Thilo Weichert

Die Europäische Datenschutz-Grundverordnung

Die am 25.5.2016 in Kraft getretene Datenschutz-Grundverordnung zielt auf den Schutz des Grundrechts auf Datenschutz bzw. generell der in der Europäischen Grundrechte-Charta (GRCh) enthaltenen Freiheiten und die Garantie des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten. Der Autor stellt den Inhalt der Verordnung im Einzelnen dar und zieht Vergleiche zur bisherigen Rechtslage. Er kommt dabei zu dem Ergebnis, dass der EU mit der DSGVO zweifellos ein fortschrittliches Regelwerk zum Datenschutz gelungen ist. Es hat indes weiterhin Defizite, die sich möglicherweise erst bei der Anwendung erweisen.

1. Rechtlicher Rahmen

Am 2.5.2016 trat nach Beschlüssen des Rats der Europäischen Union (EU) und des Parlaments der EU ein neuer Rechtsrahmen zum Schutz personenbezogener Daten in der Europäischen Union in Kraft, auf den sich diese am 15.12.2015 mit der Kommission der EU im sog. Trilog geeinigt hatten. Dieser Rechtsrahmen hat zwei Bestandteile: eine Richtlinie für den Datenschutz in den Bereichen Justiz und Polizei[1] sowie eine Europäische Datenschutz-Grundverordnung (DSGVO).[2] Das Kernstück des neuen Rechtsrahmens ist die DSGVO, mit der die Europäische Datenschutzrichtlinie (EG-DSRl) aus dem Jahr 1995[3] abgelöst wird.

Die DSGVO zielt auf den Schutz des Grundrechts auf Datenschutz bzw. generell der in der Europäischen Grundrechte-Charta (GRCh) enthaltenen Freiheiten und die Garantie des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten. Die völkerrechtlichen Grundlagen dafür sind insbesondere Art. 8 der Europäischen Menschenrechtskonvention (EMRK) sowie die Art. 7 und 8 GRCh mit den Grundrechten auf Achtung des Privat- und Familienlebens sowie auf Datenschutz.

2. Zielsetzungen

Um die Ziele eines hohen Datenschutzstandards und eines freien Datenflusses im Binnenmarkt zu erreichen, normiert die DSGVO folgende Zwischenziele:

- Es werden *einheitliche verbindliche Regelungen* angestrebt, die europaweit gelten und direkt anwendbar sind.
- Für die Anwendbarkeit der 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* steht für Unternehmen und Betroffene vorrangig die jeweilige örtliche Datenschutzbehörde bereit, mit der die wesentliche Kommunikation erfolgt. Deren Abstimmung mit den anderen Aufsichtsbehörden, in deren Zuständigkeit ein Unternehmen auf dem Markt agiert, hat innerhalb des administrativen Bereichs zu erfolgen und ist über umfangreiche Kooperations- und Kohärenzregeln festgelegt (s. u. 11).
- Die *Transparenz für die Betroffenen* soll verbessert und den modernen technischen Gegebenheiten angepasst werden.
- Der *technische Datenschutz* soll durch neue Instrumente verbessert werden. *Privacy by Design*, *Privacy by Default* und *Datensparsamkeit* werden zu zentralen Prinzipien bei der Technikgestaltung.
- Über eine *Risikofolgenabschätzung* wird zwischen risikoreichen Anwendungen und sonstigen Verfahren differenziert. Bei geringerem Risiko soll für die Unternehmen der bürokratische Aufwand reduziert werden; bei komplexen Verfahren wird ein adäquater Schutz angestrebt.
- 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.
- Über verbesserte Rechtsansprüche der Betroffenen und bessere Rechtsschutzmöglichkeiten sowie über *administrative und gerichtliche Verfahren* sollen 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.

3. Anwendungsbereich

Die 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 DSGVO nicht, z. B. im Geheimdienstbereich. 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*.[4] Eine weitere Ausnahme ist die personenbezogene Datenverarbeitung, die ausschließlich den persönlichen oder familiären Bereich erfasst (sog. *Haushaltsausnahme*). Soweit Organe der EU tätig werden, gilt weiterhin die Verordnung EG Nr. 45/2001. Unberührt bleibt auch die Datenschutzrichtlinie für den Telekommunikationsbereich, welche die Verarbeitung von Bestands- und Verkehrsdaten von Netzdiensteanbietern regelt (Art. 2). Diese Richtlinie sollte noch bis zum 25.5.2018 durch eine ePrivacy-Verordnung abgelöst werden. Hierzu gibt es einen Vorschlag der EU-Kommission vom Januar 2017[5] und eine Stellungnahme des EU-Parlaments vom Oktober 2017[6] (s. hierzu den Beitrag von Glatzner in diesem Heft).

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

4. Grundprinzipien

Das deutsche Datenschutzrecht kannte bisher keine normierten *Grundprinzipien*, anders nun in Europa gem. Art. 5 DSGVO. Bei der Auslegung der Regelungen kann und muss hierauf zurückgegriffen werden:

- 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.

Als weiterer Grundsatz wird die „*Datenminimierung*“ erwähnt. Wirtschaftsvertreter wie auch die deutsche Bundesregierung hatten noch kurz vor Abschluss des Trilogs dafür gekämpft, das Prinzip der Datensparsamkeit aus der DSGVO zu verbannen, weil damit die Chancen der europäischen Wirtschaft bei der Entwicklung zukunftsweisender und lukrativer Big-Data-Konzepte beschnitten würden.[7] 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.

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 bisher in Deutschland gültigen §§ 28 ff. Bundesdatenschutzgesetz (BDSG) werden die Legitimationsmöglichkeiten für die Verarbeitung aufgezählt:

- Einwilligung,
- Vertragserfüllung,
- 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.

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: Eine klare Zweckbestimmung muss erkennbar sein. Datenarten und Verarbeitungsbedingungen (z. B. Speicherfristen), die Betroffenen und die verarbeitenden Stellen müssen präzise benannt werden. In jedem Fall muss ein im öffentlichen Interesse liegendes Ziel in verhältnismäßiger Weise verfolgt werden.

Damit können die meisten in Deutschland geltenden *bereichsspezifischen Datenschutzregelungen* im Wesentlichen beibehalten werden. Die in der Verordnung genannten Anforderungen an solche bereichsspezifischen Regelungen entsprechen denen des Bundesverfassungsgerichts (BVerfG) an die Verfassungsmäßigkeit gesetzlicher Regelungen zur personenbezogenen Datenverarbeitung.

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, die allgemeine Voraussetzungen für rechtmäßige Datenverarbeitungen definieren. Zusätzlich werden Kriterien benannt, die bei einer Zweckänderung zu berücksichtigen sind: 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.

5. Einwilligung

Die *Einwilligung* bleibt eine zentrale Legitimation für die Datenverarbeitung (Art. 7). Die allgemeinen Anforderungen an die Einwilligung ändern sich nicht: inhaltliche Bestimmtheit, Hervorhebungspflicht, Widerrufsmöglichkeit, Freiwilligkeit.

Künftig muss die Einwilligung bzw. das Ersuchen danach „*in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache*" erfolgen. Beim Widerruf dürfen keine formellen Hürden errichtet werden. In Art. 7 Abs. 4 wird unter dem Stichwort Freiwilligkeit ein *Koppelungsverbot* normiert: Wird für einen Vertrag oder eine Dienstleistung eine Einwilligung abverlangt, „*die für die Erfüllung des Vertrags nicht erforderlich ist*", ist sie im Zweifel nicht freiwillig und damit unwirksam.

Die Autoren der 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 (Art. 8).

6. Besondere Datenkategorien

Hinsichtlich der Verarbeitung *sensitiver Daten*, also von Daten aus „*besonderen Kategorien*", gibt es keine wesentlichen Änderungen: Einen besonderen Schutz gibt es für Daten zur rassischen und ethnischen Herkunft, zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, zur Gewerkschaftszugehörigkeit, Gesundheit, zum Sexualleben und zur sexueller Ausrichtung. Hinzugekommen sind mit der DSGVO genetische Daten sowie biometrische Daten zur eindeutigen Personenidentifizierung (Art. 9 Abs. 1).

Die *Ausnahmen* von dem grundsätzlichen Verarbeitungsverbot erinnern an den bisherigen europäischen Regelungsrahmen. Möglich bleibt die explizite Einwilligung; per Spezialgesetz können aber auch Einwilligungsverbote festgelegt werden. In folgenden Fällen genügt eine gesetzliche Regelung und bedarf es keiner Einwilligung: 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 veröffentlichten 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.

Bezüglich der sensitiven Daten bestehen weitgehend nationale *gesetzliche Konkretisierungsmöglichkeiten*. Damit kann z. B. das hochkomplexe Regelungsgeflecht beim Datenschutz in den deutschen Sozialgesetzbüchern (SGB) weitgehend beibehalten wer-

den. Spezifisch (national) regelungsfähig bleibt auch die Verarbeitung besonders sensibler Berufsgeheimnisse durch Fachpersonal.

7. Betroffenenrechte

Die Rechte der Betroffenen und deren Beschränkungen sind in den Art. 12 bis 23 geregelt. In einem allgemeinen Teil werden dabei Adressatengerechtigkeit, Präzision, Transparenz, Verständlichkeit, leichte Zugänglichkeit und weitestgehende Unentgeltlichkeit eingefordert. Als Standard-Reaktionsfrist wird der verantwortlichen Stelle ein Monat vorgegeben (Art. 12).

Die meisten der normierten *Betroffenenrechte* sind bekannt: Information bei der Erhebung (Art. 13) 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). Der Löschanspruch wird mit dem schillernden Marketing-Begriff des „*Rechts auf Vergessenwerden*“ flankiert. Als Abwägungstopoi für den Löschungsanspruch werden u. a. 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 (Art. 20). Wie dies in der Praxis umgesetzt werden soll, ist noch weitgehend unklar.

Die Norm zur automatisierten Einzelentscheidung wird mit dem Zusatz „*einschließlich Profiling*“ ergänzt (Art. 22). Letztlich wird versucht, damit insbesondere sog. *Big Data-Auswertungen* zu regulieren. In Ermangelung eines differenzierenden Instrumentariums behilft sich die DSGVO auch hier mit einer Öffnungsregelung. Gefordert werden aber „*geeignete Maßnahmen zum Schutz der Rechte und Freiheiten*“. Unter Juristen ist streitig, ob von der Regelung auch das Profiling für Werbezwecke erfasst wird. Dafür spricht die explizite Nennung des Profilings, dessen praktisches Hauptanwendungsfeld das Marketing ist.

Ungewöhnlich und ärgerlich ist, dass bei der Beschränkung der Betroffenenrechte zugunsten nationaler Gesetzgebung eine Öffnungsklausel besteht, etwa zum „*Schutz der nationalen Sicherheit*“ oder zum „*Schutz der Rechte und Freiheiten anderer Personen*“ (Art. 23). Der deutsche Gesetzgeber hat von dieser Möglichkeit zum Nachteil der Betroffenen übermäßig Gebrauch gemacht (vgl. dazu den Beitrag von Schaar in diesem Heft).

8. Verantwortlichkeit

Fehlt es in der EU an einer zur Verantwortung zu ziehenden Niederlassung, muss gemäß Art. 27 ein in der EU ansässiger „Vertreter" benannt werden, der im Auftrag der verantwortlichen oder der auftragsverarbeitenden 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. Der Auftragsverarbeiter muss den Verantwortlichen präziser über Unterauftragsverhältnisse informieren, welche die gleiche Regelungstiefe aufweisen müssen wie Aufträge. Es wird klargestellt, dass ein Auftragsverarbeiter, 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 die Verantwortlichen bzw. Vertreter, weshalb diese weiterhin ein *Verfahrensverzeichnis*, genauer ein „*Verzeichnis von Verarbeitungstätigkeiten*" führen müssen (Art. 30). Dies gilt auch für Auftragsverarbeiter.

Hinsichtlich der Datensicherheit wird neuerdings ein risikoorientierter Ansatz verfolgt. Es werden keine Schutzmaßnahmen aufgeführt; vielmehr wird die *Umsetzung von Datenschutzgrundsätzen* eingefordert, zu denen auch die Datenminimierung zählt (Art. 25 Abs. 3; s. dazu auch den Beitrag von Rost in diesem Heft).

An die Stelle des technisch völlig überholten § 9 BDSG mit Anlage tritt hinsichtlich der *technisch-organisatorischen Maßnahmen* der Art. 32. 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. Gefordert werden vor Durchführung einer Verarbeitung eine explizite Risikobewertung, ein darauf abgestimmtes Schutzkonzept sowie eine regelmäßige Evaluierung.

An die Stelle der bisherigen Vorabkontrolle tritt die 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 „*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* festgeschrieben. Die Pflicht zur Bestellung besteht bei öffentlichen Stellen, bei der „*systematischen Beobachtung von betroffenen Personen*"

und bei der Verarbeitung sensibler Daten. Dies kann national noch umfassender geregelt werden. Deutschland hat hiervon Gebrauch gemacht.

9. Regulierte Selbstregulierung

Das Instrument der *Verhaltensregeln* im privaten Bereich hat in Deutschland (§ 38a BDSG) bisher 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 durch Wirtschaftsverbände 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 müssen eine „*obligatorische Überwachung*" durch installierte Verbandsmechanismen z. B. in einer Branche vorsehen. Sie unterliegen, wie bisher, der Genehmigungspflicht durch die zuständige Aufsichtsbehörde und können künftig von der EU-Kommission für verbindlich erklärt werden.

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. Private Zertifizierungsstellen bedürfen einer Akkreditierung durch die Aufsichtsbehörde oder durch eine nationale Akkreditierungsstelle, wobei die Voraussetzungen präzise in der Verordnung festgelegt sind.

10. Auslandsdatentransfer

Hinsichtlich des *grenzüberschreitenden Datentransfers* ergeben sich gegenüber der Richtlinie keine grundsätzlichen Veränderungen. Es wurden Konkretisierungen vorgenommen, die auf die Rechtsprechung des EuGH zurückgehen.

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[8] anknüpft und als Bedingungen nennt: Grundrechtsgeltung (auch im Sicherheitsbereich), geltende Datenschutz-Rechtsvorschriften und unabhängige Datenschutzkontrolle.

Liegt kein genereller Angemessenheitsbeschluss der Kommission vor, so können anstelle 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). In einem neuen Artikel 48, der implizit auf US-Regelungen wie den Patriot Act Bezug nimmt, wird klargestellt, dass Drittlands-Ge-

richts- oder Verwaltungsentscheidungen nach europäischem Recht nur dann umgesetzt werden dürfen, wenn diese auf internationalen Abkommen basieren.

11. 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. Unternehmen z. B. in Irland profitierten von der dortigen unzureichenden Datenschutzkontrolle. Hinsichtlich der *Rechtsstellung der Datenschutzbehörden* wurde einiges präzisiert, etwa 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). Die Aufsichtsbehörden sind mit den benötigten „*personellen, technischen und finanziellen Ressourcen*" auszustatten (Art. 52 Abs. 4).

Für jedes Unternehmen gibt es künftig eine *federführende Aufsichtsbehörde*, welche die wesentliche Datenschutzkommunikation mit dieser verantwortlichen Stelle führt. Für die Federführung ist der Ort der Hauptniederlassung in Europa ausschlaggebend (Art. 56).

Handelt es sich um einen Vorgang, der mehrere Aufsichtsbehörden betrifft oder zieht die federführende Behörde einen Fall an sich, 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. Besteht zwischen den betroffenen Aufsichtsbehörden keine Einigkeit, kommt ein recht komplizierter verbindlicher Abstimmungsprozess zur Anwendung (Art. 67). Bei diesem *Kohärenzverfahren* kommt der *Europäische Datenschutzausschuss (*EDSA) zum Einsatz. Jede betroffene Aufsichtsbehörde kann sich dabei einbringen. Die Beschlussfassung erfolgt regelmäßig innerhalb von 8 Wochen mit einer einfachen Mehrheit der EDSA-Mitglieder, im Rahmen eines qualifizierten Streitbeilegungsverfahrens durch den EDSA mit 2/3-Mehrheit (Art. 65).

Der Europäische Datenschutzausschuss (EDSA) besteht aus den Leitern der Aufsichtsbehörden, je einer pro EU-Mitgliedsland. In Deutschland muss aus den föderalen Aufsichtsbehörden nach nationalen Regeln ein Behördenleiter benannt werden (Art. 68). Geleitet wird der EDSA von einem Vorsitzenden und zwei Stellvertretern. Das EDSA-Sekretariat wird beim Europäischen Datenschutzbeauftragten eingerichtet (Art. 75).

12. Rechtsschutz und Sanktionen

Bisher waren die national geregelten Rechtsfolgen im Datenschutzrecht beschränkt wirkungsvoll. Im Safe-Harbor-Urteil hat der EuGH in Bezug auf Rechtsschutz und Sanktionsmöglichkeiten Verbesserungen eingefordert,[9] welche die DSGVO nun bereitstellt:

Betroffene haben nicht nur gegenüber der Aufsichtsbehörde ein Beschwerderecht (Art. 77), sondern auch gerichtliche Rechtsbehelfsmöglichkeiten (Art. 78). Ein Informationsanspruch besteht nicht nur zu den Verfahrensergebnissen, sondern auch zum Bearbeitungsstand. Mit dem neuen Instrument kann ein Betroffener eine materiellrechtlich korrekte Entscheidung gegenüber der Aufsichtsbehörde einklagen. Rechtsschutzmöglichkeiten bestehen für den Betroffenen weiterhin gegenüber der verantwortlichen Stelle oder dem Auftragsverarbeiter, wobei verbraucherfreundlich gegen private Verantwortliche die Klage im Mitgliedstaat des Betroffenen eingelegt werden kann.

Neu ist die nationale Möglichkeit zur Regelung einer *Verbandsklage*, bei der eine Einrichtung, Organisation oder Vereinigung die Rechte des Einzelnen oder von vielen Betroffenen gerichtlich geltend machen kann (Art. 80). Eine solche Norm besteht seit 2016 in Deutschland im Unterlassungsklagegesetz.[10]

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). Abhängig vom Verstoß können Geldbußen bis zu einer Höhe von 10 Mio. Euro, in vielen Fällen bis zu 20 Mio. Euro bzw. „*im Fall von Unternehmen von bis zu 2 % (4%) seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres*" verhängt werden. Geldbußen gegen öffentliche Stellen können national ausgeschlossen werden (Art. 83 Abs. 7). Hiervon hat Deutschland Gebrauch gemacht.

13. Sonderregelungen

In einigen Bereichen überlässt der europäische Verordnungsgeber es den Mitgliedstaaten, *spezifische Regelungen* zu erlassen und macht hierfür allgemeine Vorgaben. Dies gilt u. a. 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 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).

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. Das in Deutschland geltende Kirchenprivileg zur

Normierung des Datenschutzes soll weiterbestehen, soweit die Vorschriften „*mit dieser Verordnung in Einklang gebracht werden*“ (Art. 91).

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

14. Ausblick

Die DSGVO ist ab dem 25.5.2018 direkt anwendbar. Der Anspruch der Verordnung, ein EU-weit einheitliches Datenschutzniveau festzulegen, wurde in vielen Bereichen wegen der Öffnungsklauseln nicht erreicht. Diese gehen insbesondere auch auf deutsche Forderungen zurück. Das Resultat ist auch künftig eine *begrenzte Heterogenität.*

Diese Heterogenität wird aber in keiner Weise zementiert. Zwar ist es sehr wahrscheinlich, dass auslegungsbedürftige Regelungen der DSGVO 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 Öffnungsklauseln belassen den nationalen Gesetzgebern in den Mitgliedstaaten noch wichtige Regelungsspielräume. Nationale Gesetzgeber könnten darüber mit innovativer Gesetzgebung zum Vorbild für andere Mitglieder der EU werden und dadurch den digitalen Grundrechtsschutz voranbringen. Dies ist etwa im Bereich des Beschäftigtendatenschutzes möglich und wünschenswert.[11] Innovationsbedarf besteht aber nicht nur hier, sondern in vielen Bereichen der personenbezogenen Datenverarbeitung, etwa bei Big-Data-Anwendungen, bei Anforderungen an Hersteller, bei der Forschung oder im Bereich des Persönlichkeitsschutzes im Internet. Deutschland hat insofern bisher leider wenig Ehrgeiz gezeigt.

Der EU ist mit der DSGVO zweifellos ein fortschrittliches Regelwerk zum Datenschutz mit globaler Strahlkraft 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.

DR. THILO WEICHERT Jahrgang 1955, studierte Rechts- und Politikwissenschaften und promovierte mit einer Arbeit zum Datenschutz im strafrechtlichen Ermittlungsverfahren. Er gehörte von 1984 bis 1986 dem Landtag von Baden-Württemberg an, danach war er als Rechtsanwalt und Berater und ab 1992 als Referent beim niedersächsischen Datenschutzbeauftragten tätig. 1998 wechselte er nach Schleswig-Holstein, wo er von 2004 bis 2015 Datenschutzbeauftragter des Landes war. Er ist Mitglied des Netzwerks Datenschutzexpertise: *www.netzwerk-datenschutzexpertise.de*.

Anmerkungen:

1 Weichert, Die EU-Richtlinie für den Datenschutz bei Polizei und Justiz, DANA 1/2016, 8ff., http://www.netzwerk-datenschutzexpertise.de/dokument/eu-datenschutzrichtlinie-f%C3%Bcr-polizei-und-justiz.
2 ABl. L 119/1 v. 04.05.2016, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE.
3 Richtlinie 95/46/EG, ABl. L 281 v. 23.11.1995
4 Weichert 2016 (Anm. 1), 8.
5 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), v. 10. 1. 2017 2017/0003 (COD).
6 Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation, COM(2017)0010 – 'C8-0009/2017 – 2017/003(COD).
7 Weichert/Schuler, Datenschutz contra Wirtschaft und Big Data, 31.12.2015, http://www.netzwerk-datenschutzexpertise.de/big-data.
8 EuGH, U. v. 06.10.2015, C-362/14, NJW 2015, 3151 ff.
9 EuGH, U. v. 06.10.2015, C-362/14, NJW 2015, 3151 ff., Rn. 64 f.
10 Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts v. 17.02.2016, BGBl. I S. 233.
11 Siehe hierzu die Vorschläge des Netzwerks Datenschutzexpertise, http://www.netzwerk-daten schutzexpertise.de/file/150/download?token=1y0VgnAz.