cepStudie

EU-Datenschutzrecht

Ein Überblick über die bestehenden Vorschriften auf EU-Ebene und die aktuellen Reformbestrebungen der Kommission

Dr. Anja Hoffmann, LL.M. (Eur)

April 2017

Kernpunkte

- Diese Studie gibt einen Überblick über das bestehende EU-Datenschutzrecht und die geplanten Reformen.
- Personenbezogene Daten werden aktuell durch die **Datenschutzrichtlinie** [95/46/EG] geschützt, die in den EU-Staaten unterschiedlich umgesetzt wurde.
- Diese wird am 25.05.2018 durch die **Datenschutzgrundverordnung** [(EU) 2016/679] abgelöst. Unterschiedliche Umsetzungen entfallen dadurch.
- Die **Datenschutzgrundverordnung** unterwirft jede Datenverarbeitung weiterentwickelten Grundsätzen wie Transparenz, Zweckbindung und Datenminimierung. Sie legt Pflichten für die Datenverarbeiter und korrespondierende Rechte der Betroffenen fest und regelt, unter welchen Bedingungen personenbezogene Daten verarbeitet werden dürfen. Ferner regelt sie die Zusammenarbeit der nationalen Aufsichtsbehörden in Fällen grenzüberschreitender Datenverarbeitung und führt für den Fall der Nichteinigung ein Kohärenzverfahren ein.
- Für den Austausch personenbezogener Daten durch nationale Polizei- und Strafverfolgungsbehörden gilt die 2016 erlassene **Datenschutzrichtlinie für Polizei und Justiz** [(EU) 2016/680].
- Für den Austausch personenbezogener Daten und anderer Informationen über öffentliche elektronische Kommunikationsdienste und -netze gilt ergänzend die **Datenschutzrichtlinie für elektronische Kommunikation** [2002/58/EG]. Sie sieht spezielle Garantien zur Gewährleistung des Rechts auf Privatsphäre vor und schützt die Endnutzer vor Cookies und SPAM.
- Die Kommission hat am 10.01.2017 einen **Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation** [COM(2017) 10 final] vorgelegt, die die bisherige Richtlinie [2002/58/EG] ersetzen soll. Damit sollen die Vorschriften an die Datenschutzgrundverordnung angeglichen werden. Die neuen Regeln sollen künftig auch für internetbasierte Kommunikationsdienste wie Web.de, Whatsapp oder Skype gelten, um gleiche Wettbewerbsbedingungen zu schaffen. Sie sollen zudem generell auch für alle Anbieter gelten, die aus Drittstaaten heraus Kommunikationsdienste an Endnutzer in der EU erbringen.
- Eine eigenständige **Verordnung** gilt **für die Verarbeitung personenbezogener Daten durch die** Organe und Einrichtungen der **EU** [(EG) Nr. 45/2001].
- Die Kommission hat am 10.01.2017 einen **Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die** Organe, Einrichtungen und sonstigen Stellen der **EU** sowie zum freien Datenverkehr [COM(2017) 8 final] vorgelegt, der die bisherige Verordnung [(EG) Nr. 45/2001] ersetzen soll. Damit sollen die Vorschriften an das Niveau der Datenschutzgrundverordnung angeglichen werden.
- Die Kommission will den freien Fluss aller Daten in der EU gewährleisten und hierzu in näherer Zukunft einen **EU-Rechtsrahmen auch für nicht-personenbezogene** – insbesondere von Maschinen oder Sensoren generierte – **Daten** schaffen.

Inhaltsverzeichnis

1 Einleitung

„Daten sind das neue Öl", so beginnt ein Dokumentarfilm[1], der einen Einblick in die politisch motivierten Höhen und Tiefen des Gesetzgebungsprozesses zur EU-Datenschutzgrundverordnung gibt. In einer Welt, die zunehmend von Digitalisierung geprägt ist, hinterlassen wir alle in steigendem Umfang Datenspuren und geben zunehmend persönliche Informationen im Internet preis. Dies bietet einerseits ein gigantisches Potenzial für die Wirtschaft: immer mehr dieser Daten werden von Unternehmen gesammelt, aufbereitet und verkauft. Diese Unternehmen haben ein großes Interesse an einem freien und uneingeschränkten Datenfluss im digitalen EU-Binnenmarkt. Auf der anderen Seite wird die Gewährleistung grundrechtlich verbürgter Rechte wie ein solider Schutz der personenbezogenen Daten der Betroffenen und der Vertraulichkeit der von ihnen kommunizierten Informationen immer wichtiger. Um diesen gegenläufigen Interessen Rechnung zu tragen, werden die auf EU-Ebene geltenden Datenschutzregeln derzeit umfassend überarbeitet und reformiert.

Die Vorbereitungen zur Anpassung des nationalen Rechts an die 2016 verabschiedete EU-Datenschutzgrundverordnung[2] stecken mancherorts noch in den Kinderschuhen, da liegt bereits der nächste Vorschlag der im Rahmen der Digitalen Binnenmarktstrategie[3] geplanten Datenschutzreform auf dem Tisch. Wie in ihrem Arbeitsprogramm[4] angekündigt, hat die Kommission am 10.01.2017 ein weiteres Datenschutzpaket vorgelegt. Herzstück dieses Pakets ist der Entwurf einer neuen „E-Datenschutz-Verordnung", der die bisherige Datenschutzrichtlinie [2002/58/EG] für elektronische Kommunikation ersetzen soll. Diese Richtlinie gilt bislang neben der noch bis 2018 gültigen allgemeinen EU-Datenschutzrichtlinie. Sie beinhaltet spezielle Vorschriften und Garantien zur Gewährleistung des Rechts auf Privatsphäre und Vertraulichkeit der Nutzer, wenn Informationen über öffentliche elektronische Kommunikationsdienste wie Mobil- und Festnetztelefonie oder E-Mail und über ihre zugehörigen Netze ausgetauscht werden.

Welche Datenschutzvorschriften gibt es aktuell auf EU-Ebene und welche Neuerungen sind geplant? Wie unterscheiden sie sich inhaltlich, und in welchem Verhältnis stehen die Regelungen zueinander? Wann sind welche Vorschriften anwendbar?

Diese Studie trägt dazu bei, im Dschungel zahlreicher Reformbestrebungen im Datenschutzbereich den Überblick über die bestehenden und künftigen Regelungen auf EU-Ebene zu behalten. Sie stellt sowohl die derzeit geltenden EU-Rechtsakte als auch bereits in Kraft getretene, aber noch nicht anwendbare Änderungsrechtsakte und deren wesentlichen Inhalte vor. Außerdem befasst sie sich mit den aktuellen Reformvorschlägen. Dabei liegt der Schwerpunkt auf der Darstellung der Regelungen der Datenschutzgrundverordnung und des jüngsten Vorschlags einer Verordnung über Privatsphäre und elektronische Kommunikation. Auch das künftige Verhältnis dieser beiden Rechtsakte zueinander wird unter die Lupe genommen. Die Studie schließt mit einem Ausblick auf weitere anstehende Veränderungen der EU-Datenschutzlandschaft. Zur näheren Analyse und Bewertung des neuen Vorschlags einer E-Datenschutz-Verordnung wird das cep demnächst eine cepAnalyse (CA) veröffentlichen.

---

1 Titel des Films: „Democracy-Im Rausch der Daten", http://www.democracy-film.de/.

2 Verordnung [(EU) 2016/79] des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie [95/46/EG], ABl. L 119 vom 04.05.2016, S. 1ff.

3 Vgl. die Mitteilung der EU-Kommission vom 06.05.2015, Strategie für einen digitalen Binnenmarkt für Europa, KOM (2015) 192 (final), S. 15.

4 Arbeitsprogramm der Kommission für 2017, COM(2016) 710 final, Anhang I, S. 6.

2 Bestehende EU-Rechtsakte zum Schutz personenbezogener Daten

Nach Art. 8 Abs. 1 der EU-Grundrechtecharta (GRCh) hat jede Person das Recht auf Schutz ihrer personenbezogenen Daten. Darüber hinaus ist in Art. 7 GRCh sowie in Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention (EMRK) das Grundrecht auf Achtung des Privat- und Familienlebens verbürgt, welches auch die Vertraulichkeit der Kommunikation umfasst. Der Schutz dieser Grundrechte wird auf EU-Ebene durch eine ganze Reihe von Rechtsakten in das europäische Sekundärrecht umgesetzt. Diese Rechtsakte sollen den Schutz personenbezogener Daten und/oder die Vertraulichkeit der Kommunikation EU-weit gewährleisten.

Grundlegende Rechtsinstrumente für den Schutz personenbezogener Daten sind derzeit

- die noch bis zum 24. Mai 2018 geltende EU-Datenschutzrichtlinie [95/46/EG][5] und
- die 2016 in Kraft getretene EU-Datenschutzgrundverordnung [(EU) 2016/679][6], welche ab dem 25. Mai 2018 anwendbar wird und dann die EU-Datenschutzrichtlinie ersetzen wird.

Teilweise werden die EU-Datenschutzrichtlinie und künftig die Datenschutzgrundverordnung aber von spezielleren bereichsspezifischen Rechtsakten verdrängt. Die wichtigsten dieser bereits in Kraft getretenen speziellen Rechtsakte sind

- die Richtlinie [(EU) 2016/680][7] zum Schutz personenbezogener Daten bei der Verarbeitung durch Polizei und Justiz,
- die Verordnung [(EG) Nr. 45/2001][8] zum Schutz personenbezogener Daten bei der Verarbeitung durch EU-Organe und Einrichtungen sowie
- die EU-Datenschutzrichtlinie für elektronische Kommunikation [2002/58/EG][9] (nachfolgend als „E-Datenschutz-Richtlinie" bezeichnet).

Diese EU-Rechtsakte befassen sich schwerpunktmäßig mit dem Schutz personenbezogener Daten in der EU und werden nachfolgend überblicksweise dargestellt. Soweit andere sektorspezifische EU-Rechtsakte ebenfalls Regelungen zum Datenschutz enthalten, werden diese hier nicht thematisiert.

---

5 Richtlinie [95/46/EG] des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31 ff., letzte konsolidierte Fassung abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:01995L0046-20031120&from=EN. Näher dazu Kapitel 2.1.

6 Verordnung [(EU) 2016/79] des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie [95/46/EG], ABl. L 119 vom 04.05.2016, S. 1ff. Näher dazu Kapitel 2.2.

7 Richtlinie [(EU) 2016/680] des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 04.05.2016, S. 89ff. Näher dazu Kapitel 2.3.

8 Verordnung [(EG) Nr. 45/2001] vom 18. Dezember 2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.01.2001, S. 1 ff. Näher dazu Kapitel 2.4.

9 Richtlinie [2002/58/EG] über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.07.2002, S. 37ff.; letzte konsolidierte Fassung abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02002L0058-20091219&qid=1479897187385&from=EN. Näher dazu Kapitel 2.5.

2.1 Datenschutzrichtlinie [95/46/EG]

2.1.1 Regelungsinhalt

Seit 1995 gilt in der EU die allgemeine EU-Datenschutzrichtlinie [95/46/EG][10] (nachfolgend „DSRL"), die zu einer grundsätzlich umfassenden Harmonisierung der Gesetzgebung der Mitgliedstaaten über den Datenschutz geführt hat.[11] Diese Richtlinie zielt darauf ab, die Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten zu schützen.

Die DSRL regelt zum einen bestimmte Schlüsselkriterien für die rechtliche Zulässigkeit der Datenverarbeitung. So ist eine Verarbeitung von Daten grundsätzlich verboten und nur dann rechtmäßig, wenn der betroffene Dateninhaber eingewilligt hat oder einer der sonstigen in der Richtlinie geregelten Erlaubnistatbestände erfüllt ist.[12]

Zum anderen legt die DSRL grundlegende Prinzipien in Bezug auf die Qualität der Daten fest, die bei allen rechtmäßigen Tätigkeiten der Datenverarbeitung umgesetzt werden müssen.[13] Dazu gehören maßgeblich die Grundsätze der Datenvermeidung, Datensparsamkeit und Zweckbindung. Danach dürfen personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und müssen insbesondere nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden. Die Daten müssen dem angestrebten Zweck entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen. Ferner müssen sie sachlich richtig sein und gegebenenfalls auf den neuesten Stand gebracht werden und dürfen nicht länger als notwendig und nur für den Zweck, zu dem sie erhoben wurden, gespeichert werden.[14]

Verstärkt geschützt werden besondere Kategorien personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben. Die Verarbeitung dieser Daten ist ebenfalls grundsätzlich unzulässig und nur in noch begrenzteren Ausnahmefällen zulässig.[15]

Diese Schutzprinzipien finden ihren Niederschlag zum einen in den Pflichten, die den für die Datenverarbeitung Verantwortlichen – das sind diejenigen Stellen, die über die Zwecke und mittel der Verarbeitung personenbezogener Daten entscheiden[16] – obliegen. Zum anderen kommen sie zum Ausdruck in den Rechten der Personen, deren Daten verarbeitet werden.

So verpflichtet die DSRL die für die Datenverarbeitung Verantwortlichen unter anderem dazu, für die Sicherheit der Datenverarbeitung zu sorgen. Diese müssen geeignete Maßnahmen ergreifen, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten und die personenbezogenen Daten so gegen zufällige oder unrechtmäßige Zerstörung, Verlust oder Änderung sowie gegen unbefugten Zugang zu schützen.[17] Personen, die Zugang zu den Daten haben, dürfen nur auf Anweisung des Verantwortlichen handeln.[18] Konkrete Vorgaben hinsichtlich der Art und des Umfangs der Sicherheitsmaßnahmen regelt die DSRL jedoch nicht. Ferner müssen Verantwortliche der zu-

---

10 Vgl. Fn. 5.
11 EuGH, Urteil vom 6.11.2003, Rechtssache C-101/01, Rn. 96 (Lindqvist).
12 Art. 7 DSRL.
13 Art. 6 DSRL.
14 Vgl. auch http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=URISERV:l14012&from=EN.
15 Art. 8 DSRL.
16 Art. 2 lit. d) DSRL.
17 Art. 16 und 17 DSRL.
18 Art. 16 DSRL.

ständigen nationalen Kontrollstelle jede geplante Verarbeitung vorab melden. Diese Stelle prüft dann, ob Risiken für die Rechte und Freiheiten der betroffenen Personen bestehen.[19]

Entsprechend müssen die Mitgliedstaaten sicherstellen, dass betroffene Personen, deren Daten verarbeitet werden, unter näher geregelten Voraussetzungen bestimmte Rechte ausüben können.

Dazu gehören insbesondere

- das Recht auf den Erhalt von Informationen u.a. über die Identität des Verantwortlichen, Zweck der Verarbeitung und Empfänger der Daten[20];
- das Recht auf Auskunft über ihre verarbeiteten Daten[21] sowie auf Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung gegen die DSRL verstößt, insbesondere wenn die Daten unvollständig oder unrichtig sind[22] sowie
- das Recht, der Verarbeitung ihrer Daten zu widersprechen, wenn berechtigte Gründe vorliegen oder die Daten für Zwecke der Direktwerbung verarbeitet oder zu diesem Zweck an Dritte weitergegeben werden sollen.[23]

Übermittlungen personenbezogener Daten in ein Drittland sind nur zulässig, wenn in diesem laut Feststellung der Kommission ein angemessenes Schutzniveau besteht oder einer der in der Richtlinie geregelten Ausnahmetatbestände erfüllt ist.[24]

Die Mitgliedstaaten müssen schließlich gerichtliche Rechtsbehelfe für die Betroffenen bei der Verletzung ihrer Datenschutzrechte sowie bei rechtswidriger Datenverarbeitung ein Schadensersatzrecht vorsehen.[25] Ferner müssen sie unabhängige nationale Datenschutzaufsichtsbehörden einrichten, die die Einhaltung der Richtlinie überwachen.[26] Länderübergreifend wurde zudem die sogenannte „Art. 29-Datenschutzgruppe“ als unabhängiges Gremium mit beratender Funktion eingesetzt.[27]

2.1.2 Anwendungsbereich

Die DSRL findet Anwendung, wenn personenbezogene Daten – egal, ob durch Behörden oder Private – automatisch (z.B. in Datenbanken) oder in herkömmlichen papiergestützten Dateien verarbeitet werden. Sie gilt jedoch nicht, wenn die Daten ausschließlich zu persönlichen oder familiären Zwecken oder im Bereich der öffentlichen Sicherheit, der Landesverteidigung oder der Staatssicherheit verarbeitet werden.

Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Eine Person gilt als bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, beispielsweise über eine ihr zugeordnete Kennnummer. Bei der Entscheidung, ob eine Person bestimmbar ist, müssen alle Mittel berücksichtigt werden, die von dem für die Datenverarbeitung Verantwortlichen oder einem Dritten vernünftigerweise eingesetzt werden können, um die betreffende Person zu bestimmen.[28]

---

19 Art. 18 ff. DSRL.
20 Art. 10 und 11 DSRL.
21 Art. 12 lit. a) DSRL.
22 Art. 12 lit. b) und c) DSRL.
23 Art. 14 DSRL.
24 Art. 25 und 26 DSRL.
25 Art. 22, 23 DSRL.
26 Art. 28 DSRL.
27 Art. 29 DSRL.
28 Erwägungsgrund 26 DSRL.

2.1.3 Ausnahmen und Einschränkungen

Die Mitgliedstaaten dürfen die Datenschutzgrundsätze und bestimmte Rechte betroffener Personen einschränken, wenn dies z.B. für

- die Sicherheit des Staates,
- die Landesverteidigung,
- die öffentliche Sicherheit,
- die Verhütung oder Verfolgung von Straftaten,
- ein „wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union“ oder für
- „den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen“ notwendig ist.[29]

2.1.4 Geltung und Umsetzung

Die DSRL wurde in Deutschland maßgeblich im Bundesdatenschutzgesetz (BDSG) sowie in den Landesdatenschutzgesetzen umgesetzt. Sie gilt noch bis einschließlich 24.05.2018 und wird danach durch die neue EU-Datenschutzgrundverordnung[30] abgelöst.

2.2 EU-Datenschutzgrundverordnung [(EU) 2016/679]

2.2.1 EU-Datenschutzreform

Im Juni 2016 ist nach mehr als vier Jahren zäher Verhandlungen die EU-Datenschutzgrundverordnung[31] (nachfolgend: „DSGVO“) in Kraft getreten. Hintergrund der Datenschutzreform war die Tatsache, dass die unterschiedliche Umsetzung und Anwendung der DSRL in den Mitgliedstaaten zu unterschiedlichen Schutzstandards geführt hat. Durch den Wechsel von der Richtlinie zur Verordnung wollte der europäische Gesetzgeber zudem die bestehende Rechtsunsicherheit bei der Anwendung der Datenschutzregelungen auf neue Medien sowie Hemmnisse für den freien Datenverkehr und damit Wettbewerbsverzerrungen auf dem Binnenmarkt verringern.[32]

2.2.2 Wesentliche Regelungsinhalte der DSGVO

Die DSGVO baut in weiten Teilen auf Terminologie und Systematik der DSRL auf und entwickelt diese weiter.[33] Wie die DSRL gilt sie für die Verarbeitung personenbezogener Daten durch Verantwortliche und Auftragsverarbeiter. „Verantwortlicher“ ist wie schon unter der DSRL jede Stelle, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.[34] „Auftragsverarbeiter“ ist jede Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.[35]

---

29 Vgl. Art. 13 DSRL.
30 Hierzu sogleich Kapitel 2.2.
31 Vgl. Fn. 6.
32 Vgl. Erwägungsgrund 8 sowie Art. 1 der DSGVO.
33 Schantz, NJW 2016, S. 1841.
34 Art. 4 Nr. 7 DSGVO.
35 Art. 4 Nr. 8 DSGVO.

„Personenbezogene Daten“ sind wie unter der DSRL alle Informationen, die sich auf eine „identifizierte oder identifizierbare“ natürliche Person beziehen. Es genügt, dass diese Person direkt oder indirekt mittels Zuordnung zu einer Kennung (Name, Kennnummer, Standortdaten, Online-Kennung, z.B. IP-Adresse) oder zu näher bestimmten Persönlichkeitsmerkmalen identifiziert werden kann.[36] Um festzustellen, ob eine Person identifizierbar ist, müssen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person wahrscheinlich genutzt werden, um die natürliche Person zu identifizieren. Dabei sind alle objektiven Faktoren wie Zeitaufwand und Kosten einer solchen Identifizierung heranzuziehen.[37] Des Weiteren sind sowohl aktuell verfügbare Technologien als auch – neu – künftige technologische Entwicklungen zu berücksichtigen.[38] Personenbezogen sind auch pseudonymisierte Daten, die durch Heranziehung zusätzlicher Informationen, die getrennt aufbewahrt werden, noch einer spezifischen Person zugeordnet werden können.[39] Bei der Pseudonymisierung von Daten wird i.d.R. der Name oder ein anderes Identifikationsmerkmale einer Person durch ein Pseudonym (i.d.R. eine Buchstaben- oder Zahlenkombination) ersetzt, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.[40] Weil die Informationen darüber, welche Identifikationsmerkmale durch welche Pseudonyme ersetzt wurden, aber noch getrennt aufbewahrt werden, kann – anders als bei anonymisierten Daten – die Verknüpfung mit dem echten Identifikationsmerkmal wieder hergestellt werden. In diesem Fall können die Daten folglich mit Hilfe dieser Zusatzinformationen wieder einer bestimmten Person zugeordnet werden. Sind die Daten hingegen „anonymisiert“, so dass kein Rückschluss auf die betroffene Person mehr möglich ist, fehlt es an der „Personenbezogenheit“ der Daten. Die Regelungen der DSGVO sind dann auf solche Daten nicht anwendbar.

Online-Kennungen wie IP-Adressen, Cookie-Kennungen, Funkfrequenzkennzeichnungen und sonstige Kennungen sind nicht für jedermann per se personenbezogen.[41] Sie können aber in Kombination mit Zusatzinformationen dazu führen, dass eine Person identifiziert werden kann.[42] Die DSGVO selbst regelt nicht konkret, wer die Möglichkeit zur Identifizierung der betroffenen Person haben muss. Sie gibt damit keine eindeutige Antwort auf die Frage, ob eine Identifizierbarkeit und damit ein „Personenbezug“ etwa nur dann anzunehmen ist, wenn der im konkreten Fall für die Datenverarbeitung Verantwortliche den Betroffenen (allein) identifizieren kann, oder ob es genügt, wenn irgendein Dritter oder beide gemeinsam dies können.

In diesem Zusammenhang hat der Europäische Gerichtshof im Oktober 2016 klargestellt, dass eine Person auch dann identifizierbar sein kann, wenn sich nicht alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden.[43] Es kann folglich ausreichen, dass die betreffende Person nur mit Hilfe Dritter bestimmt werden kann. So ist etwa die Identifizierung einer dynamischen IP-Adresse nur möglich, wenn diese Adresse mit Zusatzinformationen verknüpft wird, über die nicht der konkret für die Datenverarbeitung Verantwortliche selbst, sondern lediglich der Internetzugangsanbieter eines Nutzers verfügt.[44] Online-Kennungen wie die IP-Adresse sind – so der EuGH – für einen Verantwortlichen aber dann personenbezogen, wenn dieser rechtlich die Möglichkeit hat, diese Zusatzinformationen zu erhalten

---

36 Art. 4 Nr. 1 DSGVO.
37 Erwägungsgrund 26 DSGVO.
38 Erwägungsgrund 26 DSGVO.
39 Vgl. Art. 4 Nr. 5 und Erwägungsgrund 26 DSGVO.
40 § 3 Abs. 6 a des deutschen Bundesdatenschutzgesetzes (BDSG); vgl. auch Art. 29 Working Party Opinion 05/2014 on Anonymization Techniques vom 10.04.2014, 0829/14/EN, WP 216; S. 20; vgl. ferner https://www.bfdi.bund.de/bfdi_wiki/index.php/3_BDSG_Kommentar_Absatz_6a.
41 Schantz, NJW 2016, S.1841 (1843).
42 Erwägungsgrund 30 DSGVO.
43 EuGH, Urteil vom 19.10.2016, C-582/14 Breyer ./. BRD, Tz. 43.
44 EuGH, Urteil vom 19.10.2016, C-582/14 Breyer ./. BRD, Tz. 49.

bzw. die betreffende Person mit deren Hilfe zu bestimmen.[45] Dies kann sogar zu bejahen sein, wenn der Verantwortliche die Zusatzinformationen nicht direkt von einem Dritten einfordern darf, weil das nationale Recht diesem die direkte Übermittlung solcher Zusatzinformationen an den Verantwortlichen verbietet. Denn laut EuGH reicht es aus, wenn der Verantwortliche rechtlich die Möglichkeit hat, eine zuständige Behörde einzuschalten, um die nötigen Zusatzinformationen zu erlangen und die Strafverfolgung einzuleiten.[46] In diesem Fall ist eine dynamische IP-Adresse, die von einem Online-Diensteanbieter beim Zugriff einer Person auf dessen Website gespeichert wird, für diesen Anbieter ein personenbezogenes Datum. Ist die Identifizierung der betreffenden Person hingegen gesetzlich verboten oder praktisch nicht durchführbar, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, soll das Risiko einer Identifizierung *de facto* vernachlässigbar und ein Personenbezug zu verneinen sein.[47] In diesem Fall wären die Vorschriften der DSGVO auf die konkrete Datenverarbeitung nicht anwendbar.

2.2.2.1 Grundprinzipien des Datenschutzes

Die DSGVO schreibt die in der DSRL niedergelegten bewährten Grundprinzipien des Datenschutzes fort. Personenbezogene Daten müssen nach den folgenden Grundsätzen[48] verarbeitet werden:

(1) Rechtmäßigkeit, Treu und Glauben und Transparenz

Wie schon unter der DSRL ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie auf Basis einer zulässigen Rechtsgrundlage erfolgt.[49] Dies ist der Fall, wenn einer der in Art. 6 DSGVO normierten Erlaubnistatbestände erfüllt ist.[50] Die Rechtsgrundlage kann sich auch aus dem sonstigen Unionsrecht oder aus nationalem Recht ergeben, soweit die DSGVO darauf verweist.[51] Aufgrund des Verordnungscharakters gilt nun unmittelbar in allen Mitgliedstaaten, dass die Datenverarbeitung nach dem Grundsatz von Treu und Glauben erfolgen muss. Im Vergleich zur DSRL wurde zudem ausdrücklich und damit klarer geregelt, dass die Datenverarbeitung für den Betroffenen transparent (nachvollziehbar) sein muss.[52] Dieser muss über die Datenverarbeitung, insbesondere über deren Umfang und deren Zwecke, informiert werden. Alle Informationen und Mitteilungen hinsichtlich der Verarbeitung seiner Daten, auf die der Betroffene nach der DSGVO Anspruch hat, müssen leicht zugänglich und in klarer und verständlicher Sprache abgefasst sein.[53]

(2) Zweckbindung

Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nur zu Zwecken verarbeitet werden, die mit dem ursprünglichen Erhebungszweck vereinbar sind.[54] Bei der Prüfung, wann eine Verarbeitung mit dem ursprünglichen Erhebungszweck noch vereinbar und eine Zweckänderung damit erlaubt ist, sind alle relevanten Umstände – beispielsweise die Art der Daten und die Folgen der Verarbeitung – zu berücksichtigen.[55] Die Beschränkung auf konkrete Zwecke schränkt beispielsweise die Nutzbarkeit von Informationen für sogenannte Big-Data-Prozesse ein.

---

45 EuGH, Urteil vom 19.10.2016, C-582/14 Breyer ./. BRD, Tz. 49.
46 EuGH, Urteil vom 19.10.2016, C-582/14 Breyer ./. BRD, Tz. 47.
47 EuGH, Urteil vom 19.10.2016, C-582/14 Breyer ./. BRD, Tz. 46.
48 Vgl. Art. 5 DSGVO.
49 Art. 5 Abs. 1 lit. a) i.V.m. Art. 6 Abs. 1 DSGVO, Art. 8 Abs. 2 S. 1 der EU-Grundrechtecharta.
50 Es handelt sich folglich ebenfalls um ein Verbot mit Erlaubnisvorbehalt.
51 Vgl. Erwägungsgrund 40 der DSGVO.
52 Art. 5 Abs. 1 lit. a) DSGVO.
53 Vgl. Erwägungsgrund 40 S. 3 DSGVO.
54 Art. 5 Abs. 1 lit. b) DSGVO.
55 Art. 6 Abs. 4 DSGVO.

(3) Datenminimierung (Datenvermeidung, Datensparsamkeit)

Die Datenverarbeitung muss dem Zweck angemessen, für diesen erheblich und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.[56] Unter der DSRL[57] reicht es dagegen noch aus, wenn der Weiterverarbeitungszweck nicht über den ursprünglichen Erhebungszweck hinausgeht. Ausnahmen gelten für die Weiterverarbeitung zu bestimmten privilegierten Zwecken, bei Einwilligung des Betroffenen oder in gesetzlich festgelegten Fällen.[58]

(4) Richtigkeit

Daten müssen sachlich richtig und – soweit erforderlich – auf dem neuesten Stand sein. Daten, die im Hinblick auf ihre Verarbeitungszwecke unrichtig sind, müssen grundsätzlich unverzüglich gelöscht oder berichtigt werden.[59]

(5) Begrenzung der Speicherdauer

Gespeicherte Daten dürfen nur solange die Identifizierung des Betroffenen ermöglichen, wie dies für die Zwecke ihrer Verarbeitung erforderlich ist. Ist der Verarbeitungszweck erfüllt oder fällt er weg, müssen die Daten gelöscht werden. Ausnahmen gelten, wenn Daten zu bestimmten näher geregelten privilegierten Archiv- oder Forschungszwecken verarbeitet werden.[60]

(6) Integrität und Vertraulichkeit

Dieser nun ausdrücklich geregelte Grundsatz verpflichtet Verantwortliche und Auftragsverarbeiter dazu, die Integrität und Vertraulichkeit der von ihnen verarbeiteten Daten sicherzustellen. Sie müssen geeignete technische und organisatorische Maßnahmen ergreifen, um eine angemessene Sicherheit der Daten zu gewährleisten und diese insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, Zerstörung oder Schädigung zu schützen.[61]

(7) Rechenschaftspflicht des Verantwortlichen

Wie unter der DSRL hat der Verantwortliche für die Einhaltung der Datenschutzgrundsätze zu sorgen. Er muss diese aber nicht nur einhalten, sondern ihre Einhaltung künftig auch Dritten – insbesondere den Aufsichtsbehörden – gegenüber nachweisen können.[62] Die Nachweispflichten zwingen die Verantwortlichen zu umfassenden Dokumentationen. Verletzen sie die Nachweispflicht, drohen Bußgelder, Schadensersatzansprüche und weitere Nachteile.

Die DSGVO entwickelt die genannten Grundsätze auch weiter. So wird etwa das Prinzip der Datenvermeidung und Datensparsamkeit durch die neuen Anforderungen „Datenschutz durch Technikgestaltung“ (engl.: „Privacy by Design“)[63] und die Verpflichtung zur datenschutzfreundlichen Voreinstellung von Produkten („Privacy by Default“)[64] konkretisiert. Danach muss der Verantwortliche bei der Datenverarbeitung ausdrücklich geeignete technische und organisatorische Datenschutzmaßnahmen treffen, z.B. Daten pseudonymisieren oder anonymisieren oder anderweitig für die

56 Art. 5 Abs. 1 lit. c) DSGVO.
57 Art. 6 Abs. 1 lit. c) DSRL.
58 Art. 6 Abs. 1 lit. b) i.V.m. Art. 89 DSGVO.
59 Art. 5 Abs. 1 lit. d) DSGVO.
60 Art. 5 Abs. 1 lit. e) DSGVO.
61 Art. 5 Abs. 1 lit. f) DSGVO. Solche Maßnahmen waren allerdings bereits unter der DSRL erforderlich, vgl. Art. 17 DSRL.
62 Art. 5 Abs. 2 DSGVO. Vgl. auch Piltz, K&R 2016, S. 557 (564).
63 Art. 25 Abs. 1 DSGVO.
64 Art. 25 Abs. 2 DSGVO.

notwendigen Datenschutzgarantien sorgen.[65] Damit personenbezogene Daten nur im für den jeweiligen Zweck erforderlichen Umfang verarbeitet werden, muss er auch sicherstellen, dass die vom Betroffenen genutzten Verfahren oder Produkte standardmäßig entsprechend datenschutzfreundlich voreingestellt sind.[66] Es muss ausgeschlossen sein, dass allein aufgrund der Voreinstellungen eine unbestimmte Zahl von Personen Zugriff auf personenbezogene Daten einer Person erlangt, ohne dass diese Person überhaupt gehandelt hat.[67] In der Konsequenz sind daher bereits die Entwickler von IT-Produkten und -Verfahren gefordert, künftig schon bei der Entwicklung sicherzustellen, dass ihre Produkte den Datenschutzprinzipien wie etwa dem Grundsatz der Datenminimierung Rechnung tragen. Denn Daten, deren Verarbeitung für den angestrebten Zweck nicht notwendig ist, sollten überhaupt nicht erst erhoben werden. Unmittelbar verpflichtet werden die Entwickler selbst hierzu durch die DSGVO allerdings nicht.[68]

2.2.2.2 Erlaubnistatbestände für Datenverarbeitungen

Wie bereits unter der DSRL ist eine Datenverarbeitung unter der DSGVO nur rechtmäßig, wenn einer der in ihr geregelten Erlaubnistatbestände vorliegt. Die DSGVO sieht sechs Erlaubnistatbestände vor[69], von denen mindestens einer erfüllt sein muss:

(1) Der Betroffene hat eingewilligt[70];

(2) Der Betroffene hat einen Vertrag geschlossen und die Verarbeitung seiner Daten ist zu dessen Erfüllung erforderlich oder dazu, auf seine Anfrage hin vorvertragliche Maßnahmen durchzuführen[71];

(3) Der Verantwortliche unterliegt nach nationalem Recht oder nach EU-Recht einer rechtlichen Verpflichtung und die Datenverarbeitung ist zu deren Erfüllung erforderlich[72];

(4) Die Verarbeitung ist erforderlich, um lebenswichtige Interessen einer natürlichen Person zu schützen[73];

(5) Der Verantwortliche handelt (nach nationalem oder EU-Recht) im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt und die Verarbeitung ist zur Wahrnehmung seiner Aufgabe erforderlich[74];

(6) Der Betroffene oder ein Dritter hat ein berechtigtes Interesse, zu dessen Wahrung die Datenverarbeitung erforderlich ist, und dieses Interesse wird von demjenigen des Betroffenen oder dessen Grundrechten und Grundfreiheiten nicht überwogen[75]. Ausdrücklich erwähnt wird,

---

65 Art. 25 Abs. 1 DSGVO.
66 Art. 25 Abs. 2 S. 1, 2 DSGVO.
67 Art. 25 Abs. 1 S.3 DSGVO.
68 Vgl. Erwägungsgrund 78 DSGVO, der von einer „Ermutigung" der Hersteller spricht. Vgl. auch Schantz, NJW 2016, S. 1841 (1846) m.w. N.
69 Art. 6 Abs. 1 DSGVO.
70 Art. 6 Abs. 1 lit. a), Art. 4 Nr. 11 DSGVO.
71 Art. 6 Abs. 1 lit. b) DSGVO.
72 Art. 6 Abs. 1 lit. c) DSGVO. Dieser Erlaubnistatbestand kann von den Mitgliedstaaten konkretisiert werden, die hierfür weiterhin auch eigene Rechtsgrundlagen schaffen können, vgl. Art. 6 Abs. 2 und 3 DSGVO. Vgl. auch Piltz, K&R 2016, S. 557 (564).
73 Art. 6 Abs. 1 lit. d) DSGVO.
74 Art. 6 Abs. 1 lit. e) DSGVO. Auch dieser Erlaubnistatbestand kann von den Mitgliedstaaten konkretisiert werden, die hierfür weiterhin auch eigene Rechtsgrundlagen schaffen können, vgl. Art. 6 Abs. 2 und 3 DSGVO. Vgl. auch Piltz, K&R 2016, S. 557 (564).
75 Art. 6 Abs. 1 lit. f) DSGVO.

dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung einem berechtigten Interesse dienen kann.[76]

Die Definition der datenschutzrechtlichen Einwilligung wurde unter der DSGVO neu gefasst.[77] Insgesamt sind die Regelungen zur Einwilligung im Vergleich zur DSRL detaillierter. Die Einwilligung muss freiwillig, in Kenntnis der Sachlage[78], unmissverständlich und für einen konkreten Fall[79] erteilt werden und jederzeit widerrufbar[80] sein.

Neu geregelt wurde, dass bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, wesentlich zu berücksichtigen ist, ob die Erfüllung eines Vertrags von der Einwilligung in eine Verarbeitung von Daten abhängt, die für die Erfüllung des Vertrags nicht erforderlich sind.[81] Mit anderen Worten gilt eine Einwilligung beispielsweise dann als nicht freiwillig erteilt, wenn ein Anbieter die Erfüllung eines Vertrags untrennbar an die Erteilung einer Einwilligung knüpft, obwohl diese Einwilligung für die Vertragserfüllung gar nicht erforderlich ist.[82] Die Erbringung einer Dienstleistung darf also künftig nicht mehr von der Erteilung der Einwilligung abhängig gemacht werden, wenn die Einwilligung für die Erbringung der Dienstleistung selbst nicht erforderlich ist (Kopplungsverbot). Ziel dieser Regelung dürfte es sein, großen Diensteanbietern wie Amazon, Google und Facebook, zu deren Diensten es keine wirklichen Alternativen gibt, die Durchsetzung ihrer Datenschutzbedingungen zu erschweren. Deren Nutzer sind gegenwärtig im Prinzip gezwungen, den Bedingungen zuzustimmen, um die Dienste nutzen zu können. Künftig dürften Großkonzerne damit ihre Dienste wohl nicht mehr von der Einwilligung in Datenschutzbedingungen abhängig machen, die weitreichendere Datennutzungen erlauben, als es die Inanspruchnahme ihrer Dienstleistungen erfordert. Der Betroffene soll eine echte oder freie Wahl haben und in der Lage sein, die Erfüllung zu verweigern oder zurückzuziehen, ohne Nachteile zu haben.[83] Zweifel an der Freiwilligkeit bestehen künftig ausdrücklich auch bei klarem Ungleichgewicht zwischen Verantwortlichem und Betroffenen.[84] Letztgenannter muss auch die Möglichkeit haben, in verschiedene Datenverarbeitungsvorgänge gesondert einwilligen zu können, wenn dies im Einzelfall angebracht ist. Komplexe Generaleinwilligungen, die der Betroffene nur als Ganzes akzeptieren kann, werden damit erschwert.[85]

Eine Einwilligung muss durch eine unmissverständliche Willensbekundung, also eine Erklärung oder eine sonstige eindeutig bestätigende Handlung erfolgen.[86] Eine solche kann zum Beispiel durch Anklicken eines Kästchens (Opt-in) oder durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft erfolgen.[87] Dagegen sollen Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person keine Einwilligung darstellen. [88] Damit dürften Opt-Out-Lösungen künftig ausgeschlossen sein.[89] Eine Einwilligung kann grundsätzlich auch durch

[76] Erwägungsgrund 47 DSGVO a. E.
[77] Vgl. die Definition der Einwilligung in Art. 4 Nr. 11 DSGVO.
[78] Erwägungsgrund 42 DSGVO.
[79] Vgl. Erwägungsgrund 32 DSGVO.
[80] Art. 7 Abs. 3 DSGVO.
[81] Art. 7 Abs. 4 DSGVO.
[82] Erwägungsgrund 43 der DSGVO.
[83] Erwägungsgrund 42 der DSGVO.
[84] Vgl. Erwägungsgrund 43 DSGVO.
[85] Schantz, NJW 2016, 1841 (1844).
[86] Art. 4 Nr. 11 i. V. m. Erwägungsgrund 32 DSGVO.
[87] Erwägungsgrund 32 S. 2 DSGVO.
[88] Erwägungsgrund 32 S. 3 DSGVO.
[89] Ebenso Schantz, NJW 2016, 1841 (1844).

entsprechende Einstellungen des Browsers erteilt werden; zweifelhaft ist jedoch, ob dies auch gilt, wenn der Browser schon werksseitig entsprechend voreingestellt ist.[90]

Künftig muss der Betroffene aufgrund der neu eingeführten Rechenschaftspflicht auch die Einwilligung des Betroffenen nachweisen können.[91] Vorformulierte Einwilligungserklärungen müssen transparent sein[92] und unterliegen künftig erstmals EU-weit einer Kontrolle nach der Klauselrichtlinie [93/13/EWG][93] – genauso wie allgemeine Geschäftsbedingungen und sonstige einseitig auferlegte Vertragsklauseln.[94] Auch datenschutzrechtliche Einwilligungserklärungen dürfen also keine missbräuchlichen Klauseln enthalten. Schließlich sieht die DSGVO Kinder erst ab einem Alter von 16 Jahren[95] als einwilligungsfähig an[96] – bisher war diese Frage im EU-Recht nicht geregelt. Anbieter von Internetdiensten, die sich direkt an Kinder wenden, dürfen Daten von jüngeren Kindern nur verarbeiten, wenn sie zuvor die Einwilligung der Eltern einholen.[97]

Die Verarbeitung besonders sensibler Daten, zu denen unter der DSGVO künftig auch genetische und biometrische Daten gehören, unterliegt wie schon bislang gesondert geregelten, strengeren Voraussetzungen.[98] Um eine Verarbeitung solch „besonderer Kategorien personenbezogener Daten" rechtfertigen zu können, muss eine Einwilligung künftig ausdrücklich erfolgt sein.[99] Allerdings können die Mitgliedstaaten die Einwilligung als Rechtfertigungsgrund für die Verarbeitung sensibler Daten ausschließen und hierdurch einen strengeren nationalen Schutzstandard schaffen.[100] Unabhängig davon können sie bei genetischen, biometrischen oder Gesundheitsdaten generell den Mindestschutzstandard der DSGVO erhöhen.[101]

2.2.2.3 Pflichten für Verantwortliche und Auftragsverarbeiter

(1) Pflicht zum Ergreifen von Maßnahmen zur Gewährleistung der Datensicherheit

Getreu dem nunmehr ausdrücklich geregelten Grundsatz der Datenintegrität und Vertraulichkeit[102] verpflichtet auch die DSGVO Verantwortliche und Auftragsverarbeiter dazu, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten.[103] Anders als die DSRL, die ebenfalls bereits bestimmte Datensicherheitsmaßnahmen vorschrieb[104], konkretisiert die DSGVO, was diese Sicherheitsmaßnahmen im Einzelnen beinhalten sollen. So sollen personenbezogene Daten pseudonymisiert und verschlüsselt werden.[105] Verantwortliche und Auftragsverarbeiter sollen in der Lage sein, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit ihrer Systeme und Dienste dauerhaft sicherzustellen und bei einem Zwischenfall die Verfügbarkeit der Daten und den Zugang zu ihnen rasch wieder-

90 Schantz, NJW 2016, 1841 (1844).
91 Art. 7 Abs. 1 DSGVO. Vgl. auch Piltz, K&R 2016, S. 557 (564).
92 Art. 7 Abs. 2 S. 1 DSGVO.
93 Richtlinie [93/13/EWG] des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen, letzte konsolidierte Fassung vgl. ABl. L 13 vom 12.12.2011, S. 1 ff.
94 Vgl. Erwägungsgrund 42 DSGVO.
95 Die Mitgliedstaaten dürfen die Altersgrenze für die Einwilligung auf maximal 13 Jahre senken, vgl. Art. 8 Abs. 2 DSGVO.
96 Art. 8 Abs. 1 S. 1 DSGVO.
97 Art. 8 Abs. 1 S. 2 DSGVO, zu all dem vgl. auch Schantz, NJW 2016, 1841 (1845).
98 Näher dazu Art. 9 DSGVO.
99 Art. 9 Abs. 2 lit. a) DSGVO.
100 Art. 9 Abs. 2 lit. a) DSGVO.
101 Art. 9 Abs. 4 DSGVO.
102 Art. 5 Abs. 1 lit. f) DSGVO. Vgl. oben Ziffer 2.2.2.1 unter (6).
103 Art. 32 i.V.m. Art. 5 Abs. 1 lit. f) DSGVO sowie oben Ziffer 2.2.2.1 unter (6).
104 Art. 16, 17 DSRL, vgl. oben Ziffer 2.1.1.
105 Art. 32 Abs. 1 lit. a) DSGVO.

herzustellen.[106] Ferner müssen sie Verfahren zur regelmäßigen Überprüfung ihrer Sicherheitsmaßnahmen entwickeln.[107]

(2) Informationspflichten bei der Datenerhebung

Die DSGVO sieht einen umfangreichen und gegenüber der DSRL[108] deutlich umfassenderen Katalog an Informationen vor, die der Verantwortliche dem Betroffenen bei der Datenerhebung zur Verfügung stellen muss.[109] Diese Informationspflichten sollen primär zu mehr Transparenz führen. Der Betroffene soll wissen, wer welche Daten über ihn auf welcher Grundlage und für welche Zwecke erhebt. Daher muss der Verantwortliche ihm in jedem Fall insbesondere seine Kontaktdaten sowie diejenigen seines Datenschutzbeauftragten, die geplanten Datenverarbeitungszwecke, die Datenempfänger und künftig – dies ist neu – auch die Rechtsgrundlage mitteilen, auf die er die Datenverarbeitung stützt.[110] Gleiches gilt für die etwaige Absicht, die Daten in ein Drittland zu übermitteln.[111] Wenn die Daten direkt beim Betroffenen erhoben werden, muss der Verantwortliche ggf. auch seine berechtigen Interessen nennen, falls er die Datenverarbeitung hierauf stützt.[112] Werden die Daten nicht beim Betroffenen erhoben, muss er zusätzlich angeben, welche Datenkategorien er verarbeitet.[113]

Erhebt der Verantwortliche die Informationen direkt beim Betroffenen, muss er diesem weitere Informationen geben, soweit dies für eine faire und transparente Datenverarbeitung „notwendig" ist.[114] Erfolgt die Datenerhebung nicht direkt beim Betroffenen, sind weitere Informationen bereits zu erteilen, wenn dies für eine faire und transparente Datenverarbeitung gegenüber dem Betroffenen „erforderlich"[115] ist. So muss er etwa die geplante Speicherdauer angeben und den Betroffenen auf seine Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Beschwerde und Datenübertragbarkeit hinweisen und ihm mitteilen, ob automatisierte Entscheidungen getroffen werden.[116] Erfolgt die Erhebung nicht beim Betroffenen, hat dieser ferner ein Recht zu erfahren, aus welcher Quelle die Daten stammen und welche Datenkategorien verarbeitet werden.[117]

Werden die Daten direkt beim Betroffenen erhoben, muss dieser ggf. auch informiert werden, ob und warum er verpflichtet ist, die Daten bereitzustellen und welche Folgen die Nichtbereitstellung hätte.[118] Beruht die Datenverarbeitung auf einer erteilten Einwilligung, so muss der Verantwortliche dies klarstellen und den Betroffenen darauf hinweisen, dass er die Einwilligung jederzeit widerrufen kann.[119] Alle Informationen müssen leicht zugänglich sein und in einer klaren und einfachen Sprache mitgeteilt werden.[120] Auch bei einer beabsichtigten Zweckänderung müssen entsprechende Informationen erteilt werden.[121] Von den Informationspflichten bei Direkterhebung gibt es

---

106 Art. 32 Abs. 1 lit. b), c) DSGVO.
107 Art. 32 Abs. 1 lit. d) DSGVO.
108 Vgl. Art. 10 DSRL.
109 Art. 13 Abs. 1 lit. a) - f) DSGVO. Vgl. auch Schantz, NJW 2016, 1841 (1845).
110 Art. 13 Abs. 1 lit. a) - c) und e) DSGVO.
111 Art. 13 Abs. 1 lit. f) DSGVO.
112 Art. 13 Abs. 1 lit. d) DSGVO.
113 Art. 14 Abs. 1 lit. d) DSGVO.
114 Art. 13 Abs. 2 DSGVO.
115 Art. 14 Abs. 2 DSGVO. Diese Änderung im Wortlaut ist neu; Art. 11 ECRL sah auch insoweit ein Notwendigkeitserfordernis vor.
116 Art. 13 Abs. 2 lit. a) - d) und f) DSGVO.
117 Art. 14 Abs. 1 lit. d) und f) DSGVO.
118 Art. 13 Abs. 2 lit. e) DSGVO.
119 Art. 13 Abs. 2 lit. c), 14 Abs. 2 lit. d) DSGVO.
120 Art. 12 Abs. 1 DSGVO.
121 Art. 13 Abs. 3 und 14 Abs. 4 DSGVO.

keine Ausnahmen, es darf nur dann darauf verzichtet werden, wenn der Betroffene bereits über die Informationen verfügt.[122] Bei indirekter Datenerhebung darf auch dann ausnahmsweise von der Informationserteilung abgesehen werden, wenn diese unmöglich oder unverhältnismäßig aufwendig wäre, die Daten ohnehin der Geheimhaltung unterliegen oder wenn Rechtsvorschriften die Datenerhebung ausdrücklich vorsehen.[123] Soweit Informationen durch Bildsymbole ausgedrückt werden können, kann die Kommission die Verantwortlichen künftig ggf. in delegierten Rechtsakten dazu verpflichten, standardisierte Bildsymbole („Icons") zu verwenden.[124]

(3) Meldepflichten bei Datenschutzverletzungen

Eine grundlegende Neuerung der DSGVO ist auch die Einführung der Pflicht, Betroffene und Aufsichtsbehörden über aufgetretene Datenschutzverletzungen zu informieren, die dazu führen können, dass Unbefugte Zugang zu den Daten erlangen. Unerheblich ist, ob eine solche Verletzung absichtlich oder unabsichtlich erfolgt,[125] zum Beispiel bei einem Hackerangriff oder bei versehentlichem Verlust eines Datenträgers, auf dem personenbezogene Daten gespeichert sind. Eine Meldung an die Aufsichtsbehörde muss binnen einer sehr kurzen Frist von 72 Stunden erfolgen, ansonsten muss die Verzögerung begründet werden.[126] Die Meldung ist ausnahmsweise dann nicht erforderlich, wenn der Verantwortliche nachweisen kann, dass trotz der Datenschutzverletzung kein Risiko für die Rechte und Freiheiten der Dateninhaber besteht.[127] Dies kann der Fall sein, wenn die Daten so verschlüsselt sind, dass eine Kenntnisnahme durch Dritte ausgeschlossen ist. Der Verantwortliche muss also stets eine Risikoabwägung durchführen. Auftragsverarbeiter müssen Verletzungen unverzüglich dem Verantwortlichen melden.[128] Auch die Nutzer sollen künftig besser über hoch risikoreiche Verletzungen ihrer Datenschutzrechte informiert werden.[129] Sie müssen allerdings dann nicht benachrichtigt werden, wenn die Daten verschlüsselt oder anders geschützt waren oder der Verantwortliche das Risiko anderweitig durch spätere Maßnahmen gemindert hat.[130] Erfordert die persönliche Benachrichtigung aller Betroffenen einen unverhältnismäßigen Aufwand, kann sie durch eine öffentliche Bekanntmachung ersetzt werden.[131] Kommen die Verantwortlichen oder Auftragsverarbeiter diesen Pflichten nicht nach, drohen Bußgelder in Höhe von bis zu 10 Millionen Euro und bei Unternehmen von bis zu 2% des gesamten weltweit erzielten Jahresumsatzes.[132]

(4) Dokumentationspflichten

Daneben treffen alle Verantwortlichen und künftig auch Auftragsverarbeiter mit mindestens 250 Mitarbeitern umfassende Dokumentationspflichten. So müssen Verantwortliche alle Verarbeitungstätigkeiten in einem Verzeichnis festhalten und dieses der Aufsichtsbehörde auf Anfrage zur Verfügung stellen.[133] Darin sind u.a. die Verarbeitungszwecke, die Kategorien der personenbezogenen Daten sowie von Betroffenen und Empfängern sowie die getroffenen Sicherheitsmaßnahmen zu dokumentieren. Künftig müssen auch Auftragsverarbeiter ein solches Verzeichnis führen

[122] Art. 13 Abs. 4 DSGVO.
[123] Art. 14 Abs. 5 DSGVO.
[124] Art. 12 Abs. 8 DSGVO. Siehe auch Schantz, NJW 2016, 1841 (1845).
[125] Art. 33 Abs. 1 i.V.m. Art. 4 Nr. 12 DSGVO.
[126] Art. 33 Abs. 1 S. 1, 2 DSGVO.
[127] Art. 33 Abs. 1 S. 1, 2. Hs. DSGVO.
[128] Art. 33 Abs. 2 DSGVO.
[129] Art. 34 Abs. 1 DSGVO.
[130] Art. 34 Abs. 3 lit. a), b) DSGVO.
[131] Art. 34 Abs. 3 lit. c) DSGVO.
[132] Art. 83 Abs. 4 DSGVO.
[133] Art. 30 Abs. 1, 4 DSGVO.

und insbesondere die Kategorien durchgeführter Verarbeitungen auflisten.[134] Ungeachtet dessen müssen Verantwortliche zahlreiche Informationen wie z.B. die Datenempfänger schon deshalb dokumentieren, um ihrer Rechenschaftspflicht bezüglich der Einhaltung der Datenschutzvorgaben nachkommen und Ansprüche des Betroffenen erfüllen zu können.

2.2.2.4 Rechte der Betroffenen

Aus den unter 2.2.2.3 dargestellten Pflichten der Verantwortlichen und Auftragsverarbeiter resultieren entsprechende korrespondierende Rechte der Betroffenen, insbesondere deren

(1) Recht auf transparente Information bei der Datenerhebung[135] und das

(2) Recht, über Datenpannen informiert zu werden.[136]

Daneben sieht die DSGVO weitere Rechte der Betroffenen vor. Dazu gehört zunächst das

(3) Recht auf Auskunft über die erhobenen Daten zu einem späteren Zeitpunkt.[137]

Parallel zu den erweiterten Informationspflichten bei der Datenerhebung wurde auch das Auskunftsrecht des Betroffenen ausgeweitet. Jeder Betroffene hat das Recht, in angemessenen Abständen[138] bei einem Verantwortlichen zu erfragen, ob dieser personenbezogene Daten verarbeitet, die ihn betreffen. Ist dies der Fall, hat er Anspruch zu erfahren, welche Kategorien von Daten zu welchen Zwecken und wie lange verarbeitet und an welche Empfänger die Daten weitergegeben wurden oder werden.[139] Der Betroffene hat das Recht, eine Kopie seiner verarbeiteten personenbezogenen Daten zu erhalten.[140] Ferner ist er berechtigt, Auskunft über seine Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Beschwerde sowie – wenn die Daten nicht direkt beim Betroffenen erhoben wurden – über deren Herkunft zu erhalten.

(4) Recht auf Berichtigung

Darüber hinaus kann der Betroffene vom Verantwortlichen die unverzügliche Berichtigung unrichtiger Daten verlangen.[141] Unvollständige Daten müssen – je nach Verarbeitungszweck – ggf. vervollständigt (ergänzt) werden.[142] Darüber hinaus hat der Betroffene ein

(5) Recht auf Löschung und auf „Vergessenwerden".

Danach hat der Betroffene Anspruch darauf, dass ihn betreffende personenbezogene Daten unverzüglich gelöscht werden[143],

- wenn diese für die Verarbeitungszwecke nicht mehr notwendig sind,
- wenn eine Rechtsgrundlage für die Verarbeitung fehlt, weil diese auf eine Einwilligung gestützt wurde, die der Betroffene widerrufen hat,

---

134 Art. 30 Abs. 2 DSGVO.
135 Art. 12 ff. DSGVO, vgl. auch oben Ziffer 2.2.2.3 (2) zur korrespondierenden Informationspflicht bei der Datenerhebung.
136 Art. 33f. DSGVO, vgl. auch oben Ziffer 2.2.2.3 (3) zur korrespondierenden Meldepflicht bei Datenschutzverletzungen.
137 Art. 5 i. V. m. Erwägungsgrund 63 DSGVO.
138 Vgl. Erwägungsgrund 63 DSGVO.
139 Art. 15 Abs. 1 DSGVO.
140 Art. 15 Abs. 3 DSGVO.
141 Art. 16 S. 1 DSGVO.
142 Art. 16 S. 2 DSGVO.
143 Art. 17 Abs. 1 lit. a)-f) DSGVO.

- wenn der Betroffene einer Verarbeitung seiner Daten zu Zwecken der Direktwerbung widersprochen hat[144],
- wenn der Betroffene ein sonstiges Widerspruchsrecht gegen die Verarbeitung ausgeübt hat und keine überwiegenden berechtigten Gründe des Verantwortlichen für die Verarbeitung vorliegen[145],
- wenn die Datenverarbeitung unrechtmäßig war;
- wenn der Verantwortliche rechtlich zur Löschung verpflichtet ist oder
- wenn es sich um Daten handelt, die Internetanbieter direkt bei Kindern erhoben haben.

Die DSGVO weitet das Löschungsrecht anknüpfend an die Rechtsprechung des Europäischen Gerichtshofs[146] zu einem „Recht auf Vergessenwerden" im Internet aus. Hat ein Verantwortlicher Daten öffentlich gemacht, zu deren Löschung er verpflichtet ist, muss er angemessene Maßnahmen treffen, um andere Verantwortliche darüber zu informieren, dass der Betroffene die Löschung aller Links zu diesen Daten oder etwaigen Kopien derselben verlangt.[147] Auch alle Empfänger, an die er die Daten gezielt übermittelt hat, muss er entsprechend informieren.[148]

(6) Weitere Rechte

Ferner kann der Betroffene unter bestimmten Voraussetzungen verlangen, dass der Verantwortliche die Verarbeitung seiner Daten vorübergehend einschränkt (z.B. sperrt).[149] Daneben kann er sich dagegen wehren, einer Entscheidung unterworfen zu werden, die ihm gegenüber rechtliche Wirkung entfaltet oder ihn sonst erheblich beeinträchtigt, obwohl sie ausschließlich auf einer automatisierten Verarbeitung beruht.[150] Zu einer solchen Verarbeitung gehört auch das sogenannte Profiling[151], bei dem z.B. Daten einer Person zu einem Profil zusammengeführt werden, um z.B. Aufschluss über ihre Zahlungsfähigkeit zu erhalten. Ausnahmen gelten u.a., wenn die Entscheidung durch geeignete Rechtsvorschriften erlaubt wird, zur Vertragserfüllung erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat.[152] In den beiden letztgenannten Fällen muss der Verantwortliche angemessene Maßnahmen treffen, um die Rechte, Freiheiten und Interessen der Betroffenen zu wahren.[153]

(7) Widerspruchsrecht gegen Datenverarbeitung, die auf berechtigte oder öffentliche Interessen gestützt wird oder in Ausübung öffentlicher Gewalt erfolgt

Stützt der Verantwortliche die Datenverarbeitung auf ein berechtigtes Interesse, kann der Betroffene dieser Datenverarbeitung aus persönlichen Gründen widersprechen.[154] Gleiches gilt, wenn der Verantwortliche im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt handelt. Der Verantwortliche darf die Daten des Betroffenen dann nur weiterverarbeiten, wenn er zwingende schutzwürdige Gründe nachweist, die die Interessen, Rechte und Freiheiten des Betroffenen über-

144 Art. 17 Abs. 1 lit. c) i.V.m. Art. 21 Abs. 2 DSGVO.
145 Art. 17 Abs. 1 lit. c) i.V.m. Art. 21 Abs. 1 DSGVO.
146 EuGH, Urteil vom 13.05.2014, Rechtssache C-131/12, Google Spain SL, Google Inc. ./. Agencia Española de Protección de Datos, dort insbesondere Tz. 96 ff, 99.
147 Schantz, NJW 2016, 1841 (1845).
148 Art. 19 Abs. 1 DSGVO.
149 Art. 18 DSGVO.
150 Art. 22 Abs. 1 DSGVO.
151 Art. 4 Nr. 4 DSGVO.
152 Art. 22 Abs. 2 DSGVO.
153 Art. 22 Abs. 3 DSGVO.
154 Art. 21 Abs. 1 DSGVO.

wiegen, oder dass er die Daten für die Geltendmachung von Rechtsansprüchen benötigt. Werden personenbezogene Daten zum Zwecke der Direktwerbung verarbeitet, kann der Betroffene dieser Verarbeitung jederzeit und uneingeschränkt widersprechen. Seine Daten dürfen dann nicht mehr für Direktwerbung verwendet werden.[155]

(8) Recht auf Datenübertragbarkeit (Portabilität)

Die DSGVO führt mit dem Recht auf Übertragbarkeit von personenbezogenen Daten[156], die ein Betroffener einem Verantwortlichen bereitgestellt hat, ein völlig neues Recht ein. Durch die Ermöglichung der Datenportabilität soll die Datensouveränität der Betroffenen gestärkt und die Mitnahme von Daten und damit ein Wechsel zu anderen Anbietern erleichtert werden. Insbesondere E-Mail-Konten oder Profile in sozialen Netzwerken, aber auch Bankkonten können so leichter zu Konkurrenten übertragen werden. Wann immer die Datenverarbeitung automatisiert oder auf der Grundlage einer Einwilligung oder einer vertraglichen Beziehung erfolgt, muss der Verantwortliche die Daten, die der Betroffene ihm bereitgestellt hat, auf dessen Anfrage in einem strukturierten, gängigen und maschinenlesbaren Format an den Betroffenen selbst oder – soweit gewünscht und technisch machbar – direkt an einen anderen Anbieter übermitteln.[157] Ein solches Recht besteht allerdings nicht, wenn die Verarbeitung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt.[158] Die Art. 29-Datenschutzgruppe hat Ende 2016 Leitlinien zur Interpretation des Rechts auf Datenübertragbarkeit veröffentlicht.[159] Darin gibt die Gruppe eine Hilfestellung zu Inhalten, Umfang, Format und Fristen der zu übermittelnden Daten und insbesondere nähere Hinweise dazu, was unter „bereitgestellten Daten" zu verstehen ist.

2.2.2.5 Sonstige wesentliche Neuerungen

(1) Datenschutz-Folgenabschätzung

Plant ein Verantwortlicher – insbesondere wenn er neue Technologien verwendet – eine bestimmte Datenverarbeitung, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss er künftig vorab eine Datenschutz-Folgenabschätzung durchführen.[160] Eine solche Folgenabschätzung muss insbesondere stets bei geplantem „Profiling", umfangreicher Verarbeitung sensibler Daten oder umfangreicher Videoüberwachung durchgeführt werden.[161] Kommt die Folgenabschätzung zu dem Ergebnis, dass die Verarbeitung ein hohes Datenschutzrisiko zur Folge hätte, muss der Verantwortliche die Aufsichtsbehörde konsultieren oder Maßnahmen zur Eindämmung des Risikos treffen.[162]

(2) Bestellung eines Datenschutzbeauftragten

Die DSGVO schreibt nunmehr erstmals auf EU-Ebene die aus Deutschland bekannte Praxis vor, dass Verantwortliche und Auftragsverarbeiter unter bestimmten Voraussetzungen einen internen Datenschutzbeauftragten bestellen müssen, der die Einhaltung der Datenschutzverpflichtungen überwacht, den Verantwortlichen bzw. Auftragsverarbeiter hierzu berät und mit der Aufsichtsbe-

155 Art. 21 Abs. 2, 3 DSGVO.
156 Art. 20 DSGVO.
157 Art. 20 Abs. 1, 2 DSGVO.
158 Art. 20 Abs. 3 DSGVO.
159 Art. 29 Datenschutzgruppe, WP 242, Guidelines on the right to data portability, 13.12.2016, abrufbar unter http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.
160 Art. 35f. DSGVO.
161 Vgl. Art. 35 Abs. 3 DSGVO.
162 Art. 36 Abs. 1 DSGVO.

hörde kommuniziert und kooperiert.[163] Diese Verpflichtung trifft vor allem öffentliche Stellen, aber auch bestimmte nichtöffentliche Stellen, deren Kerntätigkeit in der Durchführung von Datenverarbeitungsvorgängen besteht.

(3) Aufsicht, Überwachung, Kooperations- und Kohärenzverfahren, „One-Stop Shop"

Neue komplexe Kooperations- und Kohärenzmechanismen[164] sollen eine möglichst einheitliche Anwendung der DSGVO in den EU-Mitgliedstaaten gewährleisten und verhindern, dass sich in der EU sogenannte „Datenschutzoasen" herausbilden.[165] Wie schon unter der DSRL muss jeder Mitgliedstaat eine oder mehrere[166] unabhängige Aufsichtsbehörden einrichten, die dann für die Überwachung der Einhaltung der Verordnung im Hoheitsgebiet dieses Mitgliedstaats zuständig sind.[167] Die Stellung der Aufsichtsbehörden als unabhängige nationale Prüfungsinstanzen wird in der DSGVO gefestigt.[168] Zu den Aufgaben der Aufsichtsbehörden gehört es nicht nur, die Grundrechte und Grundfreiheiten der Betroffenen bei der Verarbeitung personenbezogener Daten zu schützen, sondern auch, den freien Verkehr personenbezogener Daten in der EU zu gewährleisten.[169] Im Einzelnen müssen die Aufsichtsbehörden etwa die Öffentlichkeit über Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten informieren[170] sowie Verantwortliche und Auftragsverarbeiter über ihre Pflichten nach der DSGVO aufklären.[171] Ferner müssen sie sich mit Beschwerden befassen[172] und die Anwendung der DSGVO notfalls durchsetzen – z.B. durch die Verhängung von Verboten oder Geldbußen.[173] Daneben haben die Aufsichtsbehörden zahlreiche weitere Aufgaben[174] und Befugnisse. Bei deren Erfüllung bzw. Ausübung müssen sie zur einheitlichen Anwendung der DSGVO nicht nur in ihrem Mitgliedstaat, sondern in der gesamten EU beitragen.[175] Um diese einheitliche Anwendung zu gewährleisten, müssen sie in Fällen grenzüberschreitender Datenverarbeitung[176] untereinander und mit der Kommission zusammenarbeiten.[177] Das geltende EU-Recht regelt keine detaillierten Pflichten zur Koordinierung oder Zusammenarbeit zwischen Aufsichtsbehörden bei grenzüberschreitender Datenverarbeitung.[178] Demgegenüber sieht die DSGVO ein eigenes und umfassendes Kapitel über die Zusammenarbeit der nationalen Aufsichtsbehörden sowie über ein Kohärenzverfahren vor, welches bei Nichteinigung eingeleitet

---

163 Art. 37 ff. DSGVO.
164 Art. 60 ff., Art. 63 ff. DSGVO.
165 Vgl. dazu Schantz, NJW 2016, S. 1841 (1847) sowie BfDI-Info 6 zur DSGVO, S. 18, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.html sowie
166 EU-Staaten, die mehrere Aufsichtsbehörden einrichten (wie z.B. die Bundesrepublik Deutschland aufgrund ihrer föderalen Struktur), müssen bestimmen, welche Aufsichtsbehörde die übrigen Behörden im Europäischen Datenschutzausschuss vertritt. Sie müssen auch auf nationaler Ebene ein Verfahren einführen, mit dem sichergestellt wird, dass die anderen Behörden die Regelungen der DSGVO für das Kohärenzverfahren einhalten. Vgl. hierzu Art. 51 Abs. 3 sowie Erwägungsgrund 119 der DSGVO. Vgl. auch Piltz, K&R 2016, S. 777 (781).
167 Art. 51 Abs. 1, Art. 55 Abs. 1 und Art. 57 Abs. 1 lit. a) DSGVO.
168 Piltz, K&R 2016, S. 777 (784).
169 Piltz, K&R 2016, S. 777 (781).
170 Art. 57 Abs. 1 lit. b) DSGVO.
171 Art. 57 Abs. 1 lit. d) DSGVO.
172 Art. 57 Abs. 1 lit. f) DSGVO.
173 Vgl. etwa Art. 58 Abs. 2 lit f), i) DSGVO. Daneben gibt es weitere Sanktionsmöglichkeiten, siehe Fn. 176.
174 Zu den weiteren Aufgaben und Befugnissen der Aufsichtsbehörden siehe Art. 57 Abs. 1 DSGVO (Aufgaben) bzw. Art. 58 DSGVO [Untersuchungs- und Abhilfebefugnisse (Sanktionen)]. Näher dazu Piltz, K&R 2016, S. 777 (783).
175 Piltz, K&R 2016, S. 777 (782).
176 Unter „grenzüberschreitender Verarbeitung" versteht die DSGVO gemäß Art. 4 Nr. 23 sowohl Fälle, in denen eine Datenverarbeitung im Rahmen der Tätigkeit von mindestens zwei Niederlassungen eines Verantwortlichen oder Auftragsverarbeiters in unterschiedlichen EU-Mitgliedstaaten erfolgt, als auch Datenverarbeitungen im Rahmen einer einzigen Niederlassung, die erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat haben kann.
177 Art. 51 Abs. 2 DSGVO.
178 Piltz, K&R 2017, S. 85 (85).

werden muss.[179] Zuständig ist in grenzüberschreitenden Fällen grundsätzlich die „federführende Aufsichtsbehörde". „Federführend" ist die Aufsichtsbehörde desjenigen Mitgliedstaats, in dem der Verantwortliche oder Auftragsverarbeiter seine einzige Niederlassung in der EU oder – bei mehreren Niederlassungen – seine Hauptniederlassung hat.[180] Die federführende Aufsichtsbehörde muss jedoch mit den anderen betroffenen Aufsichtsbehörden zusammenarbeiten[181] und kann diese um Amtshilfe ersuchen oder mit ihnen gemeinsame Maßnahmen durchführen.[182] Ziel ist es, zwischen den Behörden einen Konsens über die zu treffende Entscheidung zu erzielen und nach Möglichkeit einen gemeinsamen Beschluss zu fassen. Scheitert dies, muss die federführende Behörde das Kohärenzverfahren einleiten.[183] Dann ist der neu eingerichtete Europäische Datenschutzausschuss[184] befugt, einen verbindlichen Beschluss zur Streitbeilegung zwischen den Behörden zu erlassen.[185] Auf der Grundlage dieses Beschlusses trifft die federführende oder sonst zuständige Aufsichtsbehörde einen endgültigen Beschluss.[186] Ziel des Kohärenzverfahrens ist es, dass in Fällen grenzüberschreitender Datenverarbeitung, mit denen mehrere Aufsichtsbehörden befasst sind, nur ein einziger Beschluss gefasst wird.[187]

Für Unternehmen, die Niederlassungen in mehreren EU-Staaten haben und dort personenbezogene Daten verarbeiten, wird das Verfahren damit vereinfacht. Für sie ist künftig grundsätzlich nur noch eine Aufsichtsbehörde als zentraler Ansprechpartner zuständig, nämlich diejenige im Mitgliedstaat ihrer Hauptniederlassung (einheitliche Anlaufstelle oder sogenannter „One-Stop Shop").[188] Damit müssen sich Unternehmen bei grenzüberschreitenden Datenverarbeitungen grundsätzlich nicht mehr mit Datenschutzbehörden in verschiedenen Mitgliedstaaten auseinandersetzen.[189]

In Ausnahmefällen lokal beschränkter Datenverarbeitung ist anstelle der federführenden Aufsichtsbehörde die örtlich nähere Aufsichtsbehörde sachlich zuständig.[190] Sie muss jedoch die federführende Behörde über die Angelegenheit unterrichten, die sich dann ggf. mit dem Fall befassen kann.[191]

Die Regelungen zur Zuständigkeit der federführenden Behörde und zum Kohärenzverfahren gelten ausnahmsweise dann nicht, wenn personenbezogene Daten im öffentlichen Interesse oder zur Wahrnehmung einer öffentlichen Aufgabe verarbeitet werden. In diesem Fall ist stets die Aufsichtsbehörde in demjenigen Mitgliedstaat zuständig, indem sich die verarbeitende Stelle befindet.[192]

(4) Einrichtung eines Europäischen Datenschutzausschusses

Um die einheitliche Anwendung der DSGVO sicherzustellen, wurde zudem der Europäische Datenschutzausschuss (EDSA) als unabhängiges EU-Organ mit eigener Rechtspersönlichkeit neu einge-

179 Vgl. Kapitel VII (Art. 60 ff. DSGVO).
180 Art. 56 Abs. 1 DSGVO.
181 Art. 60 Abs. 1 DSGVO.
182 Art. 60 Abs. 2 DSGVO.
183 Art. 60 Abs. 4 DSGVO.
184 Vgl. dazu auch sogleich unter (4).
185 Art. 65 Abs. 1 DSGVO. Ebenso und näher zum Kohärenzverfahren Piltz, K&R 2017, S. 85 (86).
186 Art. 65 Abs. 6 DSGVO.
187 Piltz, K&R 2017, S. 85 (86).
188 Art. 56 Abs. 6 DSGVO.
189 Art. 56 Abs. 1 i.V.m. Art. 4 Nr. 23 DSGVO.
190 Art. 56 Abs. 2 i.V.m. Erwägungsgrund 127 S. 1 DSGVO. Näher dazu Piltz, K&R 2016, S. 777 (782).
191 Art. 56 Abs. 3 DSGVO. Näher hierzu Piltz, K&R 2016, S. 777 (782).
192 Art. 55 Abs. 2 sowie Erwägungsgrund 128 der DSGVO. Vgl. auch Piltz, K&R 2016, S. 777 (782).

richtet.[193] Dieser ersetzt die durch die DSRL eingesetzte Art. 29-Datenschutzgruppe, erhält jedoch mehr Befugnisse als diese.[194] Der EDSA setzt sich aus dem Leiter[195] einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern zusammen. Ein Vertreter der Europäischen Kommission ist ohne Stimmrecht zur Teilnahme berechtigt. Der EDSA erhält umfangreiche Befugnisse und Aufgaben. So soll er z.B. die Kommission in Datenschutzfragen beraten, Stellungnahmen abgeben sowie Leitlinien, Empfehlungen und Verfahren ausarbeiten.[196] Damit erhält der EDSA die Kompetenz zur inhaltlichen Interpretation der Datenschutzvorschriften der DSGVO. Wie vorstehend ausgeführt, hat der EDSA zudem ein verbindliches Letztentscheidungsrecht bei bestimmten Streitigkeiten zwischen mehreren betroffenen nationalen Aufsichtsbehörden.[197]

(5) Stärkung der Selbstregulierung

Die DSGVO stärkt ferner die Selbstregulierung durch Verhaltensregeln[198] und Zertifizierungen[199] durch die Aufsichtsbehörden oder andere unabhängige akkreditierte Stellen[200] und regelt für diese erstmals eine gesetzliche Grundlage.[201] Hält ein Verantwortlicher oder Auftragsverarbeiter bestimmte zuvor genehmigte Verhaltensregeln ein, können diese bei bestimmten Beurteilungen im Rahmen der Verordnung herangezogen werden und das Ergebnis positiv beeinflussen. Die Möglichkeit der Zertifizierung bestimmter Verarbeitungsvorgänge ist folglich ein wichtiges Instrument, um die Einhaltung der DSGVO bei diesen Verarbeitungsvorgängen nachzuweisen.[202]

(6) Haftung auch der Auftragsverarbeiter

Künftig haften nicht nur die Verantwortlichen bei einer Verletzung ihrer Pflichten nach der DSGVO, sondern auch die Auftragsverarbeiter, wenn diese ihren „speziell den Auftragsverarbeitern auferlegten Pflichten" nach der DSGVO nicht nachkommen oder sie Anweisungen des Verantwortlichen missachtet haben.[203] Die Haftung erstreckt sich auf alle Schäden, die einer Person durch diese Verletzung entstehen. Ausdrücklich sind nunmehr auch immaterielle Schäden ersatzpflichtig.

(7) Rechtsbehelfe und Verbandsklagen

Glaubt eine Person, dass die Verarbeitung ihrer personenbezogenen Daten gegen die DSGVO verstößt, kann sie bei einer Aufsichtsbehörde eine Beschwerde einlegen[204] oder gegen den Verantwortlichen oder Auftragsverarbeiter Klage – auch auf Schadensersatz – erheben.[205] Dabei kann sie sich immer an die Datenschutzbehörde ihres Mitgliedstaats wenden, egal, in welchem Mitgliedstaat der Verstoß begangen wurde. Einem Betroffenen muss auch gegen rechtsverbindliche Beschlüsse der Aufsichtsbehörden, die ihn betreffen, oder bei Untätigkeit der Behörden ein gerichtli-

193 Art. 68 sowie Erwägungsgrund 139 S. 1 DSGVO.
194 Näher dazu Piltz, K&R 2017, S. 85 (87).
195 Mitgliedstaaten wie Deutschland, in denen mehrere Aufsichtsbehörden für die Überwachung der Anwendung der DSGVO zuständig sind (in Deutschland die Bundesdatenschutzbeauftragte und die Landesdatenschutzbeauftragten), müssen einen gemeinsamen Vertreter für den EDSA benennen, vgl. Art. 68 Abs. 4 DSGVO.
196 Näheres zu den Aufgaben des EDSA vgl. Art. 70 DSGVO.
197 Art. 65 DSGVO. Vgl. bereits oben unter (3).
198 Art. 40, 41 DSGVO.
199 Art. 42, 43 DSGVO.
200 Näher zu den Zertifizierungsstellen Art. 43 DSGVO.
201 Schantz, NJW 2016, S. 1841 (1846).
202 Art. 42 Abs. 1 DSGVO.
203 Art. 82 Abs. 1 und 2 DSGVO.
204 Art. 77 Abs. 1 DSGVO.
205 Art. 79 Abs. 1 DSGVO.

cher Rechtsbehelf zur Verfügung stehen.[206] Neuerdings ermöglicht es die DSGVO EU-weit, dass sich die Betroffenen bei Beschwerden oder gerichtlichen Rechtsbehelfen von bestimmten Non-Profit-Organisationen wie Verbraucherverbänden vertreten lassen können. Diese müssen individuell mandatiert werden und dürfen dann im Namen der Betroffenen Rechtsbehelfe einlegen.[207] Solche Organisationen dürfen sogar Schadensersatzansprüche für den Betroffenen geltend machen, wenn das nationale Recht dies vorsieht.[208] Darüber hinaus werden die Mitgliedstaaten künftig ausdrücklich ermächtigt, ein Verbandsklagerecht vorzusehen oder beizubehalten. Sie dürfen regeln, dass die genannten Non-Profit-Organisationen bei Datenschutzverstößen auch unabhängig von einem Auftrag des Betroffenen eine eigene Beschwerde einlegen oder Klage erheben dürfen. Ein solches Verbandsklagerecht bzw. eine entsprechende Öffnungsklausel war in der DSRL bislang nicht ausdrücklich vorgesehen.[209] Die Geltendmachung von Schadensersatzansprüchen ohne Beauftragung wird dabei jedoch ausdrücklich ausgenommen.[210]

(8) Datentransfer in Drittländer

Wann Daten ins Ausland transferiert werden dürfen, ist künftig detaillierter als bisher geregelt. Entsprechend der bisherigen Rechtslage unter der DSRL gilt auch unter der DSGVO der allgemeine Grundsatz, dass bei jeder Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen die Bestimmungen über die internationale Datenübermittlung sowie die übrigen Regelungen der DSGVO eingehalten werden müssen.[211] Hierdurch soll sichergestellt werden, dass das Schutzniveau der DSGVO auch bei internationalen Datentransfers nicht unterschritten wird. Der Transfer personenbezogener Daten in ein Drittland ist weiterhin „ohne besondere Genehmigung" zulässig, wenn die Kommission nach Prüfung aller relevanten Umstände im Wege eines sogenannten „Angemessenheitsbeschlusses" festgestellt hat, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Datenschutzniveau bietet.[212] Bei der Prüfung der Angemessenheit des Schutzniveaus muss die Kommission künftig eine ganze Reihe nicht abschließender Prüfpunkte berücksichtigen.[213] Personenbezogene Daten dürfen auch in ein Drittland ohne angemessenes Datenschutzniveau übermittelt werden, wenn anderweitig hinreichende Garantien bestehen, die das unzureichende Schutzniveau in dem Drittstaat kompensieren.[214] Solche Garantien können sich unter anderem aus vertraglichen Vereinbarungen zwischen Datenexporteur und Datenimporteur (z.B. sogenannten Standarddatenschutzklauseln) oder verbindlichen unternehmensinternen Datenschutzregelungen („Binding Corporate Rules") ergeben, deren Anforderungen nunmehr detailliert geregelt sind.[215] Neu ist, dass geeignete Garantien künftig auch in genehmigten Verhaltensregeln oder Zertifizierungen bestehen können.[216] Auch wenn keine geeigneten Garantien vorliegen, kann eine Daten-

---

206 Art. 78 Abs. 1 und 2 DSGVO.
207 Art. 80 Abs. 1 DSGVO.
208 Piltz, K&R 2017, S. 85 (90).
209 In Deutschland wurde im Februar 2016 das Verbandsklagerecht nach § 2 Abs. 2 S. 1 Nr. 11 UKlG auf Datenschutzverstöße erweitert. Vgl. auch Schantz, NJW 2016, S. 1841 (1847) sowie Piltz, K&R 2017, S. 85 (90) m. w. N.
210 Vgl. Art. 80 Abs. 2 und Erwägungsgrund 142 DSGVO.
211 Art. 44 DSGVO.
212 Art. 45 Abs. 1 DSGVO. Jüngstes Beispiel hierfür ist der im Jahr 2016 erlassene Angemessenheitsbeschluss betreffend einer Datenübermittlung in die Vereinigten Staaten von Amerika, auch unter dem Namen „Privacy Shield" bekannt. Kritisch hierzu cepStudie „Privacy Shield – Kein ausreichender Datenschutz im unsicheren Hafen USA", abrufbar unter http://www.cep.eu/de/eu-themen/details/cep/privacy-shield-kein-ausreichender-datenschutz-im-unsicheren-hafen-usa.html.
213 Art. 45 Abs. 2 DSGVO.
214 Art. 46 DSGVO.
215 Art. 47 Abs. 1, 2 DSGVO.
216 Art. 46 Abs. 2 lit. e), f) DSGVO; vgl. auch oben Ziffer (4).

übermittlung unter bestimmten Voraussetzungen durch einen Ausnahmetatbestand[217] gerechtfertigt sein.[218] Datenübermittlungen in Drittstaaten sind nur aufgrund einer Rechtsgrundlage im Unionsrecht möglich. Entscheidungen ausländischer Behörden oder Gerichte, die Verantwortliche oder Auftragsverarbeiter zur Offenlegung oder Übermittlung personenbezogener Daten verpflichten, sind deshalb nur gültig und vollstreckbar, wenn sie auf ein Rechtshilfeabkommen oder eine andere internationale Übereinkunft gestützt werden.[219]

(9) Erhöhte Bußgelder

Im Interesse einer konsequenten Durchsetzung der DSGVO wurde die Möglichkeit, Sanktionen zu verhängen, EU-weit vereinheitlicht und erheblich verschärft.[220] Bei Verstößen gegen organisatorische Regelungen können künftig Bußgelder in Höhe von bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes verhängt werden. Bei Verstößen gegen Datenschutzgrundsätze, Betroffenenrechte, die Regelungen zur Rechtmäßigkeit der Datenverarbeitung oder bei Missachtung von Anweisungen einer Aufsichtsbehörde können die Bußgelder sogar 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes betragen.

2.2.3 Anwendungsbereich der DSGVO

2.2.3.1 Sachlicher Anwendungsbereich

Die DSGVO regelt die Verarbeitung von personenbezogenen Daten grundsätzlich umfassend im gesamten privaten und öffentlichen Bereich. Sie gilt jedoch nicht für die Verarbeitung personenbezogener Daten

- durch natürliche Personen ausschließlich zu persönlichen oder familiären Zwecken[221],
- durch die Mitgliedstaaten im Bereich der Gemeinsamen Außen- und Sicherheitspolitik (GASP)[222],
- im Rahmen von Tätigkeiten, die die nationale Sicherheit betreffen und anderen Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen[223], Art. 2 Abs. 2 lit. b) DSGVO,
- durch Polizei und Justiz zu Strafverfolgungszwecken[224] – hier gilt künftig die neue Richtlinie [(EU) 2016/680][225], sowie
- durch EU-Organe und Einrichtungen[226] – insoweit gilt die Verordnung [(EG) Nr. 45/2001], die durch eine neu gefasste Verordnung ersetzt werden soll.[227]

---

217 Diese Ausnahmetatbestände – z.B. das Vorliegen einer ausdrücklichen Einwilligung – sind in Art. 49 Abs. 1 DSGVO geregelt.
218 Näher zur Thematik des Datentransfers in Drittländer und insbesondere zur Rechtslage bei Datenübermittlungen in die USA siehe auch cepStudie „Privacy Shield": Kein ausreichender Datenschutz im unsicheren Hafen USA, April 2016, abrufbar unter http://www.cep.eu/eu-themen/details/cep/privacy-shield-kein-ausreichender-datenschutz-im-unsicheren-hafen-usa.html.
219 Art. 48 DSGVO. Vgl. auch Schantz, NJW 2016, S. 1841 (1846).
220 Siehe auch Schantz, NJW 2016, 1841 (1847).
221 Art. 2 Abs. 2 lit. c) DSGVO.
222 Art. 2 Abs. 2 lit. a) DSGVO.
223 Art. 2 Abs. 2 lit. b) DSGVO.
224 Art. 2 Abs. 2 lit. d) DSGVO.
225 Vgl. Fn. 7.
226 Art. 2 Abs. 3 DSGVO.
227 Vgl. unten Kapitel 3.2.

Darüber hinaus gilt die DSGVO nur subsidiär, soweit sie durch die E-Datenschutz-Richtlinie [2000/58/EG] verdrängt wird. Die DSGVO erlegt Personen bei der Verarbeitung von Daten im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der EU keine zusätzlichen Pflichten auf, soweit die E-Datenschutz-Richtlinie besondere Pflichten vorsieht, die dasselbe Ziel verfolgen.[228] Zugleich soll die DSGVO auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der E-Datenschutz-Richtlinie bestimmten Pflichten unterliegen, die dasselbe Ziel verfolgen.[229] Dies lässt sich so interpretieren, dass die E-Datenschutz-Richtlinie korrespondierenden Pflichten der DSGVO als lex specialis vorgeht.

2.2.3.2 Räumlicher Anwendungsbereich

2.2.3.2.1 Sitz in der EU

Wie schon die DSRL, gilt auch die DSGVO zunächst für alle Verantwortlichen oder Auftragsverarbeiter, die eine Niederlassung in der EU haben und im Rahmen der Tätigkeiten dieser Niederlassung personenbezogene Daten verarbeiten (Sitzlandprinzip).[230] Das gilt ausdrücklich auch dann, wenn die Verarbeitung der Daten selbst außerhalb der EU erfolgt.[231] Der Standort des Servers, auf dem die Daten gespeichert werden, ist damit künftig irrelevant.

2.2.3.2.2 EU als Marktort

Darüber hinaus gilt die DSGVO künftig auch über EU-Grenzen hinaus für Verantwortliche oder Auftragsverarbeiter, die keinen Sitz in der EU haben, ihre Waren oder Dienstleistungen aber in der EU anbieten und dabei Daten von Personen verarbeiten, die sich in der EU befinden.[232] Gleiches gilt, wenn die Datenverarbeitung durch außerhalb der EU niedergelassene Stellen dazu dient, das Verhalten von Betroffenen – auch deren Internetaktivitäten[233] – in der EU zu beobachten.[234] Die Einführung dieses sogenannten Marktortprinzips zählt zu den wichtigsten Neuerungen der DSGVO. Künftig kommt es nicht mehr in erster Linie auf den Sitzort des Verantwortlichen, sondern auch darauf an, wo sich der Betroffene aufhält, dessen Daten verarbeitet werden. Aus diesem Grund müssen Unternehmen aus Drittstaaten künftig einen Vertreter in der EU benennen, der als Anlaufstelle und Ansprechpartner für Betroffene und Aufsichtsbehörden fungiert. Durch die Ausweitung ihres Anwendungsbereichs auch auf außereuropäische Wirtschaftsunternehmen, die auf dem europäischen Markt tätig sind, schafft die DSGVO insoweit einheitliche Wettbewerbsbedingungen.

2.2.4 Ausnahmen und Einschränkungen

Ähnlich wie bereits unter der DSRL dürfen die Mitgliedstaaten bestimmte Rechte des Betroffenen auf Transparenz, Information, Auskunft, Berichtigung, Löschung, Vergessenwerden, Sperrung, Datenportabilität und Widerspruch sowie die Benachrichtigungspflicht des Betroffenen bei Datenpannen und die korrespondierenden Datenschutzgrundsätze gesetzlich einschränken. Voraussetzung ist jedoch, dass der Wesensgehalt der Grundrechte und Grundfreiheiten geachtet wird und

[228] Vgl. Art. 95 DSGVO.
[229] Vgl. Erwägungsgrund 173 DSGVO.
[230] Art. 3 Abs. 1 DSGVO.
[231] Art. 3 Abs. 1 letzter Hs. DSGVO.
[232] Art. 3 Abs. 2 lit. a) DSGVO.
[233] Vgl. Erwägungsgrund 24 DSGVO.
[234] Art. 3 Abs. 2 lit. b) DSGVO.

die Einschränkung in einer demokratischen Gesellschaft zu einem der in der DSGVO abschließend aufgelisteten Zwecke notwendig und verhältnismäßig ist. Zu diesen Zwecken zählen die nationale Sicherheit und Landesverteidigung, die öffentlichen Sicherheit, die Strafverfolgung oder der Schutz der Rechte und Freiheiten anderer Personen. [235]

2.2.5 Geltung und Umsetzung

Anders als die DSRL gilt die DSGVO unmittelbar in der gesamten EU, allerdings erst ab dem 25.05.2018. Ab diesem Datum werden dann EU-weit einheitliche hohe Datenschutzstandards gelten. Dem „Herauspicken" von Rosinen durch Wahl des Sitzes in dem EU-Mitgliedsstaat mit den niedrigsten Datenschutzanforderungen wird damit weithin ein Riegel vorgeschoben. Allerdings enthält die DSGVO zahlreiche Öffnungsklauseln, so dass noch gewisse Unterschiede zwischen den einzelnen nationalen Rechtsordnungen ent- oder fortbestehen werden.

Zwar bedürfen EU-Verordnungen grundsätzlich keiner Umsetzung ins nationale Recht; die Mitgliedstaaten dürfen – oder müssen – die Öffnungsklauseln jedoch rechtzeitig durch nationale Regelungen ausfüllen und ihre nationalen Datenschutzgesetze aufheben oder anpassen.

2.3 Richtlinie [(EU) 2016/680] (Datenschutzrichtlinie für Polizei und Justiz)

Für den Austausch und die sonstige Verarbeitung personenbezogener Daten durch nationale Polizei- und Strafverfolgungsbehörden in den EU-Mitgliedstaaten zu Zwecken der Strafverfolgung, Strafvollstreckung oder Gefahrenabwehr gelten die DSRL und die DSGVO nicht. Hierfür gilt vielmehr eine spezielle Richtlinie, nämlich die 2016 neu erlassene Richtlinie[(EU) 2016/680][236] (nachfolgend bezeichnet als „Datenschutzrichtlinie für Polizei und Justiz"). Diese trat am 5. Mai 2016 in Kraft und muss bis zum 6. Mai 2018 von den Mitgliedstaaten in nationales Recht umgesetzt werden. Die Richtlinie schafft erstmals EU-weite Mindeststandards[237] für die innerstaatliche Verarbeitung personenbezogener Daten durch Polizei- und Strafverfolgungsbehörden. Sie soll einerseits den Austausch personenbezogener Daten zwischen nationalen Polizei- und Justizbehörden in den EU-Mitgliedstaaten harmonisieren und verbessern[238] und andererseits die Daten von Opfern, Zeugen und möglichen Tätern bei der Verarbeitung durch solche Behörden umfassend schützen. Um Zeit und Geld zu sparen und die Effizienz der Verbrechensbekämpfung zu erhöhen, sollen Strafverfolgungsbehörden nicht länger je nach Ursprung der personenbezogenen Daten verschiedene Datenschutzregeln anwenden müssen.[239] Soweit Polizei- und Strafverfolgungsbehörden personenbezogene Daten zu anderen als den in der Richtlinie vorgesehenen Zwecken verarbeiten, findet jedoch die DSGVO Anwendung.[240]

Die neue Datenschutzrichtlinie für Polizei und Justiz orientiert sich erkennbar an der DSGVO. Ihre Definitionen[241] entsprechen weitgehend deren Begriffsbestimmungen. Die Richtlinie verlangt weitgehend die Einhaltung der gleichen Grundprinzipien des Datenschutzes, geht aber in gewis-

---

235 Vgl. Art. 23 DSGVO.

236 Richtlinie [(EU) 2016/680] des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 04.05.2016, S. 89ff.

237 Die Mitgliedstaaten dürfen strengere Bestimmungen zum Schutz der Betroffenen vorsehen, vgl. Art. 1 Abs. 3 der Richtlinie [(EU) 2016/680].

238 Vgl. Art. 1 Abs. 2 lit. b) Richtlinie [(EU) 2016/680].

239 Europäische Kommission, Pressemitteilung vom 14. April 2016, abrufbar unter http://europa.eu/rapid/press-release_STATEMENT-16-1403_de.htm.

240 Vgl. Erwägungsgrund 11 der Richtlinie [(EU) 2016/680].

241 Art. 3 Richtlinie [(EU) 2016/680].

sen Punkten nicht ganz so weit wie die DSGVO (z.B. hinsichtlich der Transparenz und der Zweckbindung).[242] Dafür finden sich neue Elemente wie die Rechenschaftspflicht des Verantwortlichen[243] sowie dessen Pflichten zur Bestellung eines Datenschutzbeauftragten[244] und zur Durchführung einer Datenschutz-Folgenabschätzung[245] auch in der Datenschutzrichtlinie für Polizei und Justiz wieder. Auch hier gelten künftig die Grundsätze „Privacy by Design" und „Privacy by Default".[246] Ebenso müssen Daten, die unrechtmäßig erhoben wurden, nicht mehr erforderlich oder unrichtig sind, gelöscht werden.[247] Gleichermaßen unterliegt der Verantwortliche ähnlichen Pflichten zum Ergreifen von Datensicherheitsmaßnahmen[248], zur Information des Betroffenen über die Datenerhebung[249] sowie zur Information der Aufsichtsbehörde und des Betroffenen bei Datenpannen.[250] Darüber hinaus ist der Betroffene zu informieren, wenn unrichtige Daten übermittelt wurden, die ihn betreffen.[251] Daraus resultieren entsprechende korrespondierende Rechte der Betroffenen insbesondere auf Information und Auskunft. Die Mitgliedstaaten können diese Rechte unter näher geregelten Voraussetzungen jedoch einschränken, um eine erfolgreiche Ermittlung und Strafverfolgung nicht zu gefährden.[252] Anders als die DSGVO unterscheidet die Richtlinie zwischen unterschiedlichen Kategorien betroffener Personen, beispielsweise Verdächtigen, Verurteilten, Opfern und Zeugen, weil deren Daten in unterschiedlichem Umfang schützenswert sind.[253] Zudem sollen die Mitgliedstaaten eine angemessene Qualität der personenbezogenen Daten gewährleisten und so weit wie möglich berücksichtigen, ob diese auf Fakten basieren oder auf persönlichen Einschätzungen beruhen.[254] Neben Rechtsbehelfen[255] regelt die Richtlinie schließlich umfassend die Datenübermittlung in Drittstaaten[256]. Ferner verpflichtet sie zur Schaffung unabhängiger Aufsichtsbehörden[257] und deren Kooperation[258] und überträgt bestimmte Aufgaben an den durch die DSGVO etablierten Europäischen Datenschutzausschuss.[259]

2.4 Verordnung [(EG) Nr. 45/2001] (Datenverarbeitung durch EU-Organe und -Einrichtungen)

Werden personenbezogene Daten natürlicher Personen durch die Organe und Einrichtungen der EU verarbeitet, gelten für den Schutz der Grundfreiheiten und Grundrechte dieser Personen ebenfalls separate Regeln, derzeit die Verordnung [(EG) Nr. 45/2001] für die Datenverarbeitung durch EU-Organe und -Einrichtungen.[260] Diese entspricht in Aufbau und Inhalt in weiten Teilen der DSRL. Danach müssen die EU-Organe bei der Verarbeitung personenbezogener Daten im Wesentlichen

242 Art. 4 Richtlinie [(EU) 2016/680], vgl. demgegenüber Art. 5 DSGVO.
243 Art. 4 Abs. 4 Richtlinie [(EU) 2016/680].
244 Art. 32 ff. Richtlinie [(EU) 2016/680].
245 Art. 27 Richtlinie [(EU) 2016/680].
246 Art. 20 Richtlinie [(EU) 2016/680].
247 Vgl. Art. 5 und 16 Richtlinie [(EU) 2016/680].
248 Art. 29 Richtlinie [(EU) 2016/680].
249 Art. 13 Richtlinie [(EU) 2016/680].
250 Art. 30 und 31 Richtlinie [(EU) 2016/680].
251 Art. 7 Richtlinie [(EU) 2016/680].
252 Art. 13 Abs. 3, 15 Richtlinie [(EU) 2016/680].
253 Vgl. Art. 6 Richtlinie [(EU) 2016/680].
254 Vgl. Art. 7 Richtlinie [(EU) 2016/680].
255 Art. 52 ff. Richtlinie [(EU) 2016/680].
256 Art. 35 ff. Richtlinie [(EU) 2016/680].
257 Art. 41 ff. Richtlinie [(EU) 2016/680].
258 Art. 50 ff. Richtlinie [(EU) 2016/680].
259 Art. 51 Richtlinie [(EU) 2016/680].
260 Verordnung [(EG) Nr. 45/2001] vom 18. Dezember 2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.01.2001, S. 1 ff.

die gleichen Grundsätze (u.a. Zweckbindung, Richtigkeit, Treu & Glauben, Speicherbegrenzung) und Verpflichtungen einhalten wie Verantwortliche, für die die DSRL gilt. Damit gehen entsprechende korrespondierende Rechte der Betroffenen einher wie unter der DSRL.

Gewisse Unterschiede ergeben sich, weil sich die Verordnung [(EG) Nr. 45/2001] anders als die DSGVO im Wesentlichen an Behörden mit spezifisch unionsrechtlichen Aufgaben richtet. So ist eine Verarbeitung unter dieser Verordnung hier u.a. dann rechtmäßig, wenn sie zur Wahrnehmung einer Aufgabe erfolgt, die aufgrund der EU-Verträge bzw. des Sekundärrechts erforderlich ist. Einen Erlaubnistatbestand der „berechtigten Interessen" gibt es für EU-Behörden hingegen nicht. Die Verordnung [(EG) Nr. 45/2001] verpflichtet jedes EU-Organ zur Ernennung eines Datenschutzbeauftragten. Darüber hinaus hat sie den Europäischen Datenschutzbeauftragten (EDSB) als unabhängige Behörde auf EU-Ebene etabliert. Zu den Aufgaben des EDSB gehört es, die Verarbeitung personenbezogener Daten durch die EU-Organen und Einrichtungen als Aufsichtsbehörde zu überwachen und die EU-Organe und Einrichtungen bei der Verarbeitung personenbezogener Daten zu beraten. Ferner arbeitet er mit anderen Kontrollstellen und Datenschutzgremien zusammen, um einen kohärenten Datenschutz sicherzustellen.[261]

Die Verordnung widmet sich schließlich in einem eigenen Kapitel[262] dem Schutz personenbezogener Daten und der Privatsphäre im Rahmen EU-interner Telekommunikationsnetze oder im Zusammenhang mit der Nutzung von Endgeräten, die unter Kontrolle eines EU-Organs oder einer EU-Einrichtung stehen. Damit enthält die Verordnung nicht nur allgemeine Datenschutzvorschriften, sondern zugleich „E-Datenschutz-Regeln" für EU-Organe.

Die Verordnung wurde durch die DSGVO weder aufgehoben noch geändert. Art. 98 DSGVO kündigte jedoch bereits an, dass die Kommission nach Inkrafttreten der DSGVO auch andere geltende EU-Rechtsakte zum Schutz personenbezogener Daten und insbesondere die Verordnung [(EG) Nr. 45/2001] überprüfen und ggf. ändern werde, um einen einheitlichen und kohärenten Datenschutz sicherzustellen. Die Kommission hat nun am 10.01.2017 einen Reformvorschlag vorgelegt, der weiter unten in Kapitel 3.2. kurz näher skizziert wird.[263]

2.5 Datenschutzrichtlinie [2002/58/EG] für elektronische Kommunikation („E-Datenschutz-Richtlinie")

2.5.1 Beschreibung der Richtlinie

Die Datenschutzrichtlinie für elektronische Kommunikation [2002/58/EG][264], nachfolgend „E-Datenschutz-Richtlinie" genannt), trat am 31.07.2002 in Kraft. Sie bezweckt einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten im elektronischen Kommunikationssektor und ergänzt insoweit die noch bis 2018 gültige DSRL, wenn personenbezogene Daten im Bereich der elektronischen Kommunikation verarbeitet werden.[265] Sie gilt neben der DSRL und soll insbesondere einen angemessenen Schutz des Rechts auf Privatsphäre und Vertraulichkeit, aber auch eine freie Zirkulation der Daten innerhalb der EU ermöglichen.[266] Zu diesem Zweck harmonisiert sie die

[261] Art. 41 Abs. 2 S. 2, Art. 46 der Verordnung [(EG) Nr.45/2001].
[262] Vgl. Kapitel IV (Art. 34 ff) der Verordnung [(EG) Nr. 45/2001].
[263] Näher zu diesem Reformvorschlag siehe unten Kapitel 3.2.
[264] Richtlinie [2002/58/EG] über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.07.2002, S. 37ff.; letzte konsolidierte Fassung abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02002L0058-20091219&qid=1479897187385&from=EN.
[265] Art. 1 Abs. 1, 2 E-Datenschutz-Richtlinie.
[266] Art. 1 Abs. 1 E-Datenschutz-Richtlinie.

von den Mitgliedstaaten erlassenen rechtlichen, ordnungspolitischen und technischen Bestimmungen zum Schutz personenbezogener Daten und der Privatsphäre. Anders als die DSRL, die nur personenbezogene Daten natürlicher Personen schützt, schützt die E-Datenschutz-Richtlinie auch die berechtigten Interessen juristischer Personen als Teilnehmer elektronischer Kommunikationen.[267]

2.5.2 Wesentliche Inhalte

Die E-Datenschutz-Richtlinie beinhaltet spezielle Vorschriften und Garantien zur Gewährleistung des Rechts auf Privatsphäre und Vertraulichkeit der Nutzer, wenn Informationen über öffentliche elektronische Kommunikationsdienste und ihre zugehörigen Netze ausgetauscht werden, z.B. über Mobil- und Festnetztelefonie oder per E-Mail. Dabei legt sie insbesondere Regeln fest, nach denen Anbieter elektronischer Kommunikationsdienste die sichere Verarbeitung personenbezogener Daten gewährleisten und die Nutzer bei Verletzung des Schutzes personenbezogener Daten benachrichtigen sollen. Darüber hinaus schützt sie die Nutzer vor Verletzungen ihrer Privatsphäre durch Cookies und andere Instrumente, die in ihren PC, Mobiltelefon oder andere Endgeräte eindringen. Ferner verbietet sie unerbetene Nachrichten (SPAM) zu Zwecken des Direktmarketings, die nur bei vorheriger Einwilligung der Nutzer („Opt-in") zulässig sind. Die Regelungen der Richtlinie gelten für alle Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen[268] wie etwa Telekommunikationsunternehmen und E-Mail-Diensteanbieter. Die wesentlichen Inhalte der E-Datenschutz-Richtlinie lassen sich nachfolgend wie folgt weiter präzisieren:

2.5.2.1 Anforderung an die Vertraulichkeit der Kommunikation

Die E-Datenschutz-Richtlinie verpflichtet die Mitgliedstaaten, die Vertraulichkeit aller Nachrichten und der entsprechenden Verkehrsdaten sicherzustellen, die über öffentliche Kommunikationsnetze und öffentlich zugängliche Kommunikationsdienste übertragen werden.[269] Insbesondere müssen sie jedwedes Mithören, Abhören, Speichern, sonstiges Abfangen oder Überwachen von Nachrichten und der damit verbundenen Verkehrsdaten ohne Einwilligung der Betroffenen verbieten. Ausnahmen gelten nur bei gesetzlicher Ermächtigung[270] oder für die rechtlich zulässige Aufzeichnung zu geschäftlichen Nachweiszwecken.[271]

2.5.2.2 Anforderungen an die Sicherheit der Datenverarbeitung

Um die Vertraulichkeit der elektronischen Kommunikation zu sichern, gehören zu den zahlreichen Verpflichtungen, die die E-Datenschutz-Richtlinie für Anbieter elektronischer Kommunikationsdienste vorsieht, zunächst besondere Anforderungen an die Sicherheit der Datenverarbeitung. Dienstleister, die öffentlich zugängliche elektronische Kommunikationsdienste in öffentlichen Kommunikationsnetzen anbieten, sind verpflichtet, geeignete Maßnahmen zu ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten, falls erforderlich gemeinsam mit dem Netzbetreiber. Das Sicherheitsniveau muss unter Berücksichtigung des Standes der Technik und der Kosten der Sicherheitsmaßnahmen im Hinblick auf die bestehenden Risiken angemessen sein.[272] Die Anbieter dürfen nur ermächtigten Personen Zugang zu personenbezogenen Daten gewähren und dies nur

[267] Art. 1 Abs. 2 i. V. m. Erwägungsgrund 8 der E-Datenschutz-Richtlinie.
[268] Art. 3 E-Datenschutz-Richtlinie.
[269] Art. 5 Abs. 1 E-Datenschutz-Richtlinie.
[270] Art. 5 Abs. 1 E-Datenschutz-Richtlinie.
[271] Art. 5 Abs. 2 E-Datenschutz-Richtlinie.
[272] Art. 4 Abs. 1 E-Datenschutz-Richtlinie.

zu rechtlich zulässigen Zwecken.[273] Ferner müssen sie die Daten vor Zerstörung, Verlust, Veränderung, Verarbeitung, Zugang oder Weitergabe schützen.[274] Um dies zu gewährleisten, müssen die Diensteanbieter ein Sicherheitskonzept für ihre Verarbeitung umsetzen.[275] Ferner müssen sie die Teilnehmer über alle besonderen Risiken der Verletzung der Netzsicherheit sowie über mögliche Abhilfen unterrichten, soweit sie selbst keine entsprechenden Maßnahmen treffen können.[276] Anbieter, die öffentlich zugängliche elektronische Kommunikationsdienste über das Internet anbieten (z.B. E-Mail-Dienste), müssen die Nutzer beispielsweise über mögliche Maßnahmen zum Schutz ihrer zu übertragenden Nachrichten informieren, z.B. über den Einsatz spezieller Software oder von Verschlüsselungstechniken.[277]

2.5.2.3 Mitteilung von Datenschutzverstößen

Kommt es dennoch zu einer Verletzung des Schutzes personenbezogener Daten, muss der Dienstleister unverzüglich die zuständige nationale Behörde und, wenn zu befürchten ist, dass die Daten oder die Privatsphäre einer Person beeinträchtigt werden, auch diese betroffene Person von der Verletzung benachrichtigen. Dies gilt nicht, wenn der Dienstleister die Daten verschlüsselt oder anderweitige technische Schutzmaßnahmen getroffen hatte, die einen unbefugten Zugang zu den Daten ausschließen. [278] Nähere Einzelheiten zu den Maßnahmen für die Benachrichtigung von Datenschutzverletzungen hat die Kommission in einer Durchführungsverordnung geregelt.[279]

2.5.2.4 Speicherdauer und Verarbeitung von Verkehrs- und Standortdaten

Die E-Datenschutz-Richtlinie schützt nicht nur die Vertraulichkeit von Kommunikationsinhalten, sondern auch von sogenannten „Verkehrsdaten“, die mit dieser Kommunikation zusammenhängen. Verkehrsdaten sind Daten, die von einem Anbieter elektronischer Kommunikationsdienste verarbeitet werden, um Nachrichten an ein elektronisches Kommunikationsnetz weiterzuleiten oder solche Vorgänge abzurechnen.[280] Zu ihnen gehören beispielsweise Informationen darüber, wer mit wem, wann und wie lange kommuniziert hat. Verkehrsdaten müssen gelöscht oder anonymisiert werden, sobald sie nicht länger für Kommunikations- oder Abrechnungszwecke erforderlich sind, es sei denn, der betreffende Nutzer hat eingewilligt, dass die Verkehrsdaten für einen anderen Zweck, z.B. für Marketing oder zur Bereitstellung von „Diensten mit Zusatznutzen“ verwendet werden dürfen.[281]

In digitalen Mobilfunknetzen werden auch sogenannte „Standortdaten“ verarbeitet, die Aufschluss über den geographischen Standort des Endgeräts eines Mobilfunknutzers geben, um die Nachrichtenübermittlung zu ermöglichen.[282] Soweit Standortdaten genauer sind, als es für die Nachrichtenübermittlung erforderlich wäre, spricht die Richtlinie von „anderen Standortdaten als Verkehrsdaten“. Betreiber digitaler Mobilfunknetze können solche genaueren Daten etwa für die Bereitstellung von sogenannten „Diensten mit Zusatznutzen“ verwenden, etwa für persönliche Verkehrsin-

---

273 Art. 4 Abs. 1a 1. Spiegelstrich E-Datenschutz-Richtlinie.
274 Art. 4 Abs. 1a 2. Spiegelstrich E-Datenschutz-Richtlinie.
275 Art. 4 Abs. 1 a 3. Spiegelstrich E-Datenschutz-Richtlinie.
276 Art. 4 Abs. 2 E-Datenschutz-Richtlinie.
277 Erwägungsgrund 20 E-Datenschutz-Richtlinie.
278 Art. 4 Abs. 3 E-Datenschutz-Richtlinie.
279 Verordnung [(EU) Nr. 611/2013] der Kommission über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie [2002/58/EG], ABl. L 173 vom 26.06.2013, S. 2 ff.
280 Art. 2 lit. b) E-Datenschutz-Richtlinie.
281 Art. 6 Abs. 1-4 E-Datenschutz-Richtlinie.
282 Vgl. Erwägungsgrund 35 der E-Datenschutz-Richtlinie.

formationen und Navigationshilfen für Fahrzeugführer[283], Wettervorhersagen-, Tarif- oder touristische Informationen. Auch diese Daten dürfen nur in anonymisierter Form oder mit Wissen und Einwilligung der Nutzer verarbeitet werden.[284] Dennoch darf die Verarbeitung von Verkehrsdaten und anderen Standortdaten nur durch besonders befugte Personen und nur im erforderlichen Umfang erfolgen.[285]

2.5.2.5 Cookies & Co.

Seit ihrer Novellierung im Jahr 2009 reglementiert die E-Datenschutz-Richtlinie zudem den Einsatz von „Cookies" und sonstiger Software, die bestimmte Handlungen eines Computernutzers überwachen und aufzeichnen. Sogenannte „Spyware", „Web-Bugs", „Hidden Identifiers" und ähnliche Instrumente können – häufig ohne Wissen des Nutzers – in dessen Endgerät (z.B. PC, Smartphone) eindringen, um Zugang zu Informationen zu erlangen oder die Nutzeraktivität zurückzuverfolgen. Sie können daher eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen.[286] Andererseits können sie aber auch – wie z.B. „Cookies" – legitime und nützliche Hilfsmittel sein, um die Wirksamkeit einer Webseitengestaltung oder Werbung zu untersuchen und die Identität der an einer Online-Transaktion beteiligten Nutzer zu überprüfen. Technisch gesehen sind „Cookies" von einem Web-Server erzeugte[287] Datensätze, die an den Web-Browser eines Nutzers gesendet und bei diesem in einer Cookie-Datei des lokalen Rechners (oder sonstigen Endgeräts, z.B. Smartphone, Tablet) abgelegt werden.[288] Cookies weisen jedem Nutzer eine bestimmte Identität zu, die i.d.R. aus Ziffern und Buchstaben besteht.[289] Sie dienen normalerweise dazu, Informationen über den Benutzer des Web-Browsers, z.B. über dessen Surf-Verhalten, zu sammeln, zu speichern und an einen Web-Server zu übermitteln. Verbindet sich der Browser erneut mit dem Cookie-setzenden Webserver, werden die lokalen Einträge mit dem Ziel an den Web-Server zurückgesendet, den Nutzer und dessen Einstellungen wiederzuerkennen. Beides geschieht in der Regel, ohne dass der Nutzer etwas davon merkt. Davon profitieren z.B. Anbieter, die Benutzerprofile anlegen und dem Web-Nutzer dann gezielt Angebote unterbreiten, die sie auf den bevorzugten Webseiten platzieren.[290] Daneben ermöglichen Cookies, dass ein Nutzer sich nicht bei jedem Besuch einer Webseite neu einloggen muss oder dass seine Einstellungen, Merklisten und Warenkörbe erhalten bleiben, da er wiedererkannt wird.[291]

Die E-Datenschutz-Richtlinie verbietet grundsätzlich das Setzen von Cookies, es sei denn, der Nutzer hat hierzu seine Einwilligung erteilt[292], nachdem er umfassend und insbesondere über die geplanten Verarbeitungszwecke der gesammelten Informationen informiert wurde. Die Einwilligung muss einer Einwilligung im Sinne der DSRL entsprechen.[293] Dabei geht es jedoch nicht nur um den Schutz personenbezogener Daten, sondern – darüber hinausgehend – um den Schutz vor Speicherung bzw. Zugriff auf alle im Endgerät gespeicherten „Informationen". Ohne Einwilligung ist ein

283 Vgl. Erwägungsgrund 35 der E-Datenschutz-Richtlinie.
284 Art. 9 Abs. 1 E-Datenschutz-Richtlinie.
285 Art. 6 Abs. 5, Art. 9 Abs. 3 E-Datenschutz-Richtlinie.
286 Vgl. Erwägungsgrund 24 der E-Datenschutz-Richtlinie.
287 Alternativ können Cookies von einem Skript (Java Skript) in der Webseite erzeugt werden, vgl. BVDW, Whitepaper: „Browsercookies und alternative Tracking-Technologien: Technische und datenschutzrechtliche Aspekte", September 2015, S. 5, abrufbar unter http://www.bvdw.org/presse/news/article/cookies-co-bvdw-whitepaper-beleuchtet-alternative-tracking-technologien.html.
288 Hoeren, Internetrecht, Stand Oktober 2016, S. 461 ff.
289 http://www.vis.bayern.de/daten_medien/datenschutz/cookies.htm.
290 Hoeren, Internetrecht, Stand Oktober 2016, S. 461 ff.
291 BVDW, Whitepaper: „Browsercookies und alternative Tracking-Technologien: Technische und datenschutzrechtliche Aspekte", a.a.O. (Fn. 287), S. 6.
292 Art. 5 Abs. 3 E-Datenschutz-Richtlinie.
293 Art. 2 lit. f) E-Datenschutz-Richtlinie.

Zugang zu diesen Informationen oder deren Speicherung ausnahmsweise erlaubt, wenn dies ausschließlich zur technischen Durchführung der Übertragung einer Nachricht[294] über ein elektronisches Kommunikationsnetz erfolgt. Gleiches gilt, wenn die Speicherung oder der Zugang „unbedingt erforderlich" sind, damit der Anbieter dem Nutzer oder Teilnehmer einen von diesem ausdrücklich gewünschten Dienst überhaupt zur Verfügung stellen kann.[295]

Unklar ist, inwieweit das formal strikte Verbot, Instrumente wie Cookies ohne Einwilligung zu nutzen, durch die Erwägungsgründe der E-Datenschutz-Richtlinie teilweise gelockert wird. Danach dürfen Instrumente wie Cookies verwendet werden, soweit sie einem rechtmäßigen Zweck dienen, etwa weil sie die Bereitstellung von Diensten der Informationsgesellschaft „erleichtern".[296] Als Voraussetzung wird hier angegeben, dass der Nutzer klar und genau darüber informiert wurde, dass und zu welchem Zweck bestimmte Informationen auf seinem Endgerät platziert werden, und dass er deren Speicherung in seinem Endgerät ablehnen oder in diese – auch für die Zukunft – einwilligen kann. Kann der Diensteanbieter sich auf einen rechtmäßigen Zweck berufen, darf er Cookies auch dann benutzen, wenn der Nutzer zwar nicht eingewilligt, die Nutzung der Cookies aber auch nicht abgelehnt hat, obwohl er informiert war und die Gelegenheit zu einem solchen „Opt-Out" hatte.

Werden Cookies zu einem „rechtmäßigen Zweck" eingesetzt, darf der Anbieter den Zugriff auf bestimmte Webseiteninhalte sogar von einer Einwilligung in die Verwendung von Cookies oder eines ähnlichen Instruments abhängig machen.[297] Laut den Erwägungsgründen der Änderungsrichtlinie[298] sollen Nutzer die Einwilligung auch über die Handhabung der entsprechenden Einstellungen ihres Browsers bzw. seiner „anderen Anwendung" (darunter dürften Mobilfunk-Applikationen – „Apps" -fallen) ausdrücken können, wenn dies „technisch durchführbar und wirksam" ist (z.B. durch Auswahl der Option „Cookies akzeptieren").

2.5.2.6 Schutz vor unerbetenen Nachrichten (SPAM) für Zwecke des Direktmarketings

Ein weiteres wichtiges Ziel der E-Datenschutz-Richtlinie ist es, die Nutzer vor ungewollten Werbeanrufen oder -nachrichten zu schützen, die mit Hilfe automatischer Anrufmaschinen ausgeführt oder per Fax oder elektronischer Post gesendet werden, ohne dass die Nutzer vorab ihre Einwilligung hierzu erteilt haben („Opt-in").[299] Unter „elektronischer Post" ist dabei jede Text-, Sprach-, Ton- oder Bildnachricht (einschließlich SMS und E-Mail) zu verstehen, die über ein öffentliches Kommunikationsnetz verschickt wird und im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.[300] Eine vorherige Einwilligung ist – ausnahmsweise und unter bestimmten Voraussetzungen – im Rahmen einer bestehenden Kundenbeziehung verzichtbar.[301] Bei bestimmten anderen Formen der Direktwerbung (z.B. persönlichen Werbe-Telefonanrufen, die nicht durch Maschinen erfolgen) stellt die E-Datenschutz-Richtlinie es den Mitgliedstaaten frei, Opt-in oder Opt-Out-Systeme vorzusehen.[302]

---

294 Eine Nachricht ist jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermittelt wird, vgl. Art. 2 lit. d) E-Datenschutz-Richtlinie.
295 Art. 5 Abs. 3 S. 2 E-Datenschutz-Richtlinie.
296 Vgl. Erwägungsgrund 25 der E-Datenschutz-Richtlinie.
297 Vgl. Erwägungsgrund 25 der E-Datenschutz-Richtlinie.
298 Vgl. Erwägungsgrund 66 der Änderungsrichtlinie [2009/136/EG] („Cookie"-Richtlinie), ABl. L 337 vom 18.12.2009, S. 11.
299 Vgl. Art. 13 E-Datenschutz-Richtlinie.
300 Art. 2 lit. h) E-Datenschutz-Richtlinie.
301 Art. 13 Abs. 3 sowie Erwägungsgrund 41 der E-Datenschutz-Richtlinie.
302 Siehe Erwägungsgrund 42 der E-Datenschutz-Richtlinie.

2.5.2.7 Sonstige Regelungen

Ferner räumt die E-Datenschutz-Richtlinie natürlichen Personen die Entscheidungsfreiheit darüber ein, ob und welche ihrer personenbezogenen Daten (z.B. Telefonnummern, E-Mail-Adressen, Postanschriften) in ein öffentliches Teilnehmerverzeichnis aufgenommen werden dürfen. Die Aufnahme von Daten ist nur mit vorheriger Einwilligung zulässig.[303] Die Mitgliedstaaten müssen aber auch entsprechende berechtigte Interessen juristischer Personen ausreichend schützen.[304]

Schließlich sieht die E-Datenschutz-Richtlinie unter bestimmten Bedingungen ein Recht von Anrufern und Angerufenen zur Unterdrückung der Anzeige ihrer Rufnummer sowie zur Abweisung von Anrufen vor, die von bestimmten angezeigten Rufnummern aus erfolgen.[305] Die Mitgliedstaaten müssen sicherstellen, dass die Rufnummernunterdrückung unter bestimmten Bedingungen ausgesetzt werden kann, um Notrufe bearbeiten oder belästigende Anrufe zurückverfolgen zu können.[306]

Darüber hinaus sind Teilnehmer berechtigt, Rechnungen ohne Einzelgebührennachweis zu erhalten[307] und die automatische Weiterschaltung von Anrufen auf ihr Endgerät abstellen zu lassen.[308]

2.5.3 Anwendungsbereich

Die E-Datenschutz-Richtlinie gilt, wenn bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der EU personenbezogene Daten verarbeitet werden.[309]

2.5.3.1 Elektronische Kommunikationsdienste

„Elektronische Kommunikationsdienste“ sind nach derzeit noch geltendem Rechtsstand Dienste, die gewöhnlich gegen Entgelt erbracht werden und ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Die E-Datenschutz-Richtlinie verweist insoweit auf die Definition der „elektronischen Kommunikationsdienste“ in der Rahmenrichtlinie für elektronische Kommunikation[310] (nachfolgend: „TK-Rahmenrichtlinie“), die kraft dieses Verweises auch für die E-Datenschutz-Richtlinie gilt.[311]

Zu den elektronischen Kommunikationsdiensten gehören ausdrücklich alle

- Telekommunikationsdienste (z.B. Festnetz- oder Mobiltelefondienste) sowie
- Übertragungsdienste in Rundfunknetzen, z.B. (digitale) Hörfunk- oder Fernsehdienste.

Ausdrücklich ausgenommen sind bislang jedoch

- Dienste, die Inhalte über elektronische Kommunikationsnetze anbieten (z.B. Youtube) oder redaktionell kontrollieren (z.B. Nachrichten-Webseiten) sowie alle

---

303 Art. 12 Abs. 1-3 E-Datenschutz-Richtlinie.
304 Art. 12 Abs. 4 E-Datenschutz-Richtlinie.
305 Art. 8 Abs. 1-6 E-Datenschutz-Richtlinie.
306 Art. 10 lit. a) und b) E-Datenschutz-Richtlinie.
307 Art. 7 Abs. 1 E-Datenschutz-Richtlinie.
308 Art. 11 E-Datenschutz-Richtlinie.
309 Art. 3 E-Datenschutz-Richtlinie.
310 Vgl. die Definition in Art. 2 lit. c) der Richtlinie [2002/21/EG] des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste („Rahmenrichtlinie“), ABl. L 108 vom 24.04.2002, S. 33.
311 Vgl. Art. 2 Abs. 1 E-Datenschutz-Richtlinie.

- „Dienste der Informationsgesellschaft" i.S.d. Richtlinie [(EU) 2015/1535][312], die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen.

Umstritten war bislang, ob die E-Datenschutz-Richtlinie auch für sogenannte „Over-the-Top-Dienste" (nachfolgend: „OTT-Dienste") gilt. Unter OTT-Diensten versteht man Inhalte, Dienste oder Applikationen, die einem Endnutzer über das öffentliche Internet zur Verfügung gestellt werden.[313] Die Bezeichnung „OTT" steht dabei nicht für eine bestimmte Art von Diensten, sondern für eine bestimmte Methode ihrer Erbringung, nämlich insbesondere deren Zurverfügungstellung über das öffentliche Internet.[314]

Nach der obigen Definition wären OTT-Dienste keine „elektronischen Kommunikationsdienste" und damit von der Anwendung der E-Datenschutz-Richtlinie ausgenommen, soweit es sich entweder um „Inhaltsdienste" oder um „Dienste der Informationsgesellschaft handelt, die nicht zumindest überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen". In diesem Zusammenhang ist es hilfreich zu wissen, dass OTT-Dienste im Einzelnen weiter in „OTT-Kommunikationsdienste" (auch bezeichnet als „OTT-I-Dienste") und „OTT-Inhaltsdienste" (sogenannte „OTT-II-Dienste") unterteilt werden.[315]

OTT-Inhaltsdienste werden durch ein inhaltliches Element unterschiedlichster Art geprägt und reichen von Suchmaschinendiensten wie Google, Bing oder Yahoo über Streaming- und Video-on-Demand-Dienste oder -plattformen wie Youtube, iTunes, Netflix, Amazon Instant Video bis hin zu Informationsportalen (z.B. Wikipedia), Homepages von Zeitungen oder Mediatheken von Fernsehsendern.[316] Diese Dienste stellen eher eine Ergänzung zu den klassischen Telekommunikationsdiensten dar, dürften als Inhaltsdienste jedoch von der Anwendung der E-Datenschutz-Richtlinie ausgenommen sein.

Reine OTT-Kommunikationsdienste weisen hingegen kein inhaltliches Angebot auf, sondern ermöglichen Individual- und Gruppenkommunikation in Form von Sprache, Bildern, Videos und sonstigen Daten unter Einsatz des „Internet Protocol" (IP).[317]

Zu den OTT-Kommunikationsdiensten gehören u.a.

- (Web-)Maildienste wie z.B. GMX, Web.de, Gmail, Hotmail;
- Sofortnachrichtendienste (Instant-Messaging-Dienste), z.B. WhatsApp, Skype, iMessage, Instagram oder Snapchat;
- Internettelefoniedienste (VoIP) bzw. Videotelefoniedienste wie z.B. Skype, Viber, WhatsApp oder FaceTime Calls.[318]

---

[312] Richtlinie [(EU) 2015/1535] des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. L 241 vom 17.09.2015, S. 1 ff.

[313] BEREC Report on OTT Services, Februar 2016, S. 3, abrufbar unter: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services.

[314] BEREC Report on OTT Services, Februar 2016, a.a.O. (Fn. 313), S. 3.

[315] Stellungnahme des Wissenschaftlichen Arbeitskreises für Regulierungsfragen (WAR) bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen Fragen der Regulierung von OTT-Kommunikationsdiensten vom 15.07.2016, S. 3. abrufbar unter: https://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/WAR/Stellungnahmen/Stellungnahme_OTT.pdf?__blob=publicationFile&v=2

[316] Stellungnahme des WAR bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Fragen der Regulierung von OTT-Kommunikationsdiensten, a.a.O. (Fn. 315), S. 4.

[317] Stellungnahme des WAR bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Fragen der Regulierung von OTT-Kommunikationsdiensten, a.a.O. (Fn. 315), S. 4.

OTT-Kommunikationsdienste gewinnen zunehmend an Bedeutung und drängen die herkömmliche Kontaktaufnahme über klassische elektronische Kommunikationsdienste immer mehr in den Hintergrund. Diese Dienste stehen daher in einer Konkurrenzbeziehung zu den klassischen Telekommunikationsdiensten wie SMS oder Sprachtelefonie. Allerdings ist die Unterscheidung zwischen Kommunikations- und Inhaltsdiensten zum Teil schwierig, weil ein und dieselbe Plattform oft ein Bündel von integrierten Diensten anbietet (z.B. bei sozialen Kommunikationsnetzen wie Facebook oder Twitter).[319]

Ob OTT-Kommunikationsdienste der E-Datenschutz-Richtlinie unterfallen, hängt maßgeblich von der Kernfrage ab, ob diese Dienstleistungen zumindest überwiegend die Übertragung von Signalen über ein öffentliches Kommunikationsnetz zum Gegenstand haben. Dagegen spricht, dass die Signalübertragung bei OTT-Diensten über das „offene Internet" erfolgt und nicht durch die OTT-Diensteanbieter selbst vorgenommen wird.[320] Der EuGH hat noch nicht darüber entschieden, ob OTT-I-Dienste Telekommunikations- bzw. elektronische Kommunikationsdienste darstellen. Er hat in einer Entscheidung aus dem Jahr 2014 lediglich festgestellt, dass ein Dienst auch dann als elektronischer Kommunikationsdienst einzuordnen sein kann, wenn die Übertragung des Signals über die Infrastruktur eines Dritten erfolgt. Es komme allein darauf an, ob der Anbieter gegenüber den Endnutzern für die Übertragung des Signals verantwortlich sei.[321] Unklar ist, was der EuGH mit „Verantwortlichkeit" meint. Hielte man eine volle Kontrolle bzw. zivilrechtliche Verantwortlichkeit des Diensteanbieters für die Signalübertragung gegenüber dem Endkunden für erforderlich, müsste man das Vorliegen eines Kommunikationsdienstes und damit eine Anwendbarkeit der E-Datenschutz-Richtlinie wohl ablehnen. Unter Bezugnahme auf das genannte EuGH-Urteil hat das VG Köln im November 2015 den Webmail-Dienst GMail von Google als Kommunikationsdienst eingeordnet, der eine überwiegende Signalübertragung zum Gegenstand hat. Der Begriff der „Verantwortlichkeit" sei weit zu fassen. Es reiche aus, dass der Anbieter sich die Signalübertragung durch Dritte (Internet-Provider) zurechnen lassen muss, ein zivilrechtliche Verantwortlichkeit sei nicht erforderlich.[322] Auch die deutsche Bundesnetzagentur hat betont, dass bei einer funktionalen und teleologischen Betrachtung insbesondere bei OTT-Instant-Messaging-Diensten Argumente für eine Signalübertragung sprächen. Die Frage müsse aber letztlich der EuGH entscheiden.[323] Die Kommission hingegen ist der Ansicht, dass sogenannte OTT-Dienste der Richtlinie derzeit nicht unterfallen.[324]

---

318 Stellungnahme des WAR bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Fragen der Regulierung von OTT-Kommunikationsdiensten, a.a.O. (Fn. 315), S. 3.

319 Stellungnahme des WAR bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Fragen der Regulierung von OTT-Kommunikationsdiensten, a.a.O. (Fn. 315), S. 1, 4.

320 Näher hierzu Wissenschaftlicher Arbeitskreis für Regulierungsfragen (WAR) bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Evolution der Regulierung in den Telekommunikations -und Mediensektoren angesichts der Relevanzzunahme von OTT-Anbietern vom 18.11.2015, S. 5, abrufbar unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/WAR/WAR_OTT.pdf;jsessionid=6152964626A73E7F1583E72086B9F14D?__blob=publicationFile&v=1.

321 EuGH, Urteil vom 30.04.2014, Rs. C-475/12 UPC DTH Sàrl ./. NMHH, Tz. 43ff., abrufbar unter: http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d0f130d69b73dda494c943e3999f9b5d8bce6b79.e34KaxiLc3eQc40LaxqMbN4PahmLe0?doclang=DE&text=&pageIndex=0&part=1&mode=DOC&docid=151525&occ=first&dir=&cid=751231.

322 VG Köln, Urteil vom 11.November 2015, AZ 21 K 450/15, Tz. 56 ff., abrufbar unter https://openjur.de/u/866817.html.

323 Stellungnahme des WAR bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Evolution der Regulierung in den Telekommunikations -und Mediensektoren angesichts der Relevanzzunahme von OTT-Anbietern, a.a.O., S. 5.

324 Vgl. etwa https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-communications-and-challenge-new-technologies-are. Die Erweiterung des Anwendungsbereichs auf solche Dienste war einer der Beweggründe für die Überarbeitung dieser Richtlinie, vgl. näher unten Ziffer 2.5.6 sowie Kapitel 3.1.

2.5.3.2 Öffentliche Zugänglichkeit der elektronischen Kommunikationsdienste

Die Kommunikationsdienste müssen darüber hinaus „öffentlich zugänglich", d.h. der Öffentlichkeit zur Verfügung gestellt[325] worden sein.[326] Hieran fehlt es etwa bei Mail-Diensten über einen unternehmensinternen Mail-Server.

2.5.3.3 In öffentlichen Kommunikationsnetzen

Schließlich muss der elektronische Kommunikationsdienst, in dessen Zusammenhang die Datenverarbeitung erfolgt, über ein „öffentliches Kommunikationsnetz" bereitgestellt werden.[327] Ein elektronisches Kommunikationsnetz ist öffentlich, wenn es ganz oder überwiegend der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten (das sind Zugangspunkte für einen Teilnehmer bzw. Endnutzer) ermöglichen. Beispiele für öffentliche Kommunikationsnetze sind das Internet sowie die Netze für Mobil- und Festnetztelefonie, nicht hingegen rein firmeninterne Netzwerke.

2.5.3.4 In der Gemeinschaft

Die E-Datenschutz-Richtlinie gilt für Dienste, die „in der Gemeinschaft" angeboten werden, d.h. unabhängig vom Standort des Dienstebetreibers für alle in der EU lebenden Personen.

2.5.3.5 Zusammenhang zwischen E-Datenschutz-Richtlinie und dem Regulierungsrahmen für den Telekommunikationssektor

Die E-Datenschutz-Richtlinie ist zugleich Teil des EU-Regulierungsrahmens für die elektronische Kommunikation und neben der allgemeinen TK-Rahmenrichtlinie[328] und zwei Verordnungen eine von vier spezifischen Richtlinien[329], die die Regulierung der Übertragung elektronischer Kommunikationen (d.h. nicht der Kommunikationsinhalte[330]) regeln.[331] Dieser Regulierungsrahmen für den Kommunikationssektor wird derzeit überarbeitet. Die Kommission hat im September 2016 eine ehrgeizige Überarbeitung der EU-Vorschriften für den Telekommunikationsbereich sowie weitere neue Initiativen vorgeschlagen, mit denen die wachsenden Anforderungen an die Netzanbindung in Europa erfüllt und Europas Wettbewerbsfähigkeit gesteigert werden sollen. Im Rahmen dieses sogenannten „Connectivity Package" schlägt die Kommission auch einen neuen „Europäischen Kodex für die elektronische Kommunikation"[332] vor, in dem die bestehenden Regelungen „zukunftsweisend" in überarbeiteter und vereinfachter Form in einer Richtlinie zusammengefasst wurden.

---

325 Vgl. Erwägungsgrund 13 der Änderungsrichtlinie [2009/136/EG] (Fn. 298).
326 Art. 3 E-Datenschutz-Richtlinie.
327 Art. 3 E-Datenschutz-Richtlinie.
328 Vgl. Fn. 310.
329 Neben der E-Datenschutz-Richtlinie sind dies die Zugangsrichtlinie [2002/19/EG], die Genehmigungsrichtlinie [2002/20/EG] sowie die Universaldiensterichtlinie [2002/22/EG].
330 Die Regulierung der Inhalte, die über elektronische Kommunikationsnetze übermittelt werden, erfolgt u.a. durch die AVMD-Richtlinie [2010/13/EU] (die derzeit ebenfalls überarbeitet wird, vgl. cep**Analyse**), sowie die E-Commerce-Richtlinie [2000/31/EG].
331 Details zum TK-Regulierungsrahmen unter https://ec.europa.eu/digital-single-market/en/telecoms-rules.
332 European Electronic Communications Code. Siehe die Neufassung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates vom 12.10.2016 über den europäischen Kodex für die elektronische Kommunikation [COM(2016) 590 (final)], abrufbar unter http://ec.europa.eu/transparency/regdoc/rep/1/2016/DE/1-2016-590-DE-F1-1.PDF.

Dieser Richtlinienvorschlag führt eine neue Definition sogenannter „interpersoneller Kommunikationsdienste“ ein[333], die künftig – neben Internetzugangsdiensten und Diensten, die ganz oder überwiegend in der Übertragung von Signalen bestehen – unter den Begriff der „elektronischen Kommunikationsdienste“ fallen. Interpersonelle Kommunikationsdienste sind Dienste, die einen direkten zwischenmenschlichen und interaktiven Informationsaustausch zwischen einer endlichen Zahl natürlicher Personen ermöglichen; z.B. Sprachanrufe, E-Mails, Mitteilungen oder Gruppenchats.[334] Nach Auffassung der Kommission ist es zukunftsorientiert, elektronische Kommunikationsdienste funktional zu bestimmen und nicht allein auf technische Parameter abzustellen. Aus Sicht des Endnutzers spiele es keine Rolle, ob ein Anbieter die Signale selbst übertrage oder ob die Kommunikation über einen Internetzugangsdienst übermittelt werde.[335] Kommt es zu keinen Änderungen im Gesetzgebungsprozess, wird der neue Kodex für die elektronische Kommunikation daher künftig in bestimmtem Umfang auch für OTT-Kommunikationsdienste gelten. Soweit OTT-Kommunikationsdienste zugleich Dienste der Informationsgesellschaft sind, gelten für sie zusätzlich die für diese Dienste geltenden Bestimmungen, sofern der Kodex oder andere EU-Rechtsakte keine spezielleren Bestimmungen enthalten.[336] Im Übrigen – d.h. soweit sie weder kommunikationsbezogene Inhalte noch den Zugang zum Internet bereitstellen und auch nicht ganz oder überwiegend in der Übertragung von Signalen bestehen – werden OTT-Inhaltsdienste durch den Kodex hingegen nicht reguliert.

2.5.4 Ausnahmen und Einschränkungen

Ebenso wie die DSRL den Mitgliedstaaten unter gewissen Voraussetzungen die Einschränkung bestimmter Rechte und Pflichten erlaubt, dürfen die Mitgliedstaaten auch bestimmte näher genannte Rechte und Pflichten der E-Datenschutz-Richtlinie (darunter die Regelungen betreffend die Vertraulichkeit, Cookies, zur Rufnummernanzeige sowie zu Verkehrs- und anderen Standortdaten) beschränken, wenn diese Beschränkung für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit oder für die Verfolgung von Straftaten oder des unzulässigen Gebrauchs elektronischer Kommunikationssysteme in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.[337]

Im Hinblick auf Rechtsbehelfe, Haftung und Sanktionen verweist die E-Datenschutz-Richtlinie auf die Bestimmungen der DSRL.[338] Gleichermaßen wird der Aufgabenbereich der unter der DSRL eingesetzten Art. 29-Datenschutzgruppe dahingehend erweitert, dass diese Gruppe auch den Schutz der Grundrechte, Grundfreiheiten und berechtigten Interessen im Bereich der elektronischen Kommunikation wahrnimmt.[339]

2.5.5 Geltung und Umsetzung

Die E-Datenschutz-Richtlinie war bis zum 31.10.2003 ins nationale Recht umzusetzen[340] und wurde in Deutschland maßgeblich im Telekommunikationsgesetz (TKG)[341] und im Telemediengesetz (TMG) umgesetzt. Nachdem die E-Datenschutz-Richtlinie im Jahr 2009 durch die sogenannte „Cookie-Richtlinie“ geändert worden war, wurde in der Vergangenheit insbesondere diskutiert, ob

333 Vgl. Art. 2 Abs. 5 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332).
334 Erwägungsgrund 17 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332).
335 Vgl. Erwägungsgrund 15 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332).
336 Vgl. Erwägungsgrund 10 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332).
337 Art. 15 Abs. 1 E-Datenschutz-Richtlinie.
338 Art. 15 Abs. 2 E-Datenschutz-Richtlinie.
339 Art. 15 Abs. 3 E-Datenschutz-Richtlinie.
340 Art. 17 Ans. 1 E-Datenschutz-Richtlinie.
341 §§ 91 ff. TKG.

Deutschland den „Cookie-Paragraphen“ und damit die Richtlinie ausreichend umgesetzt habe. Eine ausdrückliche Umsetzung erfolgte nicht. Fraglich war, ob der bestehende § 15 Abs. 3 TMG, der eine Opt-Out-Lösung vorsieht, richtlinienkonform ist. Dagegen spricht, dass die Richtlinie nach ihrem klaren Wortlaut das Setzen von Cookies nur nach Einwilligung des Nutzers erlaubt. Dennoch gingen offenbar sowohl das Bundeswirtschaftsministerium als auch die Kommission davon aus, dass Deutschland die Regelungen hinreichend umgesetzt habe. So soll die Kommission in einer Stellungnahme die Auffassung vertreten haben, dass das Datenschutzniveau in Deutschland den Anforderungen der Richtlinie bereits entspreche und die Richtlinie somit umgesetzt sei.[342] Eine Begründung hierfür wurde nicht veröffentlicht. Offen bleibt daher, ob die deutsche Opt-Out-Lösung ausreicht oder ob eine Einwilligung zwar erforderlich ist, aber ggf. durch den Nutzer stillschweigend erteilt wird, wenn er die Webseite trotz Information über die Cookie-Verwendung ohne Opt-Out weiternutzt. Diese Frage wird nun durch die Überarbeitung der E-Datenschutz-Richtlinie obsolet. Aber auch über die deutschen Grenzen hinaus wurde insbesondere die Cookie-Regelung in den Mitgliedstaaten sehr unterschiedlich umgesetzt.

2.5.6 Überarbeitung der E-Datenschutz-Richtlinie

Die E-Datenschutz-Richtlinie trat 2002 in Kraft und wurde zuletzt 2009 im Zuge der Überarbeitung des Rechtsrahmens für die elektronische Kommunikation geändert.

Bereits in ihrer digitalen Binnenmarktstrategie[343] hatte die Kommission eine Überprüfung der E-Datenschutz-Richtlinie für die Zeit nach Verabschiedung der DSGVO angekündigt, um insbesondere ein hohes Schutzniveau für die betroffenen Personen und gleiche Wettbewerbsbedingungen für alle Marktteilnehmer zu gewährleisten. Wie bereits angesprochen, gelten die meisten Regelungen der E-Datenschutz-Richtlinie in ihrer bisherigen Fassung nach Auffassung der Kommission nur für Betreiber herkömmlicher elektronischer Kommunikationsdienste. Anbieter von Diensten der Informationsgesellschaft, die das Internet zur Erbringung von Kommunikationsdiensten nutzen, sind dagegen im Allgemeinen von ihrem Anwendungsbereich ausgeschlossen.[344]

Auch in der DSGVO hat die Kommission für die Zeit nach deren Annahme eine Überprüfung der E-Datenschutz-Richtlinie angekündigt, insbesondere um die Kohärenz zwischen DSGVO und E-Datenschutz-Richtlinie zu gewährleisten.[345]

Die Kommission hat am 10. Januar 2017 einen Vorschlag für eine Verordnung betreffend die Achtung der Privatsphäre und den Schutz personenbezogener Daten in elektronischen Kommunikationen vorgelegt, der die derzeitige E-Datenschutz-Richtlinie ersetzen soll, um die angestrebten Ziele zu erreichen. Das nachfolgende Kapitel befasst sich näher mit diesem Vorschlag.

---

342 Hoeren, Internetrecht, Stand Oktober 2016, S. 464, unter Verweis auf https://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html; BVDW, Whitepaper: „Browsercookies und alternative Tracking-Technologien: Technische und datenschutzrechtliche Aspekte“, a.a.O. (Fn. 287), S. 11.

343 Vgl. die Mitteilung der EU-Kommission vom 06.05.2015, Strategie für einen digitalen Binnenmarkt für Europa, KOM (2015) 192 (final), S. 15.

344 Vgl. etwa https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-communications-and-challenge-new-technologies-are sowie bereits oben Ziffer 2.5.3.1.

345 Vgl. Erwägungsgrund 173 DSGVO.

3 Aktuelle Reformprozesse im EU-Datenschutzrecht

3.1 Der Vorschlag der Kommission für eine neue E-Datenschutz-Verordnung

3.1.1 Allgemeines

Die Kommission hat am 10. Januar 2017 einen Reformvorschlag[346] zur E-Datenschutz-Richtlinie vorgelegt. Demnach soll die derzeitige E-Datenschutz-Richtlinie aufgehoben und durch eine „Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation" (Verordnung über Privatsphäre und Kommunikation, nachfolgend als „E-Datenschutz-Verordnung" bezeichnet) ersetzt werden.

Der Verordnungsvorschlag enthält überarbeitete Vorschriften für den Schutz der Grundrechte und Grundfreiheiten im Bereich der elektronischen Kommunikation – insbesondere des Grundrechts auf Achtung des Privatlebens, Wahrung der Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten.[347] Wie schon die E-Datenschutz-Richtlinie setzt er das in Art. 7 der EU-Grundrechtecharta (GRCh) sowie Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention (EMRK) verankerte Grundrecht auf Achtung des Privatlebens für den Bereich der elektronischen Kommunikation in das europäische Sekundärrecht um.[348] Entsprechendes gilt für das ebenfalls in der GRCh (Art. 8 Abs. 1) verankerte Recht auf den Schutz personenbezogener Daten.

Ziel der Kommission ist es, die Regelungen der E-Datenschutz-Richtlinie an die geänderte technische und wirtschaftliche Realität anzupassen. Gleichzeitig sollen ihre Regelungen vereinfacht und mit denjenigen der Datenschutzgrundverordnung abgestimmt werden, um Doppelregelungen zu vermeiden und Kohärenz zu gewährleisten.[349] Auf diese Weise will die Kommission die Privatsphäre und die personenbezogenen Daten im Bereich der elektronischen Kommunikation im Einklang mit den genannten Grundrechten effektiver schützen und Rechtssicherheit schaffen.[350]

Die vorgeschlagene Verordnung soll EU-weit ein gleichwertiges Datenschutzniveau sowohl für natürliche als auch juristische Personen schaffen und zugleich den freien Verkehr elektronischer Kommunikationsdaten, -geräte und Dienste in der Union sicherstellen.[351] Die bisherige Richtlinie enthalte einige unklar gefasste Bestimmungen und habe zu einer teilweise sehr unterschiedlichen Umsetzung in den Mitgliedstaaten geführt, was die grenzüberschreitende Tätigkeit für Diensteanbieter erschwere. Insbesondere die Cookie-Regelung, welche eine Einwilligung der Endnutzer erfordere, habe ihr Ziel verfehlt, da sie bestimmte kritische Praktiken nicht erfasse, andererseits aber datenschutzrechtlich irrelevante Praktiken erschwere.[352]

Anders als die bisherige Richtlinie wird die neue E-Datenschutz-Verordnung ohne Umsetzung unmittelbar in allen EU-Mitgliedstaaten gelten und Vorrang vor nationalen Gesetzen haben. So soll eine EU-weit einheitliche Anwendung der Vorschriften gesichert werden.

---

346 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), COM(2017) 10 final, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1488238695629&uri=CELEX:52017PC0010.

347 Vgl. die Begründung des Vorschlags für eine E-Datenschutz-Verordnung, S. 2.

348 Siehe auch die Begründung des Vorschlags für eine E-Datenschutz-Verordnung, S. 2.

349 Vgl. Executive Summary of the Impact Assessment, Commission Staff Working Document, SWD(2017) 4 final, S. 2, abrufbar unter http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41246.

350 Vgl. die Begründung des Vorschlags für eine E-Datenschutz-Verordnung, S. 10.

351 Vgl. die Begründung (S. 2) sowie Erwägungsgrund 42 des Vorschlags für eine E-Datenschutz-Verordnung.

352 Vgl. die Begründung des Vorschlags für eine E-Datenschutz-Verordnung, S. 6.

3.1.2 Wesentliche Inhalte des Reformvorschlags

3.1.2.1 Definitionen

Der Vorschlag für eine E-Datenschutz-Verordnung verweist auf zahlreiche Definitionen in anderen Rechtsakten, insbesondere in der DSGVO und dem Vorschlag für einen neuen Kodex für die elektronische Kommunikation. Kraft dieses Verweises sollen künftig alle Definitionen der DSGVO auch im Rahmen der E-Datenschutz-Verordnung gelten. Darüber hinaus greift der Verordnungsvorschlag für die Definition der elektronischen Kommunikationsdienste und -netze und weiterer Begriffe auf die Definitionen im Richtlinienvorschlag für einen neuen Kodex für die elektronische Kommunikation zurück. In gleicher Weise hatte zuvor die E-Datenschutz-Richtlinie auf die Definitionen der TK-Rahmenrichtlinie verwiesen. Nach wie vor muss es sich um einen Dienst handeln, der gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbracht wird.[353] Während Inhaltsdienste[354] weiterhin ausgenommen sind[355], umfasst der neue Vorschlag neben Internetzugangsdiensten (z.B. Bereitstellung von Internetzugang über ISDN, DSL, Satellit oder Kabelmodem) und Diensten, die ganz oder überwiegend in der Übertragung von Signalen bestehen (z.B. Festnetz- und Mobiltelefonie) künftig auch sogenannte „interpersonelle Kommunikationsdienste".[356] Darunter versteht man Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch zwischen einer endlichen Zahl natürlicher Personen ermöglichen. Hierunter fallen künftig auch internetbasierte Kommunikationsdienste, die Sprachanrufe, E-Mails, Mitteilungsdienste oder Gruppenchats ermöglichen[357], sogenannte OTT-Kommunikationsdienste.[358] Dabei geht die E-Datenschutz-Verordnung insoweit über die Begriffsbestimmung im Entwurf eines Kodex für die elektronische Kommunikation[359] hinaus, als sie auch für Dienste gelten soll, die eine interaktive persönliche Kommunikation lediglich als untrennbare und untergeordnete Nebenfunktion ermöglichen. Damit dürften etwa auch Chatfunktionen im Rahmen von Online-Spielen erfasst sein. Hintergrund für diese Erweiterung ist, dass der Schutz der Vertraulichkeit der Kommunikation laut Kommission auch dann unverzichtbar ist, wenn die elektronische Kommunikationsfunktion nur eine untergeordnete Nebenfunktion eines anderen Dienstes darstellt.[360] Die Verordnung schützt „Endnutzer", das sind alle Personen, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst nutzen oder beantragen und nicht selbst solche Dienste oder öffentliche Kommunikationsnetze bereitstellen.[361] Sie schützt ferner alle Informationen in Bezug auf „Endeinrichtungen" von Endnutzern. „Endeinrichtungen" sind Einrichtungen zum Aussenden, Verarbeiten oder Empfangen von Nachrichten, die direkt oder indirekt an die Schnittstelle eines öffentlichen Telekom-

353 Art. 2 Nr. 4 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332). Siehe dazu bereits oben Ziffer 2.5.3.1.

354 Inhaltsdienste sind Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben, vgl. Art. 2 Nr. 4 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332). Vgl. auch oben Ziffer 2.5.3.1 zur vergleichbaren Situation unter der E-Datenschutz-Richtlinie.

355 Art. 2 Nr. 4 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332).

356 Vgl. Art. 2 Nr. 4,5 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332).

357 Erwägungsgrund 17 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332). Zu dem funktionalen Ansatz der Kommission vgl. bereits oben Ziffer 2.5.3 (Fn. 335).

358 Vgl. hierzu bereits oben Ziffer 2.5.3.1 und sogleich unten Ziffer 3.1.2.2.

359 Vgl. Art. 2 Abs. 5 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332).

360 Vgl. Art. 4 Abs. 2 sowie Erwägungsgrund 11 des Vorschlags für eine E-Datenschutz-Verordnung.

361 Vgl. die Definitionen von „Nutzer" und „Endnutzer" in Art. 2 Nr. 13 und 14 des Entwurfs für einen Kodex für die elektronische Kommunikation (Fn. 332).

munikationsnetzes angeschlossen sind, wobei die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden kann.[362]

Darüber hinaus enthält der Verordnungsvorschlag eigene Begriffsdefinitionen. Zentral ist dabei der Begriff der „elektronischen Kommunikationsdaten", der sowohl die „Inhalte" als auch die „Metadaten" elektronischer Kommunikationen umfasst.[363] Während „Inhalte" insbesondere Texte, Sprache, Videos, Bilder oder Töne sein können[364], sind unter „Metadaten" alle Daten zu verstehen, die in elektronischen Kommunikationsnetzen verarbeitet werden, um Inhalte elektronischer Kommunikationen zu übermitteln, zu verteilen oder auszutauschen. Dazu gehören etwa Daten über Quelle, Ziel, Datum, Uhrzeit, Dauer und Art der Kommunikation, angerufene Nummern, besuchte Webseiten oder der geografische Standort eines Geräts.[365] Weitere Begriffsdefinitionen werden aktualisiert (z.B. diejenige der „elektronischen Post") oder zur Liste hinzugefügt (z.B. die Definition der „Direktwerbung").

3.1.2.2 Erweiterung des Anwendungsbereichs auf OTT-Dienste

Zu den wesentlichen Neuerungen der neuen E-Datenschutz-Verordnung gehört es, dass ihr Anwendungsbereich auf OTT-Kommunikationsdienste erweitert wird.[366] Obwohl diese Dienste zunehmend an Bedeutung gewinnen und die herkömmliche Kontaktaufnahme über klassische elektronische Kommunikationsdienste wie die Telefonie und SMS immer mehr in den Hintergrund drängen, war die bisherige Richtlinie nach Auffassung der Kommission auf sie nicht anwendbar. Die neue E-Datenschutz-Verordnung soll hingegen durch den Verweis auf die ihrerseits erweiterte telekommunikationsrechtliche Begriffsdefinition der elektronischen Kommunikationsdienste[367] künftig auch für Webmaildienste wie GMX und web.de, Sofortnachrichtendienste wie WhatsApp, Kommunikationslösungen über soziale Netzwerke wie Facebook sowie für Internet- und Videotelefoniedienste (Voice over IP, Skype) gelten. Zu beachten ist, dass soziale Netzwerke dabei nicht insgesamt durch die E-Datenschutz-Verordnung reguliert werden, sondern lediglich ihre Messaging-Dienste (z.B. Facebook Messenger).

Ziel ist es einerseits, die Nutzer der neuen internetbasierten Kommunikationsformen in gleicher Weise zu schützen wie bei der Nutzung herkömmlichen Telekommunikationsdienste. Zweitens will die Kommission für die Anbieter neuer und herkömmlicher Kommunikationsdienste, die aus Sicht der Nutzer substituierbar sind, gleiche Wettbewerbsbedingungen schaffen.

3.1.2.3 Vertraulichkeit und Verarbeitung von Inhalten und Metadaten

Die Achtung der Privatsphäre in der Kommunikation ist ein wesentlicher Aspekt des in Art. 7 der EU-Grundrechtecharta (GRCh) niedergelegten Grundrechts einer Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.[368] Ein effektiver Schutz der Vertraulichkeit ist zugleich Grundvoraussetzung für die Ausübung anderer Grundrechte wie der Meinungs- und Informationsfreiheit, des Rechts auf den Schutz personenbezogener Daten oder der

---

362 Der Entwurf einer E-Datenschutz-Verordnung verweist insoweit in Art. 4 Abs. 1 lit. c) auf die Definition der „Endeinrichtungen" in Art. 1 Abs. 1 der Richtlinie [2008/63/EG] der Kommission vom 20. Juni 2008 über den Wettbewerb auf dem Markt für Telekommunikationsendeinrichtungen, EU-Amtsblatt L 178 vom 17.07.2000, S. 1-16.

363 Art. 4 Abs. 3 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung.

364 Art. 4 Abs. 3 lit. b) des Vorschlags für eine E-Datenschutz-Verordnung.

365 Art. 4 Abs. 3 lit. c) des Vorschlags für eine E-Datenschutz-Verordnung.

366 Vgl. hierzu bereits oben Ziffer 2.5.3.1.

367 Vgl. hierzu bereits oben Ziffer 2.5.3.1.

368 Vgl. Erwägungsgrund 1 des Vorschlags für eine E-Datenschutz-Verordnung.

Glaubens-, Gewissens- und Religionsfreiheit.[369] Vertraulichkeit bedeutet, dass die über eine Kommunikation ausgetauschten Informationsinhalte ebenso wie die externen Elemente dieser Kommunikation wie Zeit, Ort und Gesprächspartner niemandem außer den Kommunikationspartnern offengelegt werden.[370] Um dies zu gewährleisten, ist jeder Eingriff in elektronische Kommunikationsdaten wie Mithören, Abhören, Speichern, Beobachten, Scannen oder sonstiges Abfangen, Überwachen oder andere Verarbeitungen elektronischer Kommunikationsdaten grundsätzlich verboten.[371] Ein Abfangen liegt auch vor, wenn Dritte ohne Einwilligung des betreffenden Endnutzers besuchte Webseiten oder die Interaktion mit anderen beobachten.[372]

Anknüpfend an den Schutz von Verkehrs- und Standortdaten unter der E-Datenschutz-Richtlinie schützt der neue Verordnungsvorschlag sowohl die Vertraulichkeit der Kommunikationsinhalte als auch der „Metadaten"[373] einer elektronischen Kommunikation. Auch aus Metadaten lassen sich ggf. Schlussfolgerungen über das Privatleben der beteiligten Personen ziehen, z.B. in Bezug auf ihre sozialen Beziehungen, Interessen und Gewohnheiten.[374] Nicht nur Inhalte, sondern auch Metadaten können daher sensible Informationen über die an der Kommunikation beteiligten Personen offenlegen. Dies gilt auch für juristische Personen, deren Kommunikationsdaten Geschäftsgeheimnisse oder andere Informationen mit wirtschaftlichem Wert beinhalten können.[375] Elektronische Kommunikationsdaten, d.h. alle Inhalte und Metadaten, dürfen daher nur verarbeitet werden, wenn einer der in der Verordnung geregelten Ausnahmetatbestände vorliegt. Sowohl Inhalts- als auch Metadaten haben eine hohe Bedeutung für den Schutz der Privatsphäre und müssen anonymisiert oder gelöscht werden, wenn die Endnutzer keine Einwilligung erteilt haben und die Übertragung der Inhalte abgeschlossen ist oder die Metadaten nicht mehr für die Rechnungsstellung benötigt werden.[376]

Hinsichtlich der Definition der „Einwilligung" sowie der Frage, welche Anforderungen an diese zu stellen sind, verweist der Entwurf auf die DSGVO.[377] Dies gilt auch für die Einwilligungserklärungen juristischer Personen, für die die DSGVO ansonsten gar nicht gilt.[378] Endnutzer, die ihre Einwilligung zur Verarbeitung elektronischer Kommunikationsinhalte und -metadaten gegeben haben, können diese Einwilligung jederzeit widerrufen und sollen künftig alle sechs Monate an diese Möglichkeit erinnert werden.[379]

Anbieter elektronischer Kommunikationsdienste dürfen Metadaten ausnahmsweise ohne Einwilligung des Endnutzers verwenden, soweit dies zur Durchführung der Übermittlung der Kommunikation[380] oder zu Abrechnungs- und Betrugsbekämpfungszwecken[381] nötig ist. Gleiches gilt, soweit Metadaten zeitlich limitiert zur Aufrechterhaltung oder Wiederherstellung der Sicherheit und Kontinuität elektronischer Kommunikationsdienste und -netze verarbeitet werden, z.B. um Sicherheitsbedrohungen durch Schadsoftware aufzuspüren.[382] Neuerdings dürfen die Anbieter Metadaten auch ohne Einwilligung verarbeiten, soweit und solange dies notwendig ist, um verbindliche

369 Vgl. die Begründung des Entwurfs für einen Kodex für die elektronische Kommunikation, S. 9 oben (Fn. 332).
370 Vgl. Erwägungsgrund 1 des Vorschlags für eine E-Datenschutz-Verordnung.
371 Art. 5 Abs. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
372 Erwägungsgrund 15 des Vorschlags für eine E-Datenschutz-Verordnung.
373 Zur Definition der „Metadaten" vgl. oben Ziffer 3.1.2.1.
374 Vgl. Erwägungsgrund 2 des Vorschlags für eine E-Datenschutz-Verordnung.
375 Vgl. Erwägungsgrund 3 des Vorschlags für eine E-Datenschutz-Verordnung.
376 Art. 7 Abs. 1-3 des Vorschlags für eine E-Datenschutz-Verordnung.
377 Art. 9 Abs. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
378 Vgl. Erwägungsgrund 3 des Vorschlags für eine E-Datenschutz-Verordnung.
379 Art. 9 Abs. 3 des Vorschlags für eine E-Datenschutz-Verordnung.
380 Art. 6 Abs. 1 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung.
381 Art. 6 Abs. 2 lit. b) des Vorschlags für eine E-Datenschutz-Verordnung.
382 Art. 6 Abs. 1 lit. b) sowie Erwägungsgrund 16 des Vorschlags für eine E-Datenschutz-Verordnung.

Dienstqualitätsanforderungen erfüllen zu können, die der vorgeschlagene Kodex für die elektronische Kommunikation oder die Verordnung [(EU) 2015/2120][383] vorschreiben.[384]

Die Verordnung erweitert jedoch laut Kommission die Möglichkeiten für Anbieter elektronischer Kommunikationsdienste, Metadaten zu verarbeiten und zusätzliche Dienste anzubieten, wenn eine Einwilligung der Endnutzer vorliegt.[385] Bislang ist die Verarbeitung von Verkehrsdaten außer zur Übermittlung oder Abrechnung nur mit Einwilligung des Endnutzers und nur zur Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von „Diensten mit Zusatznutzen" möglich. Hierunter versteht man Dienste, die über das für die Übermittlung oder Abrechnung von Nachrichten erforderliche Maß hinaus Verkehrsdaten verarbeiten, etwa um meteorologische oder touristische Informationen zu bestimmten Standorten bereitzustellen.[386] Die Begrenzung auf die genannten Zwecke fällt künftig weg. Metadaten dürfen daher vom Anbieter des Kommunikationsdienstes über Abrechnungs- und Betrugsbekämpfungszwecke[387] hinaus künftig auch für andere, auch eigene Zwecke verwendet werden, beispielsweise zur Erbringung weiterer Dienste an den Endnutzer. Voraussetzung ist jedoch, dass diese Zwecke genau angegeben, die Anforderungen der DSGVO insbesondere an eine wirksame Einwilligung des Endnutzers eingehalten sind und der Zweck nicht auch unter Verwendung anonymisierter Daten erreicht werden könnte.[388] So können Endnutzer beispielsweise in die Verwendung ihrer Metadaten einwilligen, um Dienste zum Schutz vor betrügerischen Aktivitäten nutzen zu können.[389]

Inhaltsdaten darf der Anbieter dagegen nur zu eng gefassten Zwecken und unter klar definierten Bedingungen verarbeiten. So darf er Inhaltsdaten ebenso wie Metadaten außer zur Durchführung der Übermittlung der Kommunikation zeitlich limitiert zur Aufrechterhaltung oder Wiederherstellung der Sicherheit und Kontinuität elektronischer Kommunikationsdienste und -netze verarbeiten, z.B. um Sicherheitsbedrohungen durch Schadsoftware aufzuspüren.[390] Ansonsten ist eine Verarbeitung von Inhalten nur zulässig, wenn der Anbieter einen bestimmten Dienst an einen Endnutzer ohne diese Verarbeitung nicht erbringen kann und der bzw. die betroffene(n) Endnutzer eingewilligt haben.[391] Gleiches gilt, wenn es um die Verarbeitung der Informationen mehrerer Endnutzer zu bestimmten Zwecken geht, die durch anonymisierte Informationen nicht erfüllt werden können, wie beispielsweise beim Scannen von E-Mails zu dem Zweck, bestimmtes vorab festgelegtes Material zu entfernen, und alle betroffenen Endnutzer eigewilligt haben.[392] Weil die Verordnung die letztgenannten Fälle als hochrisikoreich einstuft, muss der Anbieter hier vor Einholung der Einwilligung aller betroffenen Endnutzer noch die Aufsichtsbehörde konsultieren und sich ggf. deren Empfehlungen beugen.[393]

---

383 Verordnung [(EU) 2015/2120] des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie [2002/22/EG] über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung [(EU) Nr. 531/2012] über das Roaming in öffentlichen Mobilfunknetzen in der Union, ABl. L 310 vom 26.11.2015, S. 1 ff.

384 Art. 6 Abs. 2 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung. Vgl. auch Erwägungsgrund 16, der hinsichtlich der erforderlichen Dienstqualitätsanforderungen beispielhaft auf Latenz und Verzögerungsschwankungen (Jitter) Bezug nimmt.

385 Vgl. Erwägungsgrund 17 des Vorschlags für eine E-Datenschutz-Verordnung.

386 Vgl. Art. 2 lit. g) sowie Erwägungsgrund 18 der E-Datenschutz-Richtlinie.

387 Art. 6 Abs. 2 lit. b) des Vorschlags für eine E-Datenschutz-Verordnung.

388 Art. 6 Abs. 2 lit. c) des Vorschlags für eine E-Datenschutz-Verordnung.

389 Vgl. Erwägungsgrund 18 des Vorschlags für eine E-Datenschutz-Verordnung.

390 Art. 6 Abs. 1 lit. b) sowie Erwägungsgrund 16 des Vorschlags für eine E-Datenschutz-Verordnung.

391 Art. 6 Abs. 3 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung.

392 Vgl. Erwägungsgrund 19 des Vorschlags für eine E-Datenschutz-Verordnung.

393 Art. 6 Abs. 3 lit. b) des Vorschlags für eine E-Datenschutz-Verordnung i.V.m. Art. 36 Abs. 2, 3 DSGVO.

Die neue Verordnung reguliert auch das Internet der Dinge. Das Vertraulichkeitsprinzip gilt ausdrücklich auch für die Übertragung von Kommunikationen von Maschine zu Maschine.[394]

3.1.2.4 Einbeziehung von Informationen in und aus Endgeräten in den Schutz der Privatsphäre – überarbeitete Vorschriften für Cookies und andere „Tracking Tools“

Techniken, mit denen die Online-Aktivitäten von Endnutzern oder deren Aufenthaltsort verfolgt oder die Funktionsweise ihrer Endgeräte unbemerkt manipuliert wird, bedrohen laut Kommission die Privatsphäre der Endnutzer in ernstzunehmender Weise, zumal dies oft ohne Wissen des Endnutzers geschieht.[395] Aus diesem Grund hat die Kommission die unklaren Regelungen der E-Datenschutz-Richtlinie zum Schutz vor Cookies und anderen Instrumenten, die Informationen über einen Endnutzer sammeln und dessen Verhalten verfolgen[396] (auch als „Tracking Tools“[397] oder „Verfolgungswerkzeuge“ bezeichnet), überarbeitet und an die technischen Entwicklungen angepasst.

Die neue Verordnung schützt künftig generell (1) alle Informationen, die in Endgeräten von Endnutzern wie PCs, Tablets oder Smartphones gespeichert sind (dazu sogleich 3.1.2.4.1) oder (2) von diesen Geräten ausgesendet, angefordert oder verarbeitet werden, um sie mit anderen Geräten oder Netzanlagen zu verbinden[398] (hierzu siehe unten 3.1.2.4.3).

3.1.2.4.1 Nutzung der Verarbeitungs- und Speicherfunktion von Endgeräten und Zugriff auf in diesen gespeicherte Informationen

Zum einen soll es Dritten ohne Einwilligung des Endnutzers künftig grundsätzlich verboten sein, Dateien auf dessen Endgerät zu speichern, dessen Verarbeitungsfunktionen zu nutzen oder auf Informationen zuzugreifen, die in diesen Endgeräten gespeichert sind.[399]

Beispielsweise werden auf Smartphones, Tablets etc. immer häufiger Fotos, Kontaktlisten, persönliche Nachrichten und andere Informationen gespeichert, die einen tiefen Einblick in die Persönlichkeit des Gerätebesitzers geben können. Tracking Tools wie Cookies, Spyware, Web Bugs und „Versteckte Kennungen“ können – häufig ohne Wissen des Endnutzers – in dessen Endgerät eindringen, um auf solche Informationen zuzugreifen, auf dem Gerät versteckte Informationen bzw. Softwarepakete zu speichern oder die Online-Aktivitäten des Endnutzers zu verfolgen. Hiergegen sollen Endnutzer effizienter geschützt werden, wenn in ihre Privatsphäre mehr als nur geringfügig eingegriffen wird.

Dritte dürfen die Verarbeitungs- und Speicherfunktion von Endgeräten immer dann nutzen oder auf darin gespeicherte Informationen zugreifen, wenn der Endnutzer hierin eingewilligt hat[400] oder wenn dies allein für die „Durchführung“ des Kommunikationsvorgangs, d.h. für die Übermittlung einer elektronischen Kommunikation „nötig“ ist.[401] Darüber hinaus ist eine solche Speicherung

394 Vgl. Erwägungsgrund 12 des Vorschlags für eine E-Datenschutz-Verordnung.
395 Erwägungsgrund 20 des Vorschlags für eine E-Datenschutz-Verordnung.
396 Vgl. dazu oben 2.5.2.5 und 2.5.5.
397 Im Internet versteht man unter „Tracking“ die quantitative Messung und das Nachvollziehen des Nutzerverhaltens auf Webseiten sowie in einem weiteren Nutzungskontext die Messung von Werbeeinblendungen zum Zweck der Auslieferungskontrolle und -steuerung, vgl. BVDW, Whitepaper: „Browsercookies und alternative Tracking-Technologien: Technische und datenschutzrechtliche Aspekte“, a.a.O. (Fn. 287), S. 2.
398 Vgl. Erwägungsgrund 20 des Vorschlags für eine E-Datenschutz-Verordnung.
399 Art. 8 Abs. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
400 Art. 8 Abs. 1 lit. b) des Vorschlags für eine E-Datenschutz-Verordnung
401 Art. 8 Abs. 1 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung.

oder Nutzung bzw. ein solcher Zugriff ausnahmsweise auch dann ohne Einwilligung zulässig, wenn damit „kein oder nur ein geringfügiger Eingriff in die Privatsphäre“ verbunden ist.[402] So soll etwa ein technisches Speichern oder ein Zugriff erlaubt sein, wenn dies für die Bereitstellung eines vom Endnutzer gewünschten Dienstes der Informationsgesellschaft[403] oder – neu – für Messungen des „Webpublikums“, d.h. der Nutzerzahlen auf der Webseite desselben Diensteanbieters „nötig“ ist. Cookies können hierfür ein legitimes Hilfsmittel sein.[404] Auch für die Dauer eines Besuchs einer Webseite sollen Cookies ohne Einwilligung der Endnutzer gesetzt werden dürfen, um diesen das Ausfüllen mehrseitiger Online-Formulare zu ermöglichen.[405] Im Übrigen ist eine Einwilligung erforderlich.

3.1.2.4.2 Datenschutzfreundliche Einstellungsmöglichkeiten („Privacy by Design“)

Um die Erteilung der Einwilligung zu vereinfachen, sieht der Entwurf der E-Datenschutz-Verordnung künftig ausdrücklich die Besonderheit vor, dass die Einwilligung – soweit technisch machbar – auch durch entsprechende technische Einstellungen eines Browsers oder einer Applikation erteilt werden kann.[406] Damit soll es Anbietern erleichtert werden, die Einwilligung für das Setzen von Cookies sowie die sonstige Nutzung der Speicherungs- oder Verarbeitungsfunktion von Endgeräten oder die Erhebung von in diesen gespeicherten Informationen einzuholen. Zugleich sollen Endnutzer vor einer Überfrachtung mit Aufforderungen zur Erteilung ihrer Einwilligung bewahrt werden.[407]

Um dies zu ermöglichen, verpflichtet die neue Verordnung alle Anbieter von Software, die eine elektronische Kommunikation ermöglicht, diese Software so zu konfigurieren, dass der Endnutzer die Speicherung fremder Informationen auf seinem Endgerät oder den Zugriff Dritter auf Informationen, die bereits dort gespeichert sind, durch transparente und benutzerfreundliche Einstellungen verhindern kann.[408] Diese Verpflichtung trifft alle Hersteller von Browsern, die es ermöglichen, Informationen aus dem Internet abzurufen und darzustellen, sowie alle Hersteller von Anwendungen (Applikationen), die Anrufe oder Nachrichtenübermittlung ermöglichen oder Navigationshilfe bieten.[409] Jeder Endnutzer soll bei der Installation der Software über die verschiedenen Einstellungsmöglichkeiten zur Privatsphäre informiert werden und zur Fortsetzung der Installation eine Auswahl treffen müssen.[410] Insoweit knüpft die E-Datenschutz-Verordnung an die in der DSGVO verankerten Prinzipien des Datenschutzes durch Technikgestaltung („Privacy-by-Design“) und durch datenschutzfreundliche Voreinstellungen („Privacy by Default“) an. Dabei soll der Endnutzer auch über die Risiken der einzelnen Optionen (z.B. langfristige Protokollierung des individuellen Surfverhaltens) informiert werden.[411] Er soll dann beispielsweise wählen können, ob er generell alle Cookies akzeptieren oder ablehnen, nur Cookies des Anbieters der aktuell von ihm genutzten Webseite („First Party Cookies“[412]) oder auch Cookies, die von anderen Domains (Drittanbietern)

---

402 Vgl. Erwägungsgrund 21 des Vorschlags für eine E-Datenschutz-Verordnung.
403 Art. 8 Abs. 1 lit. c) des Vorschlags für eine E-Datenschutz-Verordnung.
404 Art. 8 Abs. 1 lit. d) des Vorschlags für eine E-Datenschutz-Verordnung. Vgl. auch die insoweit strengere Formulierung im Erwägungsgrund 20, wonach das Speichern oder Zugreifen zur Ermöglichung eines vom Nutzer „ausdrücklich gewünschten“ Dienstes „unbedingt notwendig und verhältnismäßig“ sein muss.
405 Vgl. Erwägungsgrund 21 des Vorschlags für eine E-Datenschutz-Verordnung.
406 Art. 9 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.
407 Vgl. Erwägungsgrund 22 des Vorschlags für eine E-Datenschutz-Verordnung.
408 Art. 10 Abs. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
409 Vgl. Erwägungsgrund 22 des Vorschlags für eine E-Datenschutz-Verordnung.
410 Art. 10 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.
411 Vgl. Erwägungsgrund 24 des Vorschlags für eine E-Datenschutz-Verordnung.
412 Zur Definition der „First Party Cookies“ vgl. auch das BVDW Whitepaper: „Browsercookies und alternative Tracking-Technologien: Technische und datenschutzrechtliche Aspekte“, a.a.O. (Fn. 287), S. 6.

gesetzt werden, akzeptieren möchte („Third Party Cookies“[413]). Darüber hinaus soll er die Einstellungen jederzeit ändern, Ausnahmen für bestimmte Webseiten machen und bestimmte Webseiten auflisten können, auf denen er Cookies generell akzeptieren oder blocken möchte.[414] Die getroffene Auswahl soll dann für Dritte verbindlich und ihnen gegenüber auch durchsetzbar sein.[415] Anders als noch in einer Vorabversion[416] des Kommissionsentwurfs, die im Dezember 2016 kursierte, sollen die Softwareanbieter allerdings offenbar nicht verpflichtet sein, generell vom Start weg die datenschutzfreundlichsten Einstellungen der Software (d.h. Blocken aller Cookies) vorzukonfigurieren. Eine solche Voreinstellung hätte zur Folge, dass bei Fehlen einer aktiven Auswahl durch den Endnutzer konsequenterweise alle Cookies geblockt werden müssten. Dies erscheint nun – jedenfalls nach dem Wortlaut der E-Datenschutz-Verordnung – nicht mehr zwingend. Diese sieht lediglich eine Pflicht des Anbieters vor, den Endnutzer über die Einstellungsoptionen zu informieren und zur Auswahl einer Einstellungsoption aufzufordern, durch die er seine Einwilligung zum Setzen von Cookies erteilen oder verweigern kann. Ist die Software bereits installiert, soll der Endnutzer beim nächsten Update, spätestens aber am 25. August 2018, über die Einstellungsmöglichkeit informiert werden und eine Auswahl vornehmen müssen.[417]

3.1.2.4.3 Erhebung von Informationen, die von Endgeräten ausgesendet werden

Unter der neuen Verordnung sollen Endnutzer aber nicht nur vor Cookies, sondern auch vor neuen Verfolgungstechniken geschützt werden, die ohne einen Zugriff auf bzw. eine Speicherung von Informationen im Endgerät des Endnutzers auskommen, wie beispielsweise das „Device Fingerprinting“ (Verfolgung von Gerätekennungen). Derartige Tracking-Methoden machen es sich zu Nutze, dass netzwerkfähige Endgeräte regelmäßig bestimmte Datenpakete aussenden, um sich mit einem anderen Gerät oder Netzwerk zu verbinden oder eine solche Verbindung aufrecht zu erhalten.[418] Beispielsweise senden mobile Endgeräte aktive Signale aus, die eindeutige Identifizierungskennungen wie MAC-Adresse[419], IMEI[420] oder IMSI-Nummer[421] enthalten. Diese Informationen können innerhalb bestimmter Reichweiten auch „remote“ – d.h. per Fernzugang – abgefangen (erhoben), gesammelt und zu verschiedenen Zwecken verarbeitet werden, die mehr oder weniger in die Privatsphäre eingreifen. Das Scannen und Abfangen von Bluetooth- oder WLAN-Signalen insbesondere von Smartphones bezeichnet man auch als „Offline Tracking“. Auf diese Weise können Menschenmengen gezählt, aber auch Aufenthalte bestimmter Personen an einem bestimmten Ort über längere Zeiträume hinweg verfolgt werden.[422] Solche Techniken können für die einen nützlich sein, die Privatsphäre der Endnutzer aber u.U. ernsthaft verletzen.[423] Die E-Datenschutz-Richtlinie in ihrer bisherigen Fassung erfasst neue Techniken zur Verfolgung des (Online)-Verhaltens der Endnutzer nicht.[424]

---

413 Zur Definition der „Third Party Cookies“ vgl. auch das BVDW Whitepaper: „Browsercookies und alternative Tracking-Technologien: Technische und datenschutzrechtliche Aspekte“, a.a.O. (Fn. 287), S. 6.
414 Vgl. Erwägungsgründe 23 und 24 des Vorschlags für eine E-Datenschutz-Verordnung.
415 Vgl. Erwägungsgrund 22 des Vorschlags für eine E-Datenschutz-Verordnung.
416 Vgl. den Link zur Version bei Politico, abrufbar unter http://g8fip1kplyr33r3krz5b97d1.wpengine.netdna-cdn.com/wp-content/uploads/2016/12/POLITICO-E-Datenschutz--directive-review-draft-december.pdf, dort Erwägungsgrund 28.
417 Art. 10 Abs. 3 des Vorschlags für eine E-Datenschutz-Verordnung.
418 Vgl. Erwägungsgrund 25 des Vorschlags für eine E-Datenschutz-Verordnung.
419 Abkürzung für „Media-Access-Control-Adresse“.
420 Abkürzung für „International Mobile Station Equipment Identity“ (Internationale Mobilfunkgerätekennung).
421 Abkürzung für „International Mobile Subscriber Identity“ (Internationale Mobilfunk-Teilnehmerkennung).
422 Vgl. Erwägungsgrund 25 des Vorschlags für eine E-Datenschutz-Verordnung.
423 Vgl. die Erwägungsgründe 20 und 25 des Vorschlags für eine E-Datenschutz-Verordnung.
424 Vgl. Erwägungsgrund 6 des Vorschlags für eine E-Datenschutz-Verordnung.

Nach der neuen Verordnung ist auch die Erhebung von Informationen, die von Endgeräten zum Zweck der Verbindungsherstellung ausgesendet werden, grundsätzlich verboten, es sei denn, es liegt ein Erlaubnistatbestand vor.[425] Das „externe" Abfangen von Informationen ist aber im Vergleich zur Platzierung von Cookies in Endgeräten unter erleichterten Voraussetzungen zulässig, eine Einwilligung ist nicht erforderlich. Selbstverständlich ist die Erhebung ausgesendeter Informationen zum einen zulässig, sofern und solange sie erfolgt, um eine Verbindung herzustellen.[426] Darüber hinaus dürfen solche Informationen aber auch zu anderen Zwecken (auch zu Werbezwecken) erhoben werden. Voraussetzung ist, dass der Endnutzer durch einen klaren und deutlichen Hinweis über diese Erhebung sowie über die Möglichkeiten, die Erhebung zu stoppen oder auf ein Minimum zu beschränken, informiert wird.[427] Dabei müssen ihm auch alle sonstigen nach der DSGVO notwendigen Informationen zur Datenerhebung (Zweck, Verantwortlicher, etc.) mitgeteilt werden. Zusätzlich muss der Anbieter angemessene Sicherheitsmaßnahmen nach der DSGVO[428] ergriffen haben. Dazu zählen beispielsweise die Pseudonymisierung oder Verschlüsselung der Daten. Um die Information zu erleichtern, sollen standardisierte Bildsymbole („Icons") entwickelt werden, die dem Endnutzer in vereinfachter Form einen Überblick über die Erhebung geben sollen.[429] Einzelheiten zu deren Verwendung will die Kommission ebenso wie unter der DSGVO[430] in delegierten Rechtsakten regeln.[431]

Im Ergebnis sieht die neue Verordnung für den Schutz von Informationen, die von Endgeräten ausgesendet werden, im Vergleich zum Schutz von Informationen, die im Endgerät gespeichert sind, ein deutlich niedrigeres Schutzniveau vor. Während das Setzen von Cookies grundsätzlich eine Einwilligung der Endnutzer erfordert, genügt es für das Abfangen von Gerätekennungen, dass die Endnutzer in hinreichender Weise über diesen Vorgang informiert werden (siehe oben) und Hinweise erhalten, wie sie sich der Datenerhebung entziehen können. Sofern personenbezogene Daten für Werbezwecke oder für Profilbildungen genutzt werden, hat der Endnutzer ein Widerspruchsrecht nach Art. 21 DSGVO.

3.1.2.5 Schutz vor unerbetener Direktwerbung (SPAM)

Die neue Verordnung stärkt auch den Schutz vor unerbetener Direktwerbung („Spam"). Der Begriff der „Direktwerbung" wird ausgeweitet und erfasst künftig nicht nur kommerzielle Werbung für das Angebot von Waren oder Dienstleistungen, sondern auch Wahlwerbung durch politische Parteien oder Werbung von Non-Profit-Organisationen für die Unterstützung ihrer Zwecke.[432] Damit wird jegliche Werbung erfasst, die an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste gerichtet wird.[433] Alle Formen der Direktwerbung sind grundsätzlich nur nach vorheriger Einwilligung des Endnutzers zulässig[434], die jederzeit leicht widerrufbar sein muss.[435] Dies gilt insbesondere für E-Mails, SMS, Sofortnachrichten, automatische

[425] Art. 8 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.
[426] Art. 8 Abs. 2 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung.
[427] Art. 8 Abs. 2 lit. b) des Vorschlags für eine E-Datenschutz-Verordnung.
[428] Art. 8 Abs. 2 lit. b) S. 2 des Vorschlags für eine E-Datenschutz-Verordnung, der auf Art 32 DSGVO verweist.
[429] Art. 8 Abs. 3 des Vorschlags für eine E-Datenschutz-Verordnung.
[430] Art. 12 Abs. 8 i.V.m. Art. 92 DSGVO. Vgl. auch oben Ziffer 2.2.2.3. unter (2).
[431] Art. 8 Abs. 4 i.V.m. Art. 27 des Vorschlags für eine E-Datenschutz-Verordnung. Dabei wird die Kommission vom Kommunikationsausschuss unterstützt, der auch unter dem neuen Kodex für die elektronische Kommunikation (Fn. 332) etabliert wird, vgl. Art. 110 des diesbezüglichen Richtlinienentwurfs der Kommission (Fn. 332).
[432] Vgl. Erwägungsgrund 32 des Vorschlags für eine E-Datenschutz-Verordnung.
[433] Vgl. die Definition des Begriffs der „Direktwerbung" in Art. 4 Abs. 3 lit. f) des Vorschlags für eine E-Datenschutz-Verordnung.
[434] Art. 16 Abs. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
[435] Art. 16 Abs. 6 i.V.m. Erwägungsgrund 34 f. des Vorschlags für eine E-Datenschutz-Verordnung.

Werbeanrufe und künftig grundsätzlich auch für persönliche Werbeanrufe. Für persönliche Werbeanrufe an natürliche Personen können die Mitgliedstaaten jedoch eine Opt-Out Lösung vorsehen. Der Verordnungsentwurf enthält insoweit nunmehr eine ausdrückliche Öffnungsklausel, von der die Mitgliedstaaten Gebrauch machen können.[436] Eine derartige nationale Regelung war allerdings nach den Erwägungsgründen der E-Datenschutz-Richtlinie schon bislang möglich.[437] Auch bei Werbe-E-Mails im Rahmen bestehender Kundenbeziehungen genügt unter bestimmten Voraussetzungen weiterhin ein Opt-Out.[438] Eine Voraussetzung ist dabei, dass die Werbung durch dasselbe Unternehmen versendet wird, welches die elektronischen Kontaktdaten aufgrund der bestehenden Kundenbeziehung erlangt hatte. Ferner muss es sich um Werbung für „ähnliche Produkte oder Dienstleistungen" wie beim Rechtsgeschäft der bestehenden Kundenbeziehung handeln.[439] Bei Marketinganrufen muss künftig entweder eine Rufnummer angegeben werden, unter der der Werbetreibende kontaktiert werden kann, oder es muss durch eine besondere Vorwahl (Code) angezeigt werden, dass es sich um einen Werbeanruf handelt.[440] Details hierzu soll die Kommission in Durchführungsrechtsakten regeln dürfen.[441] Wie schon bislang sollen die Mitgliedstaaten auch die berechtigten Interessen juristischer Personen schützen, keine ungewollte Direktwerbung zu erhalten.[442]

3.1.2.6 Weitere Regelungen

Alle Anbieter nummerngebundener interpersoneller Kommunikationsdienste, die die Anzeige von Rufnummern anbieten, müssen es ihren Endnutzern einfach und kostenfrei ermöglichen, ihre Privatsphäre durch Ausübung bestimmter Rechte zu wahren. So darf der Anrufer seine Rufnummer wie bislang für einen einzelnen Anruf, für eine bestimmte Verbindung und künftig auch dauerhaft unterdrücken. Der Angerufene darf die Anzeige der Rufnummern eingehender Anrufe sowie die Anzeige seiner eigenen Rufnummer beim Anrufer unterdrücken.[443] Ferner darf der Angerufene Anrufe von unterdrückten Rufnummern abweisen[444] oder anonyme Anrufe oder von bestimmten Rufnummern eingehende Anrufe auch generell blockieren lassen.[445] Ebenso kann er weiterhin die automatische Anrufweiterleitung durch einen Dritten auf sein Endgerät unterbinden lassen.[446] Die Verordnung verpflichtet die Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste nun unmittelbar, die Unterdrückung der Rufnummernanzeige bei Anrufen bei Notdiensten anschlussbezogen zu übergehen und eine fehlende Einwilligung des Anrufers in die Verarbeitung seiner Metadaten zu ignorieren, um Notrufe effektiv beantworten zu können.[447] Es obliegt jedoch weiterhin den Mitgliedstaaten, zu regeln, unter welchen Voraussetzungen Anbieter die Unterdrückung der Anzeige der anrufenden Nummer vorübergehend aufheben müssen, wenn Endnutzer beantragen, belästigende Anrufe zurückzuverfolgen.[448]

Ferner stellt die Verordnung klar, dass personenbezogene Daten natürlicher Personen nur mit deren Einwilligung in ein öffentlich zugängliches Verzeichnis der Endnutzer elektronischer Kommuni-

[436] Art. 16 Abs. 4 des Vorschlags für eine E-Datenschutz-Verordnung.
[437] Vgl. Erwägungsgrund 42 der E-Datenschutz-Richtlinie.
[438] Art. 16 Abs. 2 i.V.m. Erwägungsgrund 33 a.E. des Vorschlags für eine E-Datenschutz-Verordnung.
[439] Vgl. Erwägungsgrund 33 a.E. des Vorschlags für eine E-Datenschutz-Verordnung.
[440] Art. 16 Abs. 3 lit. a), b) des Vorschlags für eine E-Datenschutz-Verordnung.
[441] Art. 16 Abs. 6 i.V.m. Art. 26 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.
[442] Art. 16 Abs. 5 des Vorschlags für eine E-Datenschutz-Verordnung.
[443] Art. 12 Abs. 1 lit. a), b) und d) des Vorschlags für eine E-Datenschutz-Verordnung.
[444] Art. 12 Abs. 1 lit. c) des Vorschlags für eine E-Datenschutz-Verordnung.
[445] Art. 14 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung.
[446] Art. 14 lit. b) des Vorschlags für eine E-Datenschutz-Verordnung.
[447] Art. 13 Abs. 1 sowie Erwägungsgrund 28 des Vorschlags für eine E-Datenschutz-Verordnung.
[448] Art. 13 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.

kationsdienste[449] aufgenommen werden dürfen. Die Einwilligung muss für jede Kategorie von Daten (z.B. Name, Telefonnummer, Adresse, E-Mail-Adresse) erteilt werden, die für das Verzeichnis relevant sind.[450] Der Endnutzer muss die Daten kostenlos prüfen, berichtigen und löschen können.[451] Er muss künftig auch über den Zweck des Verzeichnisses sowie darüber informiert werden, unter welchen Suchkriterien er darin aufgefunden werden kann, und in die Freischaltung dieser Suchfunktion für seine Daten einwilligen.[452] Geschützt, wenngleich in geringerem Umfang, werden auch juristische Personen. Auch sie müssen die Daten kostenfrei prüfen, berichtigen und löschen dürfen. Anders als bei natürlichen Personen bedarf die Aufnahme ihrer Daten in ein Verzeichnis jedoch keiner Einwilligung; ihnen wird jedoch das Recht zuerkannt, der Aufnahme der Daten in das Verzeichnis zu widersprechen (Opt-Out). Die Entscheidung, nicht in das Verzeichnis aufgenommen zu werden, darf weder für natürliche noch für juristische Personen Kosten nach sich ziehen.

3.1.2.7 Informationen über Sicherheitsrisiken

Der neue Verordnungsentwurf sieht ähnlich wie die E-Datenschutz-Richtlinie[453] vor, dass der Anbieter elektronischer Kommunikationsdienste die Endnutzer über ein etwa bestehendes besonderes Risiko für die Sicherheit elektronischer Kommunikationsdienste und -netze informieren muss. Liegt das Risiko außerhalb des Bereichs, innerhalb dessen der Anbieter Gegenmaßnahmen treffen kann, muss er dem Endnutzer mitteilen, welche Abhilfemaßnahmen dieser selbst ergreifen kann (z.B. Verschlüsselung) und welche Kosten hierfür voraussichtlich anfallen.[454] Diese Informationspflicht tritt neben die Pflicht des Diensteanbieters, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um unvorhergesehene Sicherheitsrisiken zu beseitigen und das normale Sicherheitsniveau wieder herzustellen.

Diese Bestimmung der E-Datenschutz-Verordnung ist neben den Sicherheitsbestimmungen der DSGVO zu lesen, welche auch Anbieter elektronischer Kommunikationsdienste als verantwortliche Datenverarbeiter dazu verpflichten, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau hinsichtlich der Sicherheit der zu verarbeitenden Daten zu gewährleisten.[455] Hat das Risiko für die Sicherheit der Kommunikationsdienste bzw. -netze Datenschutzverletzungen zur Folge, greifen auch die Informationspflichten der DSGVO. Danach müssen Datenschutzverletzungen, bei denen ein Risiko für die Rechte und Freiheiten der Betroffenen nicht ausgeschlossen werden kann, der Aufsichtsbehörde und bei hohem Risiko auch dem Betroffenen selbst gemeldet werden.[456]

Weitere Regelungen zur Datensicherheit finden sich im Entwurf der E-Datenschutz-Verordnung nicht. Um die E-Datenschutz-Verordnung mit der DSGVO abzustimmen und Doppelregelungen zu vermeiden, wurden die übrigen in der E-Datenschutz-Richtlinie geregelten Verpflichtungen zum Anbieten sicherer Kommunikationsdienste gestrichen.[457] Die Kommission geht dabei offensichtlich davon aus, dass die DSGVO die Anforderungen an die vom Verantwortlichen oder Auftragsverarbeiter zu gewährleistende Datensicherheit ausführlich regelt.

---

[449] Zur Definition des „öffentlich zugänglichen Verzeichnisses“ siehe Art. 4 Abs. 3 lit. d) des Vorschlags für eine E-Datenschutz-Verordnung.
[450] Vgl. Erwägungsgrund 31 des Vorschlags für eine E-Datenschutz-Verordnung.
[451] Art. 15 Abs. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
[452] Art. 15 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.
[453] Art. 4 Abs. 2 E-Datenschutz-Richtlinie.
[454] Art. 17 des Vorschlags für eine E-Datenschutz-Verordnung.
[455] Vgl. Art. 32 DSGVO. Siehe hierzu auch oben Ziffer 2.2.2.3 unter (1).
[456] Vgl. Art. 33, 34 DSGVO. Vgl. auch insoweit oben Ziffer 2.2.2.3 unter (3).
[457] Vgl. die Begründung des Vorschlags für eine E-Datenschutz-Verordnung, S.2.

3.1.2.8 Überwachung und Durchsetzung der Verordnung

Konsistenz mit der DSGVO wird auch insoweit geschaffen, als wegen der strengen Synergien zwischen allgemeinem Datenschutz und der Vertraulichkeit von Kommunikationen[458] künftig dieselben unabhängigen nationalen Aufsichtsbehörden sowohl für die Überwachung und Durchsetzung der Datenschutzgrundverordnung als auch der E-Datenschutz-Richtlinie zuständig sind.[459] Weil die E-Datenschutz-Richtlinie den Begriff der zu ihrer Durchsetzung „zuständigen nationalen Behörde" nicht näher definierte, wurden in einigen Mitgliedstaaten die Datenschutzbehörden, in anderen die Regulierungsbehörden für den Telekommunikationssektor und in wieder anderen (z.B. in Deutschland) sowohl Regulierungs- als auch Datenschutzbehörden mit der Überwachung betraut. In manchen Mitgliedstaaten waren die Kompetenzen innerstaatlich sogar auf drei oder vier Behörden, darunter Verbraucherschutzbehörden verteilt.[460] Künftig sind in allen Mitgliedstaaten sowohl für die Überwachung und Durchsetzung der DSGVO als auch der E-Datenschutz-Verordnung dieselbe nationalen Aufsichtsbehörden zuständig, die die Mitgliedstaaten zur Überwachung der DSGVO eingerichtet haben.[461] Die Mitgliedstaaten dürfen auch mehrere Aufsichtsbehörden errichten, wenn dies ihrer – z.B. föderalen – Struktur entspricht.[462] Die eingesetzte(n) Aufsichtsbehörde(n) müssen allerdings mit den nationalen Regulierungsbehörden für den Telekommunikationssektor zusammenarbeiten, wenn dies zweckmäßig ist.[463]

Auch für die Zusammenarbeit der Aufsichtsbehörden und das Kohärenzverfahren bei grenzüberschreitender Datenverarbeitung gelten künftig dieselben einheitlichen Regeln wie nach der DSGVO.[464] Gleichermaßen erhält der unter der DSGVO eingerichtete Europäische Datenschutzausschuss (EDSA) die Aufgabe, die einheitliche Anwendung nicht nur der DSGVO, sondern auch der E-Datenschutz-Verordnung sicherzustellen.[465] Zu diesem Zweck übt er alle ihm durch die DSGVO übertragenen Befugnisse aus.[466] Darüber hinaus berät er die Kommission zu künftigen Änderungen der E-Datenschutz-Verordnung, untersucht Fragen zur Anwendung dieser Verordnung und stellt Leitlinien, Empfehlungen und bewährte Verfahren bereit, um die einheitliche Anwendung der E-Datenschutz-Verordnung sicherzustellen.[467]

Damit sind die Aufsichtsbehörden – anders als unter der DSRL oder DSGVO, welche sich auf den Schutz personenbezogener Daten natürlicher Personen beschränken – künftig zum einen auch für die Überwachung des Schutzes der Vertraulichkeit von Kommunikationen juristischer Personen durch die E-Datenschutz-Verordnung[468] zuständig. Soweit diese auch die Vertraulichkeit nichtpersonenbezogener Daten schützt, sind sie zum anderen auch für die effektive Anwendung der Verordnung zum Schutz solcher Daten verantwortlich. Neu ist schließlich auch, dass sie die An-

458 Vgl. die Begründung des Vorschlags für eine E-Datenschutz-Verordnung, S.9.
459 Art. 18 Abs. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
460 Näher dazu Commission Staff Working Document, Impact Assessment accompanying the document „Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)" vom 10.1.2017, SWD(2017) 3 final, Part 1/3, S. 36, sowie Part 3/3, Annex 11, abrufbar unter https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.
461 Vgl. Art. 51 ff. DSGVO.
462 Vgl. Erwägungsgrund 38 des Vorschlags für eine E-Datenschutz-Verordnung sowie Erwägungsgrund 117 der DSGVO.
463 Vgl. Art. 18 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.
464 Art. 20 des Vorschlags für eine E-Datenschutz-Verordnung. Vgl. auch oben Ziffer 2.2.2.5 unter (3).
465 Art. 19 S. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
466 Art. 19 S. 2 des Vorschlags für eine E-Datenschutz-Verordnung. Zu diesen Befugnissen vgl. bereits oben Ziffer 2.2.2.5 unter (3) und (4).
467 Art. 19 S. 3 lit. a) und b) des Vorschlags für eine E-Datenschutz-Verordnung.
468 Vgl. auch Erwägungsgrund 3 des Vorschlags für eine E-Datenschutz-Verordnung.

wendung der Verordnung künftig auch gegenüber Anbietern von OTT-Kommunikationsdiensten durchsetzen müssen.

3.1.2.9 Rechtsbehelfe, Haftung und Sanktionen

Auch die Rechtsbehelfe, die Haftungsregeln und die Sanktionen werden weitgehend an die entsprechenden Regelungen in der DSGVO angeglichen.

So können betroffene Endnutzer unter den in der DSGVO geregelten Voraussetzungen Beschwerde bei einer Aufsichtsbehörde erheben oder gerichtliche Rechtsbehelfe gegen Beschlüsse oder Untätigkeit einer Aufsichtsbehörde oder gegen Verantwortliche oder Auftragsverarbeiter einlegen.[469] Ein Vertretungsrecht durch Verbraucherorganisationen wie unter der DSGVO oder die Erlaubnis für die Mitgliedstaaten, Verbandsklagen ohne Auftrag vorzusehen[470], sieht die E-Datenschutz-Verordnung hingegen nicht vor. Der vorläufige Entwurf, welcher Ende 2016 kursierte, hatte noch vergleichbare Regelungen enthalten.[471] Diese wurden jedoch offenkundig aus dem endgültigen Entwurf hinausgestrichen.

Wie die DSGVO sieht auch die E-Datenschutz-Verordnung Geldbußen in abgestufter Höhe für schwerwiegende, mittlere und sonstige Verstöße vor. So können etwa bei Verstößen gegen die Cookie-Regelungen oder das Verbot zur unerbetenen Kommunikation Bußgelder bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes[472], bei Verstößen gegen den Grundsatz der Vertraulichkeit der Kommunikation oder bei unerlaubter Verarbeitung elektronischer Kommunikationsdaten sogar Bußgelder bis zu 20 Millionen oder 4% des weltweiten Jahresumsatzes verhängt werden.[473] Die Strafen für die übrigen – weniger schwerwiegenden – Verstöße sowie die Sanktionen gegenüber Behörden sollen hingegen von den Mitgliedstaaten geregelt werden.[474]

3.1.3 Anwendungsbereich

3.1.3.1 Sachlicher Anwendungsbereich

Der Entwurf der E-Datenschutz-Verordnung regelt zum einen die Verarbeitung elektronischer Kommunikationsdaten, die bei der Erbringung und Nutzung elektronischer Kommunikationsdienste[475] erfolgt, und zum anderen den Schutz von Informationen in und aus Endgeräten von Endnutzern.[476]

Er gilt jedoch nicht für

- Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen[477];
- Tätigkeiten der Mitgliedstaaten im Bereich der Gemeinsamen Außen- und Sicherheitspolitik (GASP)[478];

---

469 Art. 21 Abs. 1 des Vorschlags für eine E-Datenschutz-Richtlinie unter Verweis auf Art. 77, 78 und 79 DSGVO. Vgl. hierzu oben Ziffer 2.2.2.5. unter (7).
470 Art. 80 Abs. 1 und 2 DSGVO, vgl. auch insoweit oben Ziffer 2.2.2.5. (7).
471 Art. 23 Abs. 5 und 6 des Vorabentwurfs (Fn. 416).
472 Art. 23 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.
473 Art. 23 Abs. 3 des Vorschlags für eine E-Datenschutz-Verordnung.
474 Art. 23 Abs. 4 und 6 des Vorschlags für eine E-Datenschutz-Verordnung.
475 Zu den Definitionen und dem gegenüber der E-Datenschutz-Richtlinie erweiterten Anwendungsbereich des Vorschlags für eine E-Datenschutz-Verordnung siehe bereits oben Ziffer 3.1.2.1 und 3.1.2.2.
476 Art 2 Abs. 1 des Vorschlags für eine E-Datenschutz-Verordnung.
477 Art. 2 Abs. 2 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung.
478 Art. 2 Abs. 2 lit. b) des Vorschlags für eine E-Datenschutz-Verordnung.

- elektronische Kommunikationsdienste, die nicht öffentlich zugänglich sind[479] (z.B. Unternehmensnetze)[480]
- Tätigkeiten zuständiger Behörden zu Zwecken der Strafverfolgung, Strafvollstreckung und Gefahrenabwehr[481] sowie
- die Verarbeitung elektronischer Kommunikationsdaten durch EU-Organe und Einrichtungen.[482] Insoweit soll eine neue Verordnung zum Schutz personenbezogener Daten bei der Verarbeitung durch EU-Organe und Einrichtungen gelten, die die Verordnung [(EG) Nr. 45/2001] ersetzen wird.[483]

Darüber hinaus lässt der neue Verordnungsvorschlag die Regelungen der E-Commerce-Richtlinie [2000/31/EC] und insbesondere deren Haftungsregeln sowie die Bestimmungen der Funkanlagen-Richtlinie [2014/53/EU] unberührt[484], die – soweit anwendbar – parallel gelten.

3.1.3.2 Territorialer Anwendungsbereich

In territorialer Hinsicht soll die E-Datenschutz-Verordnung zunächst gelten, wann immer elektronische Kommunikationsdienste „für Endnutzer in der Union" bereitgestellt oder von diesen genutzt werden.[485] Das gilt – vergleichbar mit der Regelung in der DSGVO – auch dann, wenn die Verarbeitung der elektronischen Kommunikationsdaten außerhalb der Union erfolgt[486] oder wenn die elektronischen Kommunikationsdienste von außerhalb der EU für Endnutzer in der EU bereitgestellt werden.[487] Damit kommt es weder auf den Standort des Servers, auf dem die Daten gespeichert werden, noch darauf an, ob ein Unternehmen einen Sitz in einem EU-Mitgliedstaat hat. Die Qualifikation als „Dienst" ist auch nicht davon abhängig, ob der Endnutzer für den Dienst eine Zahlung zu leisten hat.[488]

Daneben schützt die neue Verordnung alle Informationen in Bezug auf Endgeräte von Endnutzern in der Union.[489] Voraussetzung für diesen Schutz ist damit allein, dass sich der Endnutzer in der Union befindet.[490]

Unternehmen aus Drittstaaten, die keinen Sitz innerhalb der EU haben, müssen wie unter der DSGVO einen Vertreter in der Union benennen, der als Anlaufstelle und Ansprechpartner für Betroffene und Aufsichtsbehörden fungiert.[491] Durch die Erweiterung des Anwendungsbereichs der neuen E-Datenschutz-Verordnung auf außereuropäische Wirtschaftsunternehmen, die auf dem europäischen Markt tätig sind, werden wie durch die DSGVO einheitliche Wettbewerbsbedingungen geschaffen.

---

479 Art. 2 Abs. 2 lit. c) des Vorschlags für eine E-Datenschutz-Verordnung.
480 Erwägungsgrund 13 des Vorschlags für eine E-Datenschutz-Verordnung.
481 Art. 2 Abs. 2 lit. d) des Vorschlags für eine E-Datenschutz-Verordnung.
482 Art. 2 Abs. 3 des Vorschlags für eine E-Datenschutz-Verordnung.
483 Näher hierzu unten Kapitel 3.2.
484 Art. 2 Abs. 4 und 5 sowie Erwägungsgrund 10 des Vorschlags für eine E-Datenschutz-Verordnung.
485 Art 3 Abs. 1 lit. a) und b) des Vorschlags für eine E-Datenschutz-Verordnung.
486 Vgl. Erwägungsgrund 9 des Vorschlags für eine E-Datenschutz-Verordnung.
487 Vgl. Erwägungsgrund 9 des Vorschlags für eine E-Datenschutz-Verordnung.
488 Art. 3 Abs. 1 lit. a) des Vorschlags für eine E-Datenschutz-Verordnung.
489 Art. 3 Abs. 1 lit. c) des Vorschlags für eine E-Datenschutz-Verordnung.
490 Art. 3 Abs. 1 lit. c) des Vorschlags für eine E-Datenschutz-Verordnung.
491 Art. 3 Abs. 3-5 des Vorschlags für eine E-Datenschutz-Verordnung.

3.1.4 Ausnahmen und Einschränkungen

Wie bereits unter der E-Datenschutz-Richtlinie[492] dürfen die Mitgliedstaaten bestimmte Rechte und Pflichten in Bezug auf die Vertraulichkeit, Verarbeitung und Speicherdauer von elektronischen Kommunikationsdaten oder den Schutz von Informationen in und aus Endgeräten[493] gesetzlich beschränken. So können sie unter Beachtung der EU-Grundrechtecharta regeln, in welchen Fällen elektronische Kommunikationen abgefangen werden kann.[494] Voraussetzung ist jedoch, dass der Wesensgehalt der Grundrechte und Grundfreiheiten geachtet wird und die Beschränkung in einer demokratischen Gesellschaft eine „notwendige, geeignete und verhältnismäßige Maßnahme" zum Schutz bestimmter wichtiger öffentlicher Interessen darstellt, die in der DSGVO[495] abschließend aufgelistet sind (z.B. zum Schutz der nationalen oder öffentlichen Sicherheit, der Verteidigung, oder zur Strafverfolgung und -vollstreckung), oder um Überwachungs- oder Regulierungsaufgaben vorzunehmen.[496] Soweit diese Voraussetzungen erfüllt sind, dürfen die Mitgliedstaaten auch mit dem Unionsrecht vereinbare Regelungen zur Vorratsdatenspeicherung erlassen oder beibehalten, welche von dem Verordnungsentwurf nicht geregelt wird.[497] Die Verfolgung des „unzulässigen Gebrauchs von elektronischen Kommunikationssystemen"[498] wird hingegen nicht mehr als Beschränkungszweck genannt. Die Anbieter elektronischer Kommunikationsdienste müssen wie schon nach bisherigem Recht interne Verfahren einrichten, um Anfragen zu beantworten, die im Einklang mit den so erlassenen Beschränkungsgesetzen den Zugang zu elektronischen Kommunikationsdaten verlangen. Einzelheiten zu solchen Anfragen und den Verfahren müssen die Mitgliedstaaten auf Anfrage der Aufsichtsbehörde mitteilen.[499]

3.1.5 Zeitplan der Kommission

Nach dem Zeitplan der Kommission soll die neue E-Datenschutz-Verordnung ab dem gleichen Zeitpunkt gelten, ab dem die Datenschutzgrundverordnung anwendbar wird, d.h. ab dem 25. Mai 2018.[500]

3.1.6 Künftiges Verhältnis von DSGVO und geplanter E-Datenschutz-Verordnung

Die obige Darstellung der Anwendungsbereiche der DSGVO und der geplanten E-Datenschutz-Verordnung zeigt, dass die Anwendungsbereiche der beiden Verordnungen sich teilweise überschneiden. Bezüglich der Frage, wann die DSGVO und wann die E-Datenschutz-Verordnung anwendbar sind, sind die unterschiedlichen Schutzrichtungen der beiden Rechtsakte zu berücksichtigen. Während die DSGVO den Schutz und den freien Verkehr personenbezogener Daten gewährleistet, schützt die E-Datenschutz-Verordnung maßgeblich die Vertraulichkeit der Kommunikation, die auch nicht personenbezogene Daten und Daten in Bezug auf juristische Personen enthalten kann. Angesichts dieser unterschiedlichen Schutzrichtungen hat die Kommission es vorgezogen,

---

492 Art. 15 Abs. 1 E-Datenschutz-Richtlinie.
493 Eingeschränkt werden können Rechte und Pflichten aus den Artikel 5-8 des Vorschlags für eine E-Datenschutz-Verordnung, vgl. dessen Art. 11 Abs. 1.
494 Vgl. Erwägungsgrund 26 des Vorschlags für eine E-Datenschutz-Verordnung.
495 Vgl. Art. 23 Abs. 1 lit. a) - e) DSGVO.
496 Art. 11 Abs. 1 sowie Erwägungsgrund 26 des Vorschlags für eine E-Datenschutz-Verordnung.
497 Vgl. die Begründung des Vorschlags für eine E-Datenschutz-Verordnung, S. 3.
498 Art. 15 Abs. 1 E-Datenschutz-Richtlinie.
499 Art. 11 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.
500 Vgl. Art. 29 Abs. 2 des Vorschlags für eine E-Datenschutz-Verordnung.

die Vertraulichkeit elektronischer Kommunikationen in einem von der DSGVO getrennten Rechtsakt zu regeln.[501]

Die DSGVO enthält ebenso wie die bisher geltende EU-Datenschutzrichtlinie keine spezifischen, strengeren Vorgaben für die sogenannte „distanzüberwindende Kommunikation". Dies war im Rahmen des Gesetzgebungsprozesses vorgeschlagen worden, am Ende blieb es jedoch beim Verweis auf die Spezialvorschriften in der E-Datenschutz-Richtlinie.[502]

Auch der neue Vorschlag für eine E-Datenschutz-Verordnung sieht spezielle Vorschriften für den Schutz der Rechte und Grundfreiheiten natürlicher und juristischer Personen bei der Erbringung und Nutzung elektronischer Kommunikationsdienste vor. Die E-Datenschutz-Verordnung geht der DSGVO als speziellere Regelung („lex specialis") vor und präzisiert und ergänzt insoweit deren Regelungen[503], soweit personenbezogene Daten im Rahmen elektronischer Kommunikationen verarbeitet werden. Die DSGVO erfasst alle Fragen der Verarbeitung personenbezogener Daten, die durch die E-Datenschutz-Verordnung nicht speziell geregelt werden.

Zusätzliche Informationspflichten bei der Datenverarbeitung[504] sowie Pflichten zum Ergreifen von Sicherheitsmaßnahmen in der DSGVO dürften daher auch für Anbieter elektronischer Kommunikationen gelten. Darüber hinaus erscheint das Verhältnis zwischen E-Datenschutz-Verordnung und DSGVO jedoch nicht in allen Punkten klar. Fraglich ist beispielsweise, ob bzw. in welchem Umfang generell auch die allgemeinen Datenschutzgrundsätze der DSGVO für die Verarbeitung personenbezogener elektronischer Kommunikationsdaten gelten sollen. Aus den Erwägungsgründen der E-Datenschutz-Verordnung lässt sich lediglich entnehmen, dass das Schutzniveau, welches natürliche Personen nach der DSGVO genießen, nicht eingeschränkt werden soll.[505]

Außerhalb des Anwendungsbereichs der E-Privacy-Verordnung gilt die DSGVO dagegen uneingeschränkt. Beispielsweise beschränkt sich die E-Privacy-Verordnung auf den Schutz elektronischer Kommunikationsdaten, die im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste verarbeitet werden.[506] Demgegenüber gelten die DSRL und wohl auch die DSGVO auch für die Verarbeitung personenbezogener Daten im Rahmen nicht öffentlich zugänglicher elektronischer Kommunikationsdienste bzw. auch für Dienste in nichtöffentlichen Netzen.[507]

Dagegen schützt die DSGVO nicht die Daten juristischer Personen, sondern beschränkt sich wie die DSRL auf den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz ihrer personenbezogener Daten bei deren Verarbeitung.[508] Demgegenüber schützt die E-Datenschutz-Verordnung auch die berechtigten Interessen von juristischen Personen als Kommunikationsteilnehmern.[509]

---

501 Zu Schutzrichtungen und Regelungsinstrument vgl. auch die Begründung des Vorschlags für eine E-Datenschutz-Verordnung, S. 5, 6.
502 Art. 95 i.V.m. Erwägungsgrund 173 der DSGVO. Vgl. auch oben 2.2.3.1 (Sachlicher Anwendungsbereich der DSGVO).
503 Art. 1 Abs. 1 sowie S. 3 der Begründung des Vorschlags für eine E-Datenschutz-Verordnung.
504 Vgl. Erwägungsgrund 25 der E-Datenschutz-Verordnung.
505 Vgl. Erwägungsgrund 5 der E-Datenschutz-Verordnung.
506 Umkehrschluss aus Art. 2 Abs. 2 lit. c) des Vorschlags für eine E-Datenschutz-Verordnung, vgl. entsprechend Art. 3 E-Datenschutz-Richtlinie.
507 Vgl. Erwägungsgrund 10 der E-Datenschutz-Richtlinie.
508 Art. 1 Abs. 1 DSRL, Art. 1 Abs. 1, 2 DSGVO.
509 Art. 1 Abs. 2 sowie Erwägungsgrund 3 des Vorschlags für eine E-Datenschutz-Verordnung, insoweit ebenso bereits Art. 1 Abs. 2 E-Datenschutz-Richtlinie.

Die folgende Tabelle verdeutlicht die Anwendbarkeit von DSGVO und E-Datenschutz-Verordnung:

Abb. 1: Anwendbarkeit von DSGVO und E-Datenschutz-Verordnung.

	DSGVO	E-Datenschutz-VO
Verarbeitung **personenbezogener** Daten bei der Erbringung **öffentlich zugänglicher** elektronischer Kommunikationsdienste 1	nur subsidiär, soweit E-Datenschutz-Verordnung keine spezielleren Regelungen enthält	ja
Verarbeitung **personenbezogener** Daten durch Verantwortliche oder Auftragsverarbeiter, die **nicht** im Rahmen elektronischer **Kommunikationsdienste** erfolgt	ja	nein
Verarbeitung **personenbezogener** Daten bei der Erbringung von Kommunikationsdiensten, die **nicht öffentlich zugänglich** sind (z.B. in internen Unternehmensnetzwerken)	ja	nein
Verarbeitung **elektronischer Kommunikationsdaten**	Ja, soweit personenbezogene Daten	ja
Schutz von **Informationen** im Zusammenhang mit **Endgeräten**	Ja, soweit personenbezogene Daten	ja
Verarbeitung von **Daten juristischer Personen** bei der Erbringung **öffentlich zugänglicher** elektronischer Kommunikationsdienste	nein	ja

Quelle: cep.

3.2 Der Vorschlag der Kommission für eine überarbeitete Verordnung zum Schutz personenbezogener Daten bei der Verarbeitung durch EU-Organe und -Einrichtungen

3.2.1 Allgemeines

Teil des am 10. Januar 2017 von der Kommission veröffentlichten Datenschutzreformpakets ist auch ein Vorschlag[510] für eine überarbeitete Fassung der Verordnung [(EG) Nr. 45/2001], die gesonderte Datenschutzvorschriften für EU-Organe, Einrichtungen und sonstige Stellen der Union regelt, wenn diese personenbezogene Daten verarbeiten (nachfolgend als „Datenschutzverordnung für EU-Organe und -Einrichtungen" bezeichnet). Diese Verordnung, die auch Regelungen zum freien Datenverkehr enthält, soll die bisherige Verordnung [(EG) Nr. 45/2001] ersetzen und zugleich den Beschluss Nr. 1247/2002/EG über die Aufgaben des Europäischen Datenschutzbeauftragten[511] aufheben. Ziel der Kommission ist es, das Schutzniveau dieser Verordnung an das hohe Niveau der

[510] Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung [(EG) Nr. 45/2001] und des Beschlusses Nr. 1247/2002/EG, COM(2017) 8 final, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1488205011179&uri=CELEX:52017PC0008.

[511] Beschluss Nr. 1247/2002/EG des Europäischen Parlaments, des Rates und der Kommission vom 1. Juli 2002 über die Regelungen und allgemeinen Bedingungen für die Ausübung der Aufgaben des Europäischen Datenschutzbeauftragten, ABl. L 183 vom 12.07.2002, S. 1 ff.

DSGVO anzugleichen, so dass personenbezogene Daten bei der Verarbeitung durch EU-Organe nunmehr im gleichen Umfang geschützt sind. Demnach werden der freie Datenverkehr und der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch EU-Organe und Einrichtungen weiterhin außerhalb der DSGVO in einer eigenständigen Verordnung geregelt.

3.2.2 Wesentliche Inhalte des Reformvorschlags

Die Verordnung wird grundlegend angepasst. Aufbau und Text der neuen Verordnung für die Datenverarbeitung durch EU-Organe und Einrichtungen entsprechen in weiten Teilen wörtlich der DSGVO. Die bisherigen Definitionen werden weitgehend durch Verweise auf die DSGVO, die vorgeschlagene E-Datenschutz-Verordnung[512], den vorgeschlagenen Kodex für die elektronische Kommunikation[513] und die Richtlinie [2008/63/EG][514] ersetzt. Die Verordnung enthält noch einige zusätzliche Definitionen wie die der EU-Organe und Einrichtungen. Die Datenschutzgrundsätze der Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie die in der DSGVO vorgesehenen Rechte und Pflichten gelten nun vollumfänglich auch für EU-Behörden. Auch die Anforderungen an eine wirksame datenschutzrechtliche Einwilligung sind identisch. Gleichermaßen werden neue Pflichten wie diejenige zur Durchführung einer Datenschutz-Folgeabschätzung künftig auch für EU-Behörden gelten.[515] Wie schon bislang müssen alle EU-Organe und Institutionen intern einen Datenschutzbeauftragten bestellen.

Über Disziplinarmaßnahmen für einzelne Bedienstete hinaus soll es künftig auch für EU-Behörden Sanktionen in Form von Bußgeldern in Höhe von bis zu 25.000 EUR (maximal 250.000 EUR pro Jahr), bei bestimmten Verstößen sogar bis zu 50.000 EUR pro Verstoß (maximal 500.000 EUR pro Jahr) geben, die sodann in den EU-Gesamthaushalt fließen.[516]

Wie schon bislang will die Kommission auch die relevanten Spezialregelungen für die Verarbeitung elektronischer Kommunikationsdaten direkt in diese Verordnung integrieren. Die neue Verordnung enthält wie ihre Vorgängerin knapp formulierte Regelungen zum Schutz der Vertraulichkeit[517] sowie zum Schutz von Daten in Teilnehmerverzeichnissen[518] und verweist hinsichtlich des Schutzes von Informationen in und aus Endgeräten völlig auf die neue E-Datenschutz-Verordnung.[519] Weitere Regelungen zur Verarbeitung von Verkehrsdaten und zur Rufnummernanzeige sind in der neuen Verordnung nicht mehr enthalten.

3.2.3 Anwendungsbereich

Die neue Datenschutzverordnung für EU-Organe und -Einrichtungen gilt, wenn EU-Organe und -Einrichtungen, die in der Verordnung näher definiert sind[520], personenbezogene Daten verarbeiten. EU-Organe und -Einrichtungen dürfen danach den freien Verkehr personenbezogener Daten untereinander oder mit Empfängern in der EU, die der DSGVO und den nationalen Vorschriften zur Umsetzung der Datenschutzrichtlinie für Polizei und Justiz unterworfen sind, nicht einschränken.

Die DSGVO, die Datenschutzrichtlinie für Polizei und Justiz und die neue E-Datenschutz-Verordnung sollen demgegenüber für EU-Organe und -Einrichtungen nicht unmittelbar gelten. So

512 Siehe Fn. 346.
513 Siehe Fn. 332.
514 Siehe Fn. **Fehler! Textmarke nicht definiert.**.
515 Art. 39 des Verordnungsentwurfs (Fn. 510).
516 Art. 66 Abs. 1-3 und 7 des Verordnungsentwurfs (Fn. 510).
517 Art. 34 des Verordnungsentwurfs (Fn. 510).
518 Art. 36 des Verordnungsentwurfs (Fn. 510).
519 Art. 35 des Verordnungsentwurfs (Fn. 510).
520 Vgl. Art. 3 Abs. 2 lit. a) des Verordnungsentwurfs (Fn. 510).

sieht die DSGVO ausdrücklich vor, dass für die Verarbeitung personenbezogener Daten durch EU-Organe und -Einrichtungen die Verordnung [(EG) Nr. 45/2001] gilt.[521] Dies dürfte für die neue Datenschutzverordnung für EU-Organe und -Einrichtungen, die diese Verordnung ersetzen soll, fortgelten. Die Datenschutzrichtlinie für Polizei und Justiz findet ausdrücklich keine Anwendung auf die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der EU.[522] Auch die E-Datenschutz-Verordnung stellt klar, dass für die Verarbeitung elektronischer Kommunikationsdaten durch die Organe, Einrichtungen und sonstigen Stellen der EU die neue Datenschutzverordnung für EU-Organe und -Einrichtungen gelten soll.[523]

Damit soll offenbar künftig grundsätzlich nur die Datenschutzverordnung für EU-Organe und -Einrichtungen unmittelbar gelten, wenn EU-Organe und -Einrichtungen entweder personenbezogene Daten generell oder elektronische Kommunikationsdaten im Besonderen verarbeiten. Es gelten jedoch die Begriffsbestimmungen der Datenschutzgrundverordnung und der E-Datenschutz-Verordnung, soweit die Datenschutzverordnung für EU-Organe und -Einrichtungen auf diese verweist.[524] Darüber hinaus gilt die E-Datenschutz-Verordnung indirekt auch inhaltlich für EU-Organe und -Einrichtungen, soweit die Datenschutzverordnung für EU-Organe und -Einrichtungen auf sie verweist.[525]

3.2.4 Wesentliche Unterschiede im Vergleich zur DSGVO

Unterschiede zur DSGVO ergeben sich vor allem aufgrund der unterschiedlichen Zuständigkeiten insbesondere zur Überwachung der Einhaltung der Verordnung. Wie schon nach der Verordnung [(EG) Nr. 45/2001] erfolgt die Überwachung aller[526] Datenverarbeitungsvorgänge unter der Datenschutzverordnung für EU-Organe und Einrichtungen durch den Europäischen Datenschutzbeauftragten (EDBA) als unabhängige Kontrollbehörde.[527] Dieser übernimmt im Prinzip alle Aufgaben, die nach der DSGVO die nationalen Datenschutzbehörden als zuständige Aufsichtsbehörden innehaben. Daher benötigt die Datenschutzverordnung für EU-Organe und -Einrichtungen im Gegensatz zur DSGVO keine Regelungen, die die Kompetenzen und Zusammenarbeit der nationalen Datenschutzbehörden oder das Kohärenzverfahren betreffen. Stattdessen enthält sie Vorschriften zu Ernennung, Kompetenzen, Aufgaben und Zuständigkeiten des EDBA. So können Betroffene[528] oder das Personal[529] einer EU-Behörde oder Einrichtung ungeachtet ihrer gerichtlichen Rechtsbehelfe weiterhin auch eine Beschwerde beim EDBA einreichen, wenn sie der Auffassung sind, dass Vorschriften der Verordnung verletzt wurden.

Wo die DSGVO auf das nationale Recht verweist, werden diese Verweise in der Datenschutzverordnung für EU-Organe und -Einrichtungen durch Verweise auf EU-Recht ersetzt. Wo die DSGVO Öffnungsklauseln enthält, finden sich in der Datenschutzverordnung für EU-Organe und -Einrichtungen z.T. bereits konkrete Regelungen. So wurde etwa das Mindestalter für die Einwilli-

521 Art. 2 Abs. 3 DSGVO.
522 Art. 2 Abs. 3 lit. b) der Datenschutzrichtlinie für Polizei und Justiz (Fn. 7).
523 Vgl. Art. 2 Abs. 3 des Vorschlags für eine E-Datenschutz-Verordnung.
524 Vgl. Art. 3 Abs. 1 lit. a) und b) des Verordnungsentwurfs (Fn. 510), die auf die Begriffsbestimmungen der DSGVO und der E-Datenschutz-Verordnung verweisen.
525 Vgl. Art. 35 des Verordnungsentwurfs (Fn. 510), der den Schutz der Informationen in und aus Endgeräten von Nutzern beim Zugriff auf öffentlich zugängliche Webseiten und mobile Anwendungen der EU-Organe und -Einrichtungen regelt und insoweit auf Art 8 E-Datenschutz-Verordnung verweist.
526 Ausgenommen ist lediglich Datenverarbeitung durch den EuGH in Ausübung seiner gerichtlichen Funktion, vgl. Art. 58 Abs. 1 lit. a) des Verordnungsentwurfs (Fn. 510).
527 Art. 1 Abs. 3 des Verordnungsentwurfs (Fn. 510).
528 Vgl. Art. 63 Abs. 1 des Verordnungsentwurfs (Fn. 510).
529 Art. 68 des Verordnungsentwurfs (Fn. 510).

gung in Datenverarbeitungen durch Dienste der Informationsgesellschaft auf 13 Jahre festgelegt.[530]

Auch EU-Organe dürfen bestimmte Rechte und Pflichten der Verordnung beschränken, und zwar durch EU-Rechtsakte auf der Grundlage der EU-Verträge oder durch behördeninterne Regelungen, wenn diese veröffentlicht wurden. Die Anzahl der Zwecke, zu denen EU-Organe und -Einrichtungen Rechte und Pflichten einschränken dürfen, erscheint dabei teilweise weiter zu sein als die von der DSGVO vorgesehenen Einschränkungsmöglichkeiten für die Mitgliedstaaten. Beispielsweise sind zusätzlich u. a. Einschränkungen zum Schutz der inneren Sicherheit von EU-Organen und Einrichtungen und ihrer elektronischen Kommunikationsnetzwerke sowie zu bestimmten privilegierten Forschungs- und Archivzwecken zulässig.

Ferner verzichtet die Datenschutzverordnung für EU-Organe und -Einrichtungen auf diejenigen Regelungen der DSGVO, die für die Datennutzung durch EU-Organe nicht passen, wie etwa auf

- den Erlaubnistatbestand der „berechtigten Interessen“,
- das Widerspruchsrecht gegen die Datennutzung zu Direktmarketingzwecken,
- die Pflicht zur Vertreterbestellung für Unternehmen ohne Sitz in der EU,
- die Regelungen zur Zertifizierung von Unternehmen oder zu Verhaltensregeln für Unternehmen[531] sowie auf
- die Vorschriften für besondere Verarbeitungssituationen[532].

Gleiches gilt für in der DSGVO bereits geregelte Fragen wie den Erlass von Angemessenheitsbeschlüssen durch die Kommission zur Ermöglichung des Drittstaatentransfers oder zur Einrichtung des Europäischen Datenschutzausschusses, an dem auch der EDPA teilnimmt.[533]

Während für Streitigkeiten im Rahmen der DSGVO die mitgliedstaatlichen Gerichte zuständig sind[534], ist schließlich – wie schon bislang – der EuGH für alle Streitigkeiten über die Vorschriften der Datenschutzverordnung für EU-Organe und -Einrichtungen zuständig.[535] Hinsichtlich der Haftung für Schadensersatz verweist die Verordnung auf die EU-Verträge.[536] Während eine Vertretung durch Verbände bei Beschwerden oder Schadensersatzansprüche möglich ist, ist die Möglichkeit einer „Verbandsbeschwerde“ ohne individuellen Auftrag hier nicht vorgesehen.[537] Auch in weiteren Regelungen finden sich noch gewisse Unterschiede im Detail.

3.2.5 Zeitplan der Kommission

Geht es nach der Kommission, soll die überarbeitete Verordnung zeitgleich mit der Datenschutzgrundverordnung und der E-Datenschutz-Verordnung ab dem 25. Mai 2018 anwendbar sein.[538]

---

530 Art. 8 Abs. 1 des Verordnungsentwurfs (Fn. 510).
531 Art. 40 ff. DSGVO.
532 Art. 85 ff. DSGVO.
533 Art. 68 Abs. 3 DSGVO, Art. 58 Abs. 1 lit. k) des Verordnungsentwurfs (Fn. 510).
534 Art. 78 Abs. 3 , Art. 79 Abs. 2 DSGVO.
535 Art. 64 des Verordnungsentwurfs (Fn. 510).
536 Art. 65 des Verordnungsentwurfs (Fn. 510).
537 Vgl. Art. 67 des Verordnungsentwurfs (Fn. 510) gegenüber Art. 80 DSGVO.
538 Art. 73 Abs. 2 des Verordnungsentwurfs (Fn. 510).

4 Ausblick auf weitere Reformbestrebungen der EU im Bereich Datenschutz

Über die Gewährleistung des freien Flusses und des Schutzes personenbezogener Daten hinaus plant die Kommission, den EU-Binnenmarkt auch für Industriedaten, insbesondere von Rohdaten, die von Maschinen oder Sensoren generiert werden und keinen Personenbezug aufweisen, weiter voranzutreiben. Hierzu hat sie am 10. Januar 2017 parallel zu den Vorschlägen für eine neue E-Datenschutz-Verordnung und eine geänderte Verordnung betreffend die Datenverarbeitung durch EU-Organe auch eine „Mitteilung[539] über den Aufbau einer europäischen Datenwirtschaft" veröffentlicht. In dieser Mitteilung weist sie darauf hin, dass es derzeit an rechtlichen Regeln zum Schutz und zum freien Verkehr insbesondere von maschinengenerierten Daten ohne Personenbezug fehlt[540] und dass im Zuge der wachsenden Datenwirtschaft auch die Unsicherheit dahingehend wächst, wo solche Daten gespeichert oder verarbeitet werden dürfen.[541] Viele Mitgliedstaaten sehen insoweit – sei es gesetzlich oder durch verwaltungsrechtliche Regeln oder Praktiken – Einschränkungen vor, die möglicherweise ungerechtfertigt sind[542] und nach Auffassung der Kommission beseitigt werden müssen. In ihrer Mitteilung gibt die Kommission einen Überblick über rechtliche Hindernisse für den freien Fluss solcher Daten in der EU und stellt Überlegungen an, wie solche Beschränkungen abgebaut werden können. Um weitere Informationen darüber zu erhalten, in welchem Umfang digitale nicht personenbezogene maschinengenerierte Daten ausgetauscht bzw. gehandelt werden, welche Hindernisse aktuell hierfür bestehen (z.B. nationale Anforderungen, an welchem Ort solche Daten zu speichern oder zu verarbeiten sind)[543] und welche Haftungsfragen sich in den Bereichen „Internet der Dinge" und „Robotik" stellen, hat die Kommission zugleich eine öffentliche Konsultation[544] zu dieser Thematik gestartet. Man darf gespannt sein, ob es der EU neben dem Geflecht von Rechtsakten zum Schutz personenbezogener Daten auch gelingen wird, einen europäischen Rechtsrahmen für den Verkehr von Industriedaten zu schaffen, der die Industrie 4.0 in der EU ankurbeln wird.

539 https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy.
540 Communication (Fn. 539), S. 10.
541 Communication (Fn. 539), S. 3.
542 Communication (Fn. 539), S. 3.
543 Communication (Fn. 539), S. 3.
544 https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy.

Die Autorin:

Dr. Anja Hoffmann ist Wissenschaftliche Referentin im Fachbereich Binnenmarkt & Wettbewerb und Zivil- & Verfahrensrecht am Centrum für Europäische Politik.

cep | Centrum für Europäische Politik

Kaiser-Joseph-Straße 266 | D-79098 Freiburg

Telefon +49 761 38693-0 | www.cep.eu

Das cep ist der europapolitische Think Tank der gemeinnützigen Stiftung Ordnungspolitik. Es ist ein unabhängiges Kompetenzzentrum zur Recherche, Analyse und Bewertung von EU-Politik.