilligung als solche oder als Vertragsbestandteil bezeichnet wurde.

Die Autoren der EU-DSGVO legten sich nicht auf eine Altersgrenze für die Einwilligungsfähigkeit von *Kindern* bzw. Jugendlichen fest. In Deutschland wird bisher auf die Einsichtsfähigkeit abgestellt. Da hierüber in den nationalen Rechtskulturen unterschiedliche Vorstellungen herrschten und eine Einigung nicht möglich war, können die nationalen Gesetzgeber künftig zwischen vollendetem 13. und 16. Lebensjahr eigene Festlegungen vornehmen. Unter dieser Grenze muss bei einem Einwilligungsbedarf die Zustimmung der Eltern eingeholt werden. Es wird zudem klargestellt, dass die Einwilligung zur Datenverarbeitung und die sonstige Geschäftsfähigkeit getrennt voneinander zu beurteilen sind (Art. 8).

10. Besondere Datenkategorien

Hinsichtlich der Verarbeitung *sensitiver Daten*, also von Daten aus „besonderen Kategorien“, gibt es keine wesentlichen Änderungen: Einen besonderen Schutz gibt es auch in Zukunft für Daten zur rassischen und ethnischen Herkunft, zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben und sexueller Ausrichtung. Eine Präzisierung erfolgt dadurch, dass in den Katalog die genetischen Daten sowie biometrische Daten zur eindeutigen Personenidentifizierung aufgenommen wurden (Art. 9). Trotz der zunehmenden Schutzbedürftigkeit von Finanztransaktionsdaten, die sich durch die zunehmende Digitalisierung des Zahlungsverkehrs und deren Bedeutung für Identitätsdiebstähle ergibt, wurde die Kategorie nicht in den Schutzbereich der sensitiven Daten aufgenommen.

Die *Ausnahmen* von dem grundsätzlichen Verarbeitungsverbot erinnern an den bisherigen europäischen Regelungsrahmen. Als Ausnahme wird zunächst die explizite Einwilligung genannt. Es ist erfreulich, dass in begründeten Fällen spezialgesetzliche Einwilligungsverbote ausdrücklich zugelassen werden. In folgenden Fällen muss keine Einwilligung eingeholt werden: bei Ausübung von Rechten aus dem Arbeitsrecht, der sozialen Sicherheit und des Sozialschutzes, zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit, bei der Verarbeitung durch einen sog. Tendenzbetrieb, bei vom Betroffenen offenkundig veröffentlichen Daten, zur Durchsetzung rechtlicher Ansprüche, zur Gesundheitsvorsorge, Arbeitsmedizin, medizinischen Diagnostik, zur Versorgung und Behandlung, zur

Verwaltung im Gesundheits- und Sozialbereich, im öffentlichen Gesundheitswesen, für Archivzwecke, zur wissenschaftlichen und historischen Forschung und für statistische Belange.

Die gegenüber den bisherigen Erlaubnistatbeständen zur Verarbeitung sensitiver Daten vorgenommenen *Änderungen* sollen bisherige Regelungsdefizite beseitigen. So wird nicht mehr zwischen öffentlicher und privater Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich unterschieden, so dass, anders als bisher, Privatversicherungen von der Ausnahmeregelung mit erfasst sein können.

Bzgl. der sensitiven Daten bestehen weitgehend nationale *gesetzliche Konkretisierungsmöglichkeiten*, wobei erhöhte Verarbeitungsvoraussetzungen nötig sein können. Damit kann das hochkomplexe Regelungsgeflecht beim Datenschutz im deutschen Sozialrecht weitgehend beibehalten werden. So sehr das von Seiten der Verantwortlichen begrüßt werden dürfte, so schade ist es, dass die EU-DSGVO nicht dazu zwingt, das unstrukturiert gewordene Datenschutzrecht in den Sozialgesetzbüchern I bis XII einer Totalrevision und Bereinigung zu unterwerfen.

In der Verordnung wird ein spezifisch (national) regelungsfähiger Aspekt explizit erwähnt: die Verarbeitung besonders sensibler Daten durch Fachpersonal, das z. B. einem besonderen *Berufsgeheimnis* unterliegt. Das vorliegende Regelungskonzept machte es überflüssig, nochmals gesondert die Verarbeitung für Gesundheitszwecke zu normieren, wie es zunächst von der Kommission in einem Art. 81 vorgesehen war (siehe aber Art. 90 zu Berufsgeheimnissen allgemein). Werden Berufsgeheimnisse nicht von den in Art. 9 genannten Tatbeständen erfasst, so muss im Einzelfall geprüft werden, ob die in § 203 StGB sowie in weiteren nationalen Spezialgesetzen enthaltenen Berufsgeheimnisse von nationalen Ausnahmeklauseln erfasst werden und ob eine Kollision zur EU-DSGVO entstanden ist.

Für Daten über *strafrechtliche Verurteilungen* und Straftaten oder damit zusammenhängende Sicherungsmaßregeln werden in Art. 10 spezifische Verarbeitungsvoraussetzungen benannt: Die Verarbeitung muss „unter behördlicher Aufsicht“ erfolgen; anderenfalls bedarf es angemessener gesetzlicher Garantien.

11. Betroffenenrechte

Die Rechte der Betroffenen und deren Beschränkungen sind in den Art. 12 bis 23 geregelt. Anders als bisher ist der Normierung der einzelnen Rechte ein *allgemeiner Teil* vorangestellt, in dem Adressatengerechtigkeit, Präzision, Transparenz, Verständlichkeit, leichte Zugänglichkeit und weitestgehende Unentgeltlichkeit eingefordert werden. Als Standard-Reaktionsfrist wird der verantwortlichen Stelle ein Monat vorgegeben (Art. 12).

Die meisten der normierten *Betroffenenrechte* sind bekannt: Information bei der Erhebung (Art. 12) bzw. Information, wenn die Daten nicht beim Betroffenen erhoben werden (Art. 14), Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Sperrung (Art. 18), was technisch präziser als „Einschränkung der Verarbeitung“ bezeichnet wird, Widerspruch generell (Art. 21) bzw. bei automatisierten Einzelentscheidungen (Art. 22) und der zu einem Nutzungsverbot für Werbezwecke führende spezifische Werbewiderspruch (Art. 21 Abs. 2 u. 3).

Gegenüber den bisherigen Regelungen gibt es einige kleine *Verbesserungen*: So wird klargestellt, dass zum Berichtigungsanspruch auch das Recht auf Vervollständigung unvollständiger Daten gehört. Der Löschanspruch wird mit dem schillernden Marketing-Begriff des „Rechts auf Vergessenwerden" flankiert. Als Abwägungstopoi für den Löschungsanspruch werden die Rechte auf freie Meinungsäußerung und auf Information genannt.

Neu ist das Recht auf *Datenübertragbarkeit*. Dieses Recht bezieht sich auf Daten, die ein Wirtschaftsunternehmen vom Betroffenen auf der Basis eines Vertrages oder einer Einwilligung erhalten hat. Wenn die Verarbeitung automatisiert erfolgt, soll der Betroffene deren Bereitstellung in einer zu einem anderen Unternehmen übertragbaren Form verlangen können. Die Datenübertragung kann über den Betroffenen, aber wahlweise auch direkt zum neuen Diensteanbieter erfolgen (Art. 20). Wie dies in der Praxis umgesetzt werden soll, ist sowohl technisch als auch (außerhalb des Anwendungsbeispiels „soziale Netzwerke") vom Umfang her noch weitgehend unklar.

Die Regelung zur automatisierten Einzelentscheidung wird mit dem Zusatz „einschließlich Profiling" ergänzt. Letztlich wird versucht, damit einen Teilbereich so genannter *Big Data-Auswertungen* zu regulieren. Da der Verordnungsgeber erkannt hat, dass ihm hierzu sowohl Erfahrung als auch das nötige differenzierende Instrumentarium fehlen, behilft er sich erneut mit einer Öffnungsregelung für die nationalen oder europäischen Normgeber. Um in diesem exorbitant wichtigen Feld aber die europarechtliche Kontrolle zu wahren, werden bei der Normierung „geeignete Maßnahmen zum Schutz der Rechte und Freiheiten" gefordert. Problematisch an der Regelung bleibt, dass Big-Data-Anwendungen, die nicht auf „Entscheidungen" hinauslaufen, ausdrücklich nicht erfasst werden. Bisher war streitig, ob die Entscheidung, jemandem auf Basis von Profiling Werbung zuzusenden, unter die Regelung zu automatisierten Entscheidungen fällt. Durch die Einbeziehung des Profiling kann herausgelesen werden, dass diese Streitfrage zumindest beim Einsatz dieser Methode, was auch immer genau darunter verstanden wird, zugunsten der Betroffenen zu beantworten ist.

Eine ungewöhnliche, aber angesichts der anscheinend bestehenden nationalen Unterschiede einzig konsensfähige Regelung wurde bei der Beschränkung der Betroffenenrechte gewählt: während das Betroffenenrecht selbst sich direkt aus der Verordnung ergibt, werden die Einschränkungen national geregelt, wobei dem nationalen Gesetzgeber hierfür materielle Vorgaben gemacht werden. Dabei werden bekannte Abwägungsmuster benannt, vom „Schutz der nationalen Sicherheit" bis zum „Schutz der Rechte und Freiheiten anderer Personen" (Art. 23).

12. Verantwortlichkeit

Im Kapitel IV der Verordnung werden unter der Überschrift „Verantwortlicher und Auftragsdatenverarbeiter" verschiedene Aspekte geregelt, unter anderem auch, was bisher dem Begriff „*technisch-organisatorische Maßnahmen*" behandelt wurde. Die nun vorgelegten Regelungen gehen über das bisherige Verständnis teilweise weit hinaus. Die Verantwortlichkeiten nach der EU-DSGVO beschränken sich auch nicht auf dieses Kapitel, sondern erstrecken sich natürlich zudem auf die – an anderer Stelle geregelten – materiell-rechtlichen Pflichten wie z. B. die Erlaubnisregelungen und die Umsetzung der Betroffenenrechte.

Hinsichtlich der Datensicherheit wird, anders dies bisher explizit der Fall war, ein risikoorientierter Ansatz verfolgt. Dabei werden keine Schutzmaßnahmen aufgeführt, sondern die *Umsetzung von Datenschutzgrundsätzen* eingefordert, zu denen auch die Datenminimierung zählt (vgl. Ziffer 8). Als beschränkte Entlastung von Nachweispflichtenwird die in Art. 42 normierte Zertifizierung erwähnt (Art. 25 Abs. 3).

Der *gemeinsamen Verantwortlichkeit mehrerer Stellen*, die begründet wird durch die gemeinsame Festlegung der Zwecke und Mittel der Datenverarbeitung, wird ein eigenständiger Artikel 26 gewidmet. Dabei wird, anders als bisher, eine „Vereinbarung in transparenter Form“ gefordert, in der die Verantwortungsverteilung zu regeln ist. Fehlt eine Regelung, so hat dies für Betroffene keine nachteiligen Rechtsfolgen, da diese sich an jeden der Verantwortlichen wenden können. Angesichts der zunehmenden Arbeitsteilung bei der Datenverarbeitung, die oft nicht auf expliziten textlichen Vereinbarungen basiert, kann bezweifelt werden, ob mit der Regelung ein Fortschritt erreicht wird, der über die reine Benennung des Problems hinausgeht. Insofern hat der EuGH vom deutschen Bundesverwaltungsgericht (BVerwG) die Gelegenheit erhalten, eine dann auch für die EU-DSGVO geltende Interpretation vorzugeben, nachdem dieses dem EuGH am 25.02.2016 Fragen zur „Verantwortlichkeit“ von Facebook-Fanpagebetreibern vorlegte.[16]

Fehlt es in der EU an einer zur Verantwortung zu ziehenden Niederlassung, so muss gemäß Art. 27 ein in der EU ansässiger „*Vertreter*“ benannt werden, der im Auftrag der verantwortlichen oder der auftragsdatenverarbeitenden Stelle bzgl. aller Datenschutzfragen als „Anlaufstelle“ tätig wird.

Die *Auftragsdatenverarbeitung* in Art. 28 hat einen über den heutigen § 11 BDSG hinausgehenden Detaillierungsgrad, ohne aber die darin enthaltenen Grundprinzipien in Frage zu stellen. Die gegenseitigen Hinweis- und Informationspflichten werden genauer benannt. So soll der Auftragsdatenverarbeiter den Verantwortlichen präziser über Unterauftragsverhältnisse informieren. Unteraufträge müssen die gleiche Regelungstiefe aufweisen wie Aufträge. Es erfolgen Bezugnahmen zu genehmigten Zertifizierungen nach Art. 42 sowie genehmigten Standardvertragsklauseln. Es wird klargestellt, dass ein Auftragsdatenverarbeiter, der auftragswidrig Zwecke und Mittel der Datenverarbeitung bestimmt, als Verantwortlicher zu behandeln ist.

Ein erklärtes Ziel der EU-DSVGO ist es, den bürokratischen Aufwand des Datenschutzes abzubauen. Dies soll aber nicht dazu führen, dass der für einen wirksamen Datenschutz nötige Aufwand nicht erbracht wird. Und nötig ist in jedem Fall der Überblick über die personenbezogene Datenverarbeitung für den Verantwortlichen bzw. Vertreter, weshalb diese weiterhin ein *Verfahrensverzeichnis*, genauer ein „Verzeichnis von Verarbeitungstätigkeiten“ führen muss (Art. 30). Dies gilt auch für die Auftragsdatenverarbeiter. Nicht verpflichtet werden Stellen mit weniger als 250 Beschäftigten, es sei denn, es bestehen besondere Verarbeitungsrisiken, etwa durch die Verarbeitung von besonderen Datenkategorien oder von Daten über Straftaten.

An die Stelle des technisch völlig überholten § 9 BDSG mit Anlage tritt hinsichtlich der *technisch-organisatorischen Maßnahmen* der Art. 30. Dieser fordert statt bestimmter Schutzmaßnahmen die Einhaltung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit und benennt als Instrumente u. a. die Pseudonymisierung und die Verschlüsselung. Warum ausgerechnet diese

[16] BVerwG, B. v. 25.02.2016, Az. 1 C 28.14.

Maßnahmen durch explizite Nennung aus einer Vielzahl möglicher Maßnahmen herausgehoben werden und was unter „Belastbarkeit“ zu verstehen ist, bleibt zunächst das Geheimnis des Gesetzgebers. Gefordert wird vor Durchführung einer Verarbeitung eine explizite Risikobewertung, ein darauf abgestimmtes Schutzkonzept sowie eine regelmäßige Evaluierung.

An die Stelle der bisherigen Vorabkontrolle tritt eine risikoorientierte „*Datenschutz-Folgeabschätzung*“ bei spezifisch benannten Verfahren (systematische Personenbewertung, Verarbeitung sensibler Daten, Überwachung öffentlicher Räume) unter Einbeziehung eines möglicherweise vorhandenen Datenschutzbeauftragten (Art. 35). Es besteht die Pflicht zu einer „*vorherigen Konsultation*“ der Datenschutzaufsichtsbehörde, wenn ein hohes Risiko besteht, sofern der „Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft“ (Art. 36).

In den Art. 33 und 34 ist die Meldung bzw. Benachrichtigung von Datenschutzverletzungen gegenüber der Aufsichtsbehörde sowie den Betroffenen (sog. *Breach Notification*) geregelt.

Entgegen der Befürchtung vieler deutscher Datenschützer sind in den Art. 37 bis 39 prominent die Benennung, die Stellung und die Aufgaben der (betrieblichen bzw. behördlichen) *Datenschutzbeauftragten* normiert und festgeschrieben. Die Pflicht zur Bestellung besteht bei öffentlichen Stellen, bei der „systematischen Beobachtung von betroffenen Personen“ und bei der Verarbeitung sensibler Daten. Eine Bestellung kann national darüberhinausgehend verpflichtend gemacht werden, so dass der bestehende deutsche Regelungsrahmen beibehalten werden kann. Die rechtliche Ausgestaltung des Datenschutzbeauftragten sowie dessen Aufgaben orientieren sich stark an den bisher geltenden deutschen Bestimmungen.

13. Regulierte Selbstregulierung

Das Instrument der *Verhaltensregeln* im privaten Bereich hat bisher nicht nur in Deutschland (§ 38a BDSG) wenig Resonanz gefunden. Das soll sich künftig dadurch ändern, dass deren Funktion und die Anreize hierfür erhöht werden (Art. 40, 41). So können hierüber für Kleinst- bzw. kleinere und mittlere Unternehmen Standardisierungen und damit Vereinfachungen vorgenommen werden. Über Verhaltensregeln können „geeignete Garantien“ festgelegt werden, die bei Datenübermittlungen in Drittländer innerhalb einer Branche verpflichtend sind. Die Regeln können und müssen eine „obligatorische Überwachung“ durch installierte Verbandsmechanismen z. B. in einer Branche vorsehen. Die Verhaltensregeln unterliegen, wie bisher, der Genehmigungspflicht durch die nach Art. 51 zuständige Aufsichtsbehörde und können von der EU-Kommission für verbindlich erklärt werden. Die Überwachung der Verhaltensregeln kann zu diesem Zweck akkreditierten Stellen übertragen werden (Art. 40). Durch die verbandsinterne Streitbeilegung können Verbände den Datenschutz also selbst in die Hand nehmen und dadurch zugleich die Aufsichtsbehörden entlasten.

Völlig neu ist auf europäischer Ebene die *Zertifizierung* gemäß den Art. 42, 43. Zertifizierungsverfahren, die freiwillig sind und transparent sein müssen, können von privaten Zertifizierungsstellen oder Aufsichtsbehörden durchgeführt werden. Unter anderem ist ein „Europäisches Datenschutzsiegel“ vorgesehen, für das der Europäische Datenschutzausschuss (EDA) Prüfkriterien festlegt. Private Zertifizierungsstellen bedürfen einer Akkreditierung durch die Aufsichtsbehörde oder durch eine nationale Akkreditierungsstelle, wobei die Voraussetzungen präzise

in der Verordnung festgelegt sind. Zwecks Übersichtlichkeit werden alle anerkannten Zertifizierungsverfahren und Datenschutzsiegel in ein einheitliches Register aufgenommen. Sind die Voraussetzungen nicht (mehr) erfüllt, können sowohl Zertifizierungen als auch Akkreditierungen wieder entzogen werden. Die Kommission kann über Durchführungsakte technische Standards sowie Verfahrensvorgaben festlegen.

14. Auslandsdatentransfer

Hinsichtlich des *grenzüberschreitenden Datentransfers* ergeben sich gegenüber der Richtlinie keine grundsätzlichen Veränderungen. Wohl aber wurden viele Konkretisierungen vorgenommen, die insbesondere auch die Rechtsprechung des EuGH aufgreifen.

Innerhalb der EU gibt es keine spezifischen Übermittlungsbeschränkungen (Art. 1 Abs. 3). Gleiches gilt, wenn von der Kommission die *Angemessenheit des Datenschutzstandards* im Empfängerland festgestellt wurde. Für die Angemessenheitsprüfung enthält Art. 41 Abs. 2 einen umfangreichen Kriterienkatalog, der an die Kriterien des Safe-Harbor-Urteils des EuGHs[17] anknüpft. Darin werden folgende Bedingungen genannt: Grundrechtsgeltung, auch im Bereich der öffentlichen Sicherheit, der Verteidigung und der nationalen Sicherheit, geltende Datenschutz-Rechtsvorschriften und unabhängige Datenschutzkontrolle. Eine Überprüfung ist alle 4 Jahre nötig.

Liegt kein genereller Angemessenheitsbeschluss der Kommission vor, so können an die Stelle staatlicher Datenschutzsicherungen im Empfängerland „geeignete Garantien“ treten, die bindend und durchsetzbar sein müssen. Als Beispiele werden nun ausdrücklich Standardvertragsklauseln und unternehmensinterne Datenschutzvorschriften (sog. Binding Corporate Rules – BCRs) genannt, aber auch genehmigte Verhaltensregeln oder Zertifizierungen (Art. 46). Für die Regelungen in BCRs werden in Art. 47 präzise Anforderungen festgelegt, zu denen die Umsetzung der Betroffenenrechte, die Haftungsübernahme im Fall von Verstößen, Beschwerde- und Konfliktlösungsverfahren und die Kooperation mit der Aufsichtsbehörde gehören. In einem neuen Artikel 48, der implizit auf US-Regelungen wie den Patriot Act Bezug nimmt, wird klargestellt, dass Drittlands-Gerichts- oder Verwaltungsentscheidungen nach europäischem Recht nur dann umgesetzt werden dürfen, wenn diese auf internationalen Abkommen basieren. Diese Regelung steht konzeptionell und inhaltlich im Konflikt mit dem Ende Februar 2016 vorgestellten Privacy Shield zur Datenübermittlung von Europa in die USA, das zu exekutiven und judikativen Entscheidungen führen wird, die nicht auf internationalen Abkommen beruhen.[18]

Im *Einzelfall* können weiterhin Übermittlungen ohne allgemeine Garantien erfolgen, etwa bei ausdrücklicher Einwilligung, zur Vertragserfüllung, bei einem Betroffeneninteresse oder einem wichtigen öffentlichen Interesse, zur Durchsetzung von Rechtsansprüchen, zum Schutz lebenswichtiger Interessen oder in Rahmen einer Einzelentscheidung, die aber geeignete Garantien vorsehen muss.

---

17 EuGH, U. v. 06.10.2015, C-362/14.

18 Dazu siehe Netzwerk Datenschutzexpertise, http://www.netzwerk-datenschutzexpertise.de/file/148/download?token=AAhXas9k.

15. Aufsichtsbehörden, Kooperation und Kohärenz

Dass es bisher massive Vollzugs- und Durchsetzungsdefizite im Datenschutz gibt, liegt u. a. daran, dass es keine verbindlichen Konfliktlösungsinstrumente zwischen den unabhängigen Datenschutzbehörden gab. So konnten z. B. Unternehmen in einem Land von der dortigen unzureichenden Datenschutzkontrolle profitieren. Dies wird durch Abstimmungszwänge in Zukunft erschwert. Hinsichtlich der Einrichtung, der Rechtsstellung und den Aufgaben der *Datenschutzbehörden* selbst wurde wenig geändert. Es erfolgen v. a. Konkretisierungen zur Unabhängigkeit (Art. 52), zur demokratischen Legitimation und fachlichen Qualifikation (Art. 43), zur Verschwiegenheit (Art. 54 Abs. 2), zur Zuständigkeit (Art. 55), zu den sehr umfassenden Aufgaben (Art. 57) und zu den ebenso äußerst umfassenden Befugnissen (Art. 58). Jeder Mitgliedstaat wird verpflichtet, die Aufsichtsbehörde bzw. -behörden mit den benötigten „personellen, technischen und finanziellen Ressourcen“ auszustatten (Art. 52 Abs. 4), was angesichts der gewachsenen Aufgaben bei den Behörden zu einer massiven Besserausstattung führen muss.

Neu ist die Etablierung einer auf ein Unternehmen bezogenen *federführenden Aufsichtsbehörde*, welche die wesentliche Datenschutzkommunikation mit einer verantwortlichen Stelle führt. Federführend ist die für die Hauptniederlassung in Europa zuständige Behörde. Diese ist nur dann nicht zwingend zuständig, wenn der konkrete Vorgang ausschließlich den Zuständigkeitsbereich einer anderen Aufsichtsbehörde betrifft. Aber auch in diesem Fall kann die federführende Behörde den Vorgang innerhalb einer Frist von drei Wochen an sich ziehen (Art. 56).

Handelt es sich um einen Vorgang, der mehrere Aufsichtsbehörden betrifft oder zieht die federführende Behörde den Fall an sich, so kommen die Regelungen zur *Zusammenarbeit* zur Anwendung (Art. 60). Dazu gehören die Amtshilfe für einzelne Fragestellungen oder Sachverhaltsermittlungen, wozu der angefragten Behörde regelmäßig nur ein Monat zur Verfügung steht (Art. 61), ein umfassender zweckdienlicher Informationsaustausch und die Vorlage eines Beschlussvorschlags durch die federführende Behörde. Hiergegen kann eine andere betroffene Behörde innerhalb von vier Wochen Einspruch einlegen. Wird dem nicht abgeholfen, erfolgt das Kohärenzverfahren. Wurde kein Einspruch eingelegt, so sind alle betroffenen Behörden an den Beschluss gebunden, der dann gegenüber der (Haupt-)Niederlassung ergeht und dem Beschwerdeführer mitgeteilt wird. Eine einheitliche Beschwerde kann in Teilbeschlüsse aufgeteilt werden. Für die Zusammenarbeit wird ein gemeinsames elektronisches Kommunikationsverfahren genutzt (Art. 67).

Eine besondere Form der Zusammenarbeit besteht in *gemeinsamen Maßnahmen* (Art. 62). Diese erfolgen, wenn Beschlüsse erhebliche Auswirkungen auf die Zuständigkeitsbereiche von mehreren Behörden haben werden. Hierzu lädt eine Aufsichtsbehörde ein; jede betroffene Behörde kann sich anschließen. Die teilnehmenden Behördenmitarbeiter erhalten dann Kompetenzen gemäß dem jeweils geltenden nationalen Recht.

Im *Kohärenzverfahren*, also bei unterschiedlichen Meinungen zu einem Beschlussvorschlag, wird die Stellungnahme des *Europäischen Datenschutzausschusses (*EDA) eingeholt. Außerdem kann jede Aufsichtsbehörde bei Angelegenheiten mit allgemeiner Geltung oder Auswirkungen eine solche Stellungnahme bewirken. Die Beschlussfassung erfolgt regelmäßig innerhalb von 8 Wochen mit einer einfachen Mehrheit der EDA-Mitglieder. Soweit erforderlich und zweckdienlich, werden Informationen

übersetzt. Teilt eine Aufsichtsbehörde unter Angabe der maßgeblichen Gründe dem EDA mit, dass sie der EDA-Stellungnahme nicht folgt, so findet in einem weiteren Schritt eine Streitbeilegung durch den EDA statt (Art. 65). Diese erfolgt in Form eines innerhalb von einem Monat gefällten Beschlusses, für den eine 2/3-Mehrheit im EDA nötig ist. Die EDA-Beschlüsse werden auf der EDA-Webseite allgemein veröffentlicht.

Abweichend vom Kohärenzverfahren kann eine betroffene Aufsichtsbehörde ein *Dringlichkeitsverfahren* durchführen, durch das einstweilige Maßnahmen mit einer Geltungsdauer von höchstens 3 Monaten festgelegt werden (Art. 66).

Der Europäische Datenschutzausschuss besteht aus den Leitern der Aufsichtsbehörden, je einer pro Land. In Deutschland muss aus den föderalen Aufsichtsbehörden nach nationalen Regeln ein Behördenleiter benannt werden (Art. 68). Hauptaufgabe des EDA, dem eine eigene Rechtspersönlichkeit zukommt, ist die Abgabe von Stellungnahmen und die Beschlussfassung im Kohärenzverfahren. Daneben nennt Art. 70 viele weitere Aufgaben, u. a. die Beratung der Kommission, die Bereitstellung von Leitlinien, Empfehlungen und Verfahren, die Förderung von Verhaltensregeln und Zertifizierungsverfahren, die Akkreditierung von Zertifizierungsstellen, Stellungnahmen zum „angemessenen Schutzniveau“, die Förderung der Zusammenarbeit zwischen den Aufsichtsbehörden, einschließlich Information und Schulung des Personals sowie die Öffentlichkeitsarbeit. Geleitet wird der EDA von einem Vorsitzenden und zwei Stellvertretern, die mit einfacher Mehrheit gewählt werden. Das EDA-Sekretariat wird beim Europäischen Datenschutzbeauftragten eingerichtet (Art. 75).

16. Rechtsschutz und Sanktionen

Bisher waren die national geregelten Rechtsschutz- und Sanktionsmöglichkeiten im Datenschutzrecht sehr begrenzt. Im Safe-Harbor-Urteil hatte der EuGH schon Nachbesserungen eingefordert.[19] In diesem Bereich erfolgen in der EU-DSGVO nun sehr weitgehende Verbesserungen:

So haben *Betroffene* nicht nur gegenüber der Aufsichtsbehörde ein Beschwerderecht (Art. 77). Sie erhalten zudem eine gerichtliche Rechtsbehelfsmöglichkeit gegen eine sie betreffende rechtsverbindliche Entscheidung sowie auch, wenn eine Beschwerde nicht innerhalb von drei Monaten behandelt wurde; die abschließende Entscheidung darf längere Zeit in Anspruch nehmen (Art. 78). Ein Informationsanspruch besteht nicht nur zu den Verfahrensergebnissen, sondern auch zum Bearbeitungsstand. Mit dem neuen Instrument kann ein Betroffener eine materiell-rechtlich korrekte Entscheidung gegenüber der Aufsichtsbehörde einklagen, was bisher nicht anerkannt, geschweige denn effektiv realisiert war. Eine Rechtsschutzmöglichkeit besteht für den Betroffenen weiterhin – wie bisher – gegenüber der verantwortlichen Stelle oder dem Auftragsdatenverarbeiter, wobei verbraucherfreundlich gegen private Verantwortliche die Klage im Mitgliedstaat des Betroffenen eingelegt werden kann.

Neu ist eine Art *Verbandsklage*, bei der eine Einrichtung, Organisation oder Vereinigung die Rechte des einzelnen oder von vielen Betroffenen gerichtlich geltend machen kann. Darüber hinaus besteht für

[19] EuGH, U. v. 06.10.2015, C-362/14, NJW 2015, 3151 ff., Rn. 64 f.

die Mitgliedstaaten das Recht, unabhängig von Aufträgen von Betroffenen, Verbandsklagen zuzulassen (Art. 80). Entsprechendes erfolgte erst kürzlich in beschränktem Umfang in Deutschland.[20]

Um in Europa divergierende Entscheidungen bei parallelen Verfahren zu vermeiden, kann ein zuständiges Gericht sein Verfahren aussetzen, wenn derselbe Gegenstand vor einem anderen Gericht innerhalb des Geltungsbereichs der Verordnung anhängig ist. Es erfolgt dann eine Abstimmung zwischen den Gerichten oder eine Zusammenführung der Verfahren (Art. 81).

Wie schon bisher (in Deutschland nur im privaten Bereich), haben die Aufsichtsbehörden die Möglichkeit, Warnungen und *Untersagungsverfügungen* zu erlassen (Art. 58 Abs. 2 lit. a-h, j).

Daneben sind Sanktionen in Form von *empfindlichen Geldbußen* möglich, die „in jedem Fall wirksam, verhältnismäßig und abschreckend“ sein müssen (Art. 83 Abs. 1). Dafür benennt die Verordnung eine Vielzahl von Sanktionszumessungskriterien, die es künftig ermöglichen, über Vergleiche europaweit eine Angleichung bzw. Harmonisierung zu erreichen. Abhängig vom Verstoß können Geldbußen bis zu einer Höhe von 10, in besonderen Fällen bis zu 20 Mio. € bzw. „im Fall von Unternehmen von bis zu 2 % (4%) seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres“ verhängt werden. Ob und wenn ja, wie und in welchem Umfang Geldbußen bei Datenschutzverstößen durch öffentliche Stellen verhängt werden können, bleibt den Mitgliedstaaten überlassen (Art. 83 Abs. 7). Sieht die Verordnung für bestimmte Verstöße keine Sanktionen vor, so bleibt es den Mitgliedstaaten vorbehalten, auch diese zu sanktionieren (Art. 84).

17. Sonderregelungen

In einigen Bereichen überlässt der europäische Verordnungsgeber es den Mitgliedstaaten, *spezifische Regelungen* zu erlassen und macht hierfür Vorgaben. Dies gilt für die Datenverarbeitung „zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken“ (Art. 85), für den Zugang der Öffentlichkeit zu amtlichen Dokumenten (Art. 86), die Verwendung einer nationalen Kennziffer (Art. 87), die Datenverarbeitung im Beschäftigtenkontext (Art. 88) und die Verarbeitung „zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen und historischen Forschungszwecken und zu statistischen Zwecken“ (Art. 89).

Auf zunächst *geplante Sonderregelungen* zur Verarbeitung im öffentlichen Sektor generell, was die Bundesregierung lange gefordert hatte (Art. 80aa im Entwurf), sowie für Gesundheitszwecke (Art. 80b im Entwurf) wurde verzichtet, weil nationale Normierungsbefugnisse schon in die materiellen Regelungen (Art. 6 Abs. 3, 9 Abs. 2, 10) aufgenommen worden sind. Europäisch oder national geregelte (berufliche) Geheimhaltungspflichten können neben dem Datenschutzrecht weiterhin Anwendung finden. Dies betrifft in Deutschland beispielsweise den § 203 StGB und bereichsspezifische Konkretisierungen etwa im Anwalts-, Arzt- oder Notarrecht (Art. 90). Das in Deutschland geltende Kirchenprivileg zur Normierung des Datenschutzes soll weiterbestehen, soweit die Vorschriften „mit dieser Verordnung in Einklang gebracht werden“ (Art. 91).

[20] Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts v. 17.02.2016, BGBl. I S. 233.

Im Kommissionsentwurf war noch vorgesehen, dass die EU-Kommission eine Vielzahl von Befugnissen zum *Erlass delegierter Rechtsakte* erhält. Diese Möglichkeiten wurden weitgehend eingeschränkt, sind aber in einem gewissen Rahmen weiterhin vorgesehen (Art. 92).

In Art. 97 ist eine regelmäßige *Evaluation* der Verordnung vorgesehen, deren Ergebnis erstmals spätestens vier Jahre nach Inkrafttreten vorgelegt werden muss.

18. Ausblick

Die EU-DSGVO wird voraussichtlich im Juni 2018 in Kraft treten.

Der Anspruch der Verordnung, ein EU-weit einheitliches Datenschutzniveau festzulegen, wurde in vielen Bereichen nicht erreicht. Die EU-DSGVO enthält viele Öffnungsklauseln, durch die Mitgliedstaaten voneinander abweichende Regelungen erlaubt werden. Dieses Regelungskonzept war angesichts der bisher bestehenden, stark divergierenden nationalen Regelungen unvermeidbar. Viele Mitgliedstaaten forderten, bestimmte, aus ihrer Sicht bewährte Mechanismen beizubehalten. Dies gilt insbesondere auch für die Regierung Deutschlands, wo derzeit das europaweit wohl am stärksten ausdifferenzierte Datenschutzrecht besteht. Das Resultat, eine auch zukünftige *begrenzte Heterogenität,* war auch deshalb nicht zu vermeiden, weil differenziertere Regelungen den EU-Gesetzgeber zweifellos überfordert hätten.

Diese Heterogenität wird aber in keiner Weise zementiert. Eine *vereinheitlichende Wirkung* kann schon dadurch erreicht werden, dass durch diverse Meldepflichten gegenüber der Kommission ein Überblick über divergierende Regelungen verschafft wird. Da viele Öffnungsklauseln sich nicht nur an die nationalen, sondern auch an den EU-Gesetzgeber wenden, besteht die Aussicht, dass die EU weitere – bereichsspezifische – Regelungen erlässt.

Vorläufig ist es sehr wahrscheinlich, dass auslegungsbedürftige Regelungen in der Verordnung national oder gar regional von Anwendern, Aufsichtsbehörden und Gerichten unterschiedlich ausgelegt werden. Durch die Vorlagemöglichkeit beim EuGH nach Art. 267 AEUV sowie generell durch die Rechtsprechung des EuGH – etwa in Fällen des Art. 263 AEUV – kommt diesem Gericht auf lange Sicht eine wichtige, rechtsvereinheitlichende Funktion zu.

Die *deutschen Gesetzgeber* in Bund und Ländern – wie auch die der anderen Mitgliedsländer – sind aufgefordert, ihre bisherigen Datenschutzregelungen bis zum Inkrafttreten der Verordnung anzupassen. Dies bedeutet, dass das BDSG sowie die Landesdatenschutzgesetze zu Ausführungsgesetzen der EU-DSGVO umgestaltet werden müssen. Eine erste Meinungsbildung hierzu fand am 24.02.2016 im Ausschuss „Digitale Agenda“ des Deutschen Bundestags statt.[21] So können unter Anknüpfung an die Verordnung nationale Besonderheiten bewahrt bleiben, wie z. B. die teilweise weitergehenden Regelungen zum betrieblichen Datenschutzbeauftragten in Deutschland. Dieser Pluralismus innerhalb der EU kann und sollte für einen europäischen Föderalismus befruchtend sein und den Wettbewerb um die besten Datenschutzinstrumente befördern. Bereichsspezifische

[21] Fachgespräch Europäische Datenschutz-Grundverordnung, Ausschuss Digitale Agenda, Ausschussdrucksachen 18(24)90-93.

Regelungen – vom Aufenthaltsgesetz bis zu den Statistikgesetzen – sind daraufhin zu überprüfen, ob sie weiterhin mit der EU-DSGVO vereinbar sind.

Die vielfältigen Öffnungsregelungen belassen den nationalen Gesetzgebern in den Mitgliedstaaten einen teilweise noch sehr weitgehenden Regelungsspielraum. Diese Öffnungsregelungen beschränken sich nicht darauf, die allgemeinen Regelungen der EU-DSGVO zu präzisieren. Nationale Gesetzgeber können durch innovative Gesetzgebung auch als Vorbild für andere Mitglieder der EU dienen und dadurch den digitalen Grundrechtsschutz voranbringen. Dies ist etwa im Bereich des Beschäftigtendatenschutzes möglich und wünschenswert.[22] Innovationsbedarf besteht aber nicht nur hier, sondern in praktisch allen Bereichen der personenbezogenen Datenverarbeitung.

Der EU ist mit der EU-DSGVO zweifellos ein fortschrittliches Regelwerk zum Datenschutz gelungen. Dieses hat aber weiterhin Defizite, die sich möglicherweise erst bei der Anwendung erweisen. Die technische, ökonomische und soziale Entwicklung fordert schon heute und laufend weitere Ergänzungen und Modifikationen, mit denen der digitale Grundrechtsschutz fortgeschrieben werden kann und muss. Der Ball liegt also nun wieder im Feld der nationalen Gesetzgeber, die auf der sicheren Rechtsgrundlage der aktuellen EU-DSGVO aufsetzen können und sollten.

[22] Siehe hierzu die Vorschläge des Netzwerks Datenschutzexpertise, http://www.netzwerk-datenschutzexpertise.de/file/150/download?token=1y0VgnAz.

Abkürzungen

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise in der Europäischen Union
Art.	Artikel
BCRs	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BVerwG	Bundesverwaltungsgericht
DANA	DatenschutzNachrichten (Zeitschrift)
EDA	Europäischer Datenschutzausschuss
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EG-DSRl	Europäische Datenschutzrichtlinie
EuGH	Europäischer Gerichtshof
EuGRCh	Europäische Grundrechtecharta
EU-DSGVO	Europäische Datenschutz-Grundverordnung
ff.	fortfolgende
lit.	Buchstabe
Mio.	Millionen
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Rn.	Randnummer
StGB	Strafgesetzbuch
U./u.	Urteil/und
US/A	United States/of America
v.	von
vgl.	vergleiche
z. B.	zum Beispiel