

HANDBUCH

Handbuch zum europäischen Datenschutzrecht

Ausgabe 2018



Das Manuskript für dieses Handbuch wurde im April 2018 fertiggestellt.

Künftige aktualisierte Fassungen werden auf der Webseite der FRA unter fra.europa.eu, der Webseite des Europarates unter coe.int/dataprotection, der Webseite des Europäischen Gerichtshofs für Menschenrechte unter echr.coe.int im „Case-Law“-Menü und der Webseite des Europäischen Datenschutzbeauftragten unter edps.europa.eu verfügbar sein.

Foto (Umschlag und Innenseiten): © iStockphoto

© Agentur der Europäischen Union für Grundrechte und Europarat, 2019

Nachdruck mit Quellenangabe gestattet.

Bei Verwendung oder Vervielfältigung von Fotos und Materialien, die nicht dem Urheberrecht der Agentur der Europäischen Union für Grundrechte oder des Europarates unterliegen, muss die Zustimmung direkt bei den Rechteinhabern eingeholt werden.

Weder die Agentur der Europäischen Union für Grundrechte/der Europarat noch irgendeine andere Person, die im Namen der Agentur der Europäischen Union für Grundrechte/des Europarates handelt, kann für die Verwendung der in diesem Handbuch enthaltenen Informationen verantwortlich gemacht werden.

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2019

Europarat: ISBN 978-92-871-9848-8

FRA – print: ISBN 978-92-9491-905-2

FRA – web: ISBN 978-92-9491-904-5

doi:10.2811/792433

doi:10.2811/704945

TK-05-17-225-DE-C

TK-05-17-225-DE-N

Printed by Imprimerie Centrale in Luxembourg

GEDRUCKT AUF CHLORFREI GEBLEICHTEM RECYCLINGPAPIER (PCF)



Dieses Handbuch wurde in englischer Sprache verfasst. Der Europarat und der Europäische Gerichtshof für Menschenrechte (EGMR) übernehmen keine Verantwortung für die Qualität der Übersetzungen in andere Sprachen. Die in diesem Handbuch zum Ausdruck gebrachten Ansichten sind für den Europarat und den EGMR nicht verbindlich. Das Handbuch bezieht sich auf ausgewählte Kommentare und Handbücher. Der Europarat und der EGMR übernehmen keine Verantwortung für deren Inhalt; des Weiteren stellt deren Aufnahme in diese Liste keine Billigung dieser Veröffentlichungen dar. Weitere Veröffentlichungen sind auf die Webseite der Bibliothek des EGMR angeführt: echr.coe.int/Library.

Der Inhalt dieses Handbuchs stellt keinen offiziellen Standpunkt des Europäischen Datenschutzbeauftragten (EDSB) dar und ist für die Ausübung der Zuständigkeiten des EDSB nicht verbindlich. Der EDSB übernimmt keine Verantwortung für die Qualität der Übersetzungen in andere Sprachen als Englisch.



Handbuch zum europäischen Datenschutzrecht

Ausgabe 2018

Vorwort

Die Digitalisierung in unseren Gesellschaften nimmt immer mehr zu. Angesichts dieser Veränderungen sind wir alle jeden Tag und in jeder erdenklichen Weise von dem Tempo der technologischen Entwicklungen sowie von der Art und Weise, wie personenbezogene Daten verarbeitet werden, betroffen. Kürzlich wurden die Rechtsrahmen der Europäischen Union (EU) und des Europarats, die den Schutz von Privatsphäre und personenbezogenen Daten sicherstellen, überarbeitet.

Europa nimmt beim Datenschutz weltweit eine führende Position ein. Die Datenschutzstandards der EU stützen sich auf das Übereinkommen Nr. 108 des Europarats, auf EU-Instrumente wie die Datenschutz-Grundverordnung und die Datenschutzrichtlinie für Polizei und Strafjustiz sowie auf die einschlägige Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Gerichtshofs der Europäischen Union.

Die von der EU und dem Europarat vorgenommenen Datenschutzreformen sind umfangreich und mitunter komplex und haben weitreichende Vorteile und Konsequenzen für den Einzelnen sowie für Unternehmen. Das vorliegende Handbuch soll das Bewusstsein stärken und das Wissen über Datenschutzvorschriften erweitern, insbesondere bei Angehörigen der Rechtsberufe, die nicht unbedingt Fachleute auf diesem Gebiet sind und sich im Rahmen ihrer Tätigkeit mit Datenschutzfragen befassen müssen.

Das Handbuch wurde von der Agentur der Europäischen Union für Grundrechte (FRA) in Zusammenarbeit mit dem Europarat (gemeinsam mit der Kanzlei des Europäischen Gerichtshofs für Menschenrechte) und dem Europäischen Datenschutzbeauftragten erarbeitet. Es bietet eine Aktualisierung der Ausgabe von 2014 und ist Teil einer Reihe von Handbüchern zu rechtlichen Themen, die die FRA und der Europarat gemeinsam verfasst haben.

Wir möchten uns bei den Datenschutzbehörden von Belgien, Estland, Frankreich, Georgien, Irland, Italien, Monaco, der Schweiz, Ungarns und des Vereinigten Königreichs für deren hilfreiche Rückmeldungen zum Entwurf des Handbuchs bedanken. Darüber hinaus möchten wir dem Referat Datenschutz und dem Referat Internationale Datenströme und Datenschutz der Europäischen Kommission unseren Dank aussprechen. Unser Dank gilt ebenfalls dem Gerichtshof

der Europäischen Union für seine Dokumentationshilfe bei der Abfassung dieses Handbuchs. Schließlich möchten wir dem Bayerischen Landesbeauftragten für den Datenschutz und der Sigmund Freud Privatuniversität Wien für wertvolle Hinweise zur deutschen Übersetzung danken.

Christos Giakoumopoulos

Generaldirektor Menschenrechte und Rechtsstaatlichkeit Europarat

Giovanni Buttarelli

Europäischer
Datenschutzbeauftragter

Michael O’Flaherty

Direktor der Agentur der Europäischen Union für Grundrechte

Inhaltsverzeichnis

VORWORT	3
ABKÜRZUNGEN UND AKRONYME	11
ZUR ANWENDUNG DIESES HANDBUCHS	13
1 KONTEXT UND HINTERGRUND DES EUROPÄISCHEN DATENSCHUTZRECHTS	17
1.1. Das Recht auf Schutz personenbezogener Daten	20
Kernpunkte	20
1.1.1. Das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten: eine kurze Einführung	20
1.1.2. Internationaler Rechtsrahmen: Vereinte Nationen	25
1.1.3. Europäische Menschenrechtskonvention	26
1.1.4. Übereinkommen Nr. 108 des Europarates	28
1.1.5. Das Datenschutzrecht der Europäischen Union	32
1.2. Einschränkungen des Rechts auf Schutz personenbezogener Daten	42
Kernpunkte	42
1.2.1. Anforderungen an einen rechtmäßigen Eingriff gemäß EMRK	43
1.2.2. Bedingungen für rechtmäßige Einschränkungen gemäß der EU-Charta	50
1.3. Interaktion mit anderen Rechten und berechtigten Interessen	62
Kernpunkte	62
1.3.1. Freiheit der Meinungsäußerung	63
1.3.2. Berufsgeheimnis	82
1.3.3. Religions- und Weltanschauungsfreiheit	85
1.3.4. Freiheit der Kunst und der Wissenschaft	87
1.3.5. Schutz des geistigen Eigentums	89
1.3.6. Datenschutz und wirtschaftliche Interessen	93
2 DATENSCHUTZTERMINOLOGIE	97
2.1. Personenbezogene Daten	99
Kernpunkte	99
2.1.1. Hauptaspekte des Konzepts der personenbezogenen Daten	100
2.1.2. Besondere Kategorien personenbezogener Daten	115
2.2. Datenverarbeitung	117
Kernpunkte	117
2.2.1. Der Begriff „Datenverarbeitung“	117
2.2.2. Automatisierte Datenverarbeitung	118
2.2.3. Nicht automatisierte Datenverarbeitung	120

2.3.	Verwender personenbezogener Daten	121
Kernpunkte		121
2.3.1.	Verantwortliche und Auftragsverarbeiter	121
2.3.2.	Empfänger und Dritte	132
2.4.	Einwilligung	134
Kernpunkte		134
3	KERNGRUNDSÄTZE DES EUROPÄISCHEN DATENSCHUTZRECHTS	137
3.1.	Die Grundsätze der Rechtmäßigkeit der Verarbeitung, der Verarbeitung nach Treu und Glauben und der Transparenz der Verarbeitung	139
Kernpunkte		139
3.1.1.	Rechtmäßigkeit der Verarbeitung	140
3.1.2.	Verarbeitung nach Treu und Glauben	141
3.1.3.	Transparenz der Verarbeitung	143
3.2.	Grundsatz der Zweckbindung	146
Kernpunkte		146
3.3.	Grundsatz der Datenminimierung	150
Kernpunkte		150
3.4.	Grundsatz der sachlichen Richtigkeit der Daten	152
Kernpunkte		152
3.5.	Grundsatz der Speicherbegrenzung	154
Kernpunkt		154
3.6.	Grundsatz der Datensicherheit	156
Kernpunkte		156
3.7.	Grundsatz der Verantwortlichkeit (Rechenschaftspflicht)	160
Kernpunkte		160
4	VORSCHRIFTEN DES EUROPÄISCHEN DATENSCHUTZRECHTS	165
4.1.	Vorschriften über die Rechtmäßigkeit der Verarbeitung	168
Kernpunkte		168
4.1.1.	Rechtmäßige Gründe für die Datenverarbeitung	168
4.1.2.	Verarbeitung besonderer Datenkategorien (sensible Daten)	189
4.2.	Vorschriften über die Sicherheit der Verarbeitung	196
Kernpunkte		196
4.2.1.	Elemente der Datensicherheit	197
4.2.2.	Vertraulichkeit	201
4.2.3.	Meldungen von Verletzungen des Schutzes personenzbezogener Daten	204

4.3.	Vorschriften über den Grundsatz der Verantwortlichkeit und über die Förderung der Einhaltung der Vorschriften	207
	Kernpunkte	207
4.3.1.	Datenschutzbeauftragte	208
4.3.2.	Verzeichnis von Verarbeitungstätigkeiten	212
4.3.3.	Datenschutz-Folgenabschätzung und vorherige Konsultation	214
4.3.4.	Verhaltensregeln	217
4.3.5.	Zertifizierung	219
4.4.	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	220
5	UNABHÄNGIGE AUFSICHT	223
	Kernpunkte	224
5.1.	Unabhängigkeit	228
5.2.	Zuständigkeit und Befugnisse	231
5.3.	Zusammenarbeit	235
5.4.	Der Europäische Datenschutzausschuss	237
5.5.	Das Kohärenzverfahren der DSGVO	239
6	RECHTE BETROFFENER PERSONEN UND IHRE DURCHSETZUNG	241
6.1.	Rechte der betroffenen Personen	245
	Kernpunkte	245
6.1.1.	Recht auf Information	246
6.1.2.	Recht auf Berichtigung	261
6.1.3.	Recht auf Löschung („Recht auf Vergessenwerden“)	263
6.1.4.	Recht auf Einschränkung der Verarbeitung	270
6.1.5.	Recht auf Datenübertragbarkeit	271
6.1.6.	Widerspruchsrecht	272
6.1.7.	Automatisierte Entscheidungen im Einzelfall einschließlich Profiling	277
6.2.	Rechtsbehelfe, Haftung, Sanktionen und Schadensersatz	281
	Kernpunkte	281
6.2.1.	Recht eine Beschwerde bei einer Aufsichtsbehörde einzureichen	282
6.2.2.	Recht auf wirksamen gerichtlichen Rechtsbehelf	284
6.2.3.	Haftung und Recht auf Schadensersatz	293
6.2.4.	Sanktionen	294
7	INTERNATIONALE DATENÜBERMITTLUNGEN UND FREIER VERKEHR PERSONENBEZOGENER DATEN	297
7.1.	Wesen der Übermittlung personenbezogener Daten	299
	Kernpunkte	299

7.2.	Freier Verkehr personenbezogener Daten zwischen Mitgliedstaaten oder zwischen Vertragsparteien	300
Kernpunkt		300
7.3.	Übermittlung personenbezogener Daten an Drittländer/Nicht-Vertragsparteien und internationale Organisationen	302
Kernpunkte		302
7.3.1.	Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses	303
7.3.2.	Datenübermittlung vorbehaltlich geeigneter Garantien	308
7.3.3.	Ausnahmen für bestimmte Fälle	314
7.3.4.	Datenübermittlung auf Grundlage internationaler Abkommen	317
8	DATENSCHUTZ IN DEN BEREICHEN POLIZEI UND STRAFJUSTIZ	323
8.1.	Datenschutzrecht des Europarates im Bereich nationale Sicherheit, Polizei und Strafjustiz	325
Kernpunkte		325
8.1.1.	Die Polizei-Empfehlung	327
8.1.2.	Das Budapester Übereinkommen über Computerkriminalität	333
8.2.	EU-Datenschutzrecht im Bereich Polizei und Strafjustiz	334
Kernpunkte		334
8.2.1.	Datenschutzrichtlinie für Polizei- und Strafverfolgungsbehörden	335
8.3.	Sonstige spezifische Rechtsinstrumente für den Datenschutz im Bereich der Strafverfolgung	346
8.3.1.	Datenschutz in den Justiz- und Strafverfolgungsbehörden der EU	356
8.3.2.	Datenschutz in den gemeinsamen Informationssystemen auf EU-Ebene	366
9	BESONDERE ARTEN VON DATEN UND IHRE ENTSPRECHENDEN DATENSCHUTZVORSCHRIFTEN	385
9.1.	Elektronische Kommunikation	386
Kernpunkte		386
9.2.	Beschäftigtendaten	391
Kernpunkte		391
9.3.	Gesundheitsdaten	396
Kernpunkte		396
9.4.	Datenverarbeitung für Forschungszwecke und statistische Zwecke	402
Kernpunkte		402
9.5.	Finanzdaten	406
Kernpunkte		406

10 MODERNE HERAUSFORDERUNGEN BEIM SCHUTZ	
PERSONENBEZOGENER DATEN	411
10.1. Big Data, Algorithmen und künstliche Intelligenz	414
Kernpunkte	414
10.1.1. Definition der Begriffe „Big Data“, „Algorithmen“ und „künstliche Intelligenz“	415
10.1.2. Abwägung der Vorteile und Risiken von Big Data	418
10.1.3. Probleme im Zusammenhang mit dem Datenschutz	421
10.2. Das Web 2.0 und das Web 3.0: Soziale Netzwerke und das Internet der Dinge	428
Kernpunkte	428
10.2.1. Bestimmung der Begriffe „Web 2.0“ und „Web 3.0“	428
10.2.2. Abwägung der Vorteile und Risiken	431
10.2.3. Datenschutzthemen	433
WEITERFÜHRENDE LITERATUR	441
VERZEICHNIS DER RECHTSSACHEN	449
Ausgewählte Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte	449
Ausgewählte Rechtsprechung des Gerichtshofs der Europäischen Union	455
INDEX	461

Abkürzungen und Akronyme

ABl.	Amtsblatt der Europäischen Union
AEMR	Allgemeine Erklärung der Menschenrechte
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
C.SIS	Zentrale Unterstützungseinheit des Schengener Informationssystems
CCTV	Closed circuit television (Videoüberwachungsanlage)
Charta	Charta der Grundrechte der Europäischen Union
CRM	Customer relations management (Kundenbeziehungsmanagement)
DSB	Datenschutzbeauftragter
DSGV	Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EFSA	Europäische Behörde für Lebensmittelsicherheit
EFTA	Europäische Freihandelsassoziation
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
ENISA	Europäische Agentur für Netz- und Informationssicherheit
ENU	Nationale Europol-Stelle
ESMA	Europäische Wertpapier- und Marktaufsichtsbehörde
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union (bis Dezember 2009 als Europäischer Gerichtshof bezeichnet)
EuHb	Europäischer Haftbefehl
eu-LISA	Europäische Agentur für IT-Großsysteme
EuroPriSe	Europäisches Datenschutzgütesiegel
EUStA	Europäische Staatsanwaltschaft
EUV	Vertrag über die Europäische Union

EWR	Europäischer Wirtschaftsraum
FRA	Agentur der Europäischen Union für Grundrechte
GKI	Gemeinsame Kontrollinstanz
GPS	Global positioning system (weltweites Ortungssystem über Satelliten)
IKT	Informations- und Kommunikationstechnologie
IPBPR	Internationaler Pakt über bürgerliche und politische Rechte
N.SIS	Nationaler Teil des Schengener Informationssystems
NRO	Nichtregierungsorganisation
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PIN	Persönliche Identifikationsnummer
PNR	Passenger Name Record (Fluggastdatensätze)
SCG	Supervision Coordination Group (Koordinierungsgruppe für die Aufsicht)
SEPA	Single Euro Payments Area (Einheitlicher Euro-Zahlungsverkehrsraum)
SEV	Sammlung der Europaratsverträge
SIS	Schengener Informationssystem
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEN-Tele	Transeuropäische Telekommunikationsnetze
Übereinkommen Nr. 108	Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten. Das Änderungsprotokoll (SEV Nr. 223) zu dem Übereinkommen 108 ("Modernisiertes Übereinkommen 108") wurde vom Ministerkomitee des Europarats bei seiner 128. Sitzung angenommen, die in Elsinore, Dänemark am 17. und 18. Mai 2018 stattfand. Verweise auf das "Modernisierte Übereinkommen 108" beziehen sich auf das Übereinkommen in seiner Änderung durch das Protokoll SEV Nr. 223.
UN	Vereinte Nationen
VIS	Visa-Informationssystem
ZIS	Zollinformationssystem

Zur Anwendung dieses Handbuchs

Dieses Handbuch bietet einen Überblick über die seitens der Europäischen Union (EU) und des Europarates festgesetzten Rechtsnormen in Bezug auf den Datenschutz. Es soll Angehörigen von Rechtsberufen Hilfestellung bieten, die nicht auf den Bereich Datenschutz spezialisiert sind, einschließlich Rechtsanwälten,¹ Richtern oder Angehörigen anderer Rechtsberufe, sowie Personen, die für andere Einrichtungen einschließlich Nichtregierungsorganisationen (NRO) arbeiten und sich möglicherweise mit rechtlichen Fragen im Zusammenhang mit Datenschutz auseinandersetzen müssen.

Das Handbuch dient als vorrangige Informationsquelle zum einschlägigen EU-Recht und zur Europäischen Menschenrechtskonvention (EMRK), sowie zum Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) und zu anderen Instrumenten des Europarates.

Die Kapitel beginnen grundsätzlich mit einer Tabelle, aus der die einschlägigen Rechtsvorschriften für die im jeweiligen Kapitel behandelten Themen hervorgehen. Die Tabelle behandelt sowohl das Recht des Europarates als auch das EU-Recht und enthält eine Auswahl der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) und des Gerichtshofs der Europäischen Union (EuGH). Anschließend werden die einschlägigen Rechtsvorschriften dieser beiden unterschiedlichen europäischen Systeme entsprechend ihrer Relevanz für die jeweils behandelten Themen nacheinander vorgestellt. So kann der Leser erkennen, in welchen Punkten sich die beiden Rechtssysteme decken und wo die Unterschiede liegen. Damit soll den Lesern das Auffinden der wichtigsten, auf ihre Situation zutreffenden Informationen erleichtert werden, vor allem, wenn sie nur dem Recht des Europarates unterliegen. In einigen Kapiteln, wenn dies einer präzisen Darstellung des Inhalts dienlich ist, kann die Reihenfolge der Themen in den Tabellen leicht von der Reihenfolge der Themen im Kapitel selbst abweichen. Überdies liefert das Handbuch auch einen kurzen Überblick über den Rechtsrahmen der Vereinten Nationen.

Juristen in Nicht-EU-Ländern, die jedoch Mitgliedstaaten des Europarates und damit Vertragsparteien der EMRK und des Übereinkommens Nr. 108 sind,

¹ Im Interesse einer besseren Lesbarkeit verzichtet dieses Handbuch auf die durchgehende Nennung der männlichen und weiblichen Form, auch wenn selbstverständlich alle Geschlechter gemeint sind.

können direkt zu den auf den Europarat bezogenen Abschnitten übergehen, die die für ihr Land relevanten Informationen enthalten. Juristen in Nicht-EU-Ländern müssen darüber hinaus berücksichtigen, dass die Datenschutzvorschriften der EU seit der Annahme der Datenschutz-Grundverordnung der EU für nicht in der EU ansässige Organisationen und sonstige Stellen gelten, sofern diese personenbezogene Daten verarbeiten und betroffenen Personen in der Union Waren und Dienstleistungen anbieten oder deren Verhalten überwachen.

Für Juristen aus EU-Mitgliedstaaten sind beide Abschnitte relevant, da in diesen Ländern beide Rechtssysteme gelten. Es sollte beachtet werden, dass die sowohl im Rahmen des Europarates (Modernisiertes Übereinkommen Nr. 108 in seiner Änderung durch das Protokoll SEV Nr. 223) als auch im Rahmen der EU (Annahme der Datenschutz-Grundverordnung und der Richtlinie (EU) 2016/680) erfolgten Reformen und Modernisierungen parallel durchgeführt wurden. Die Regulierungsbehörden in beiden Rechtssystemen haben sich größte Mühe gegeben, die Kohärenz und Vereinbarkeit der beiden Rechtsrahmen zu gewährleisten. Folglich haben die Reformen eine größere Harmonisierung zwischen dem Datenschutzrecht des Europarates und dem Datenschutzrecht der EU geschaffen. Werden weitere Informationen zu einem bestimmten Thema benötigt, befindet sich im Abschnitt „Weiterführende Literatur“ eine Liste mit fachspezifischerem Material. Informationen zu den Bestimmungen des Übereinkommens 108 und seines Zusatzprotokolls aus dem Jahr 2001, die bis zum Inkrafttreten des Änderungsprotokolls weiter gelten, sind der 2014 veröffentlichten Ausgabe dieses Handbuchs zu entnehmen.

Das Recht des Europarates wird anhand von kurzen Bezugnahmen auf ausgewählte Rechtssachen vor dem EGMR vorgestellt. Diese Rechtssachen wurden aus den zahlreichen vorhandenen Urteilen und Entscheidungen des EGMR zu Datenschutzfragen ausgewählt.

Das einschlägige EU-Recht umfasst angenommene Rechtsakte, einschlägige Bestimmungen der EU-Verträge und die Charta der Grundrechte der Europäischen Union, die der EuGH in seiner Rechtsprechung ausgelegt hat. Darüber hinaus stellt das Handbuch Stellungnahmen und Leitlinien vor, die seitens der Artikel-29-Datenschutzgruppe angenommen wurden, dem gemäß der Datenschutzrichtlinie mit der Bereitstellung fachkundiger Beratung an die EU-Mitgliedstaaten beauftragten Beratungsgremium, das ab 25. Mai 2018 durch den Europäischen Datenschutzausschuss (EDSA) ersetzt wird. Stellungnahmen des Europäischen Datenschutzbeauftragten liefern überdies wichtige Einblicke in die Auslegung des EU-Rechts und wurden daher in dieses Handbuch aufgenommen.

Die in diesem Handbuch genannten Rechtssachen oder Zitate daraus stellen Beispiele der umfangreichen Rechtsprechung sowohl seitens des EGMR als auch des EuGH dar. Die Anleitungen am Ende des Handbuchs dienen dem Leser als Unterstützung für die Online-Suche nach Rechtssachen. Die dargelegte Rechtsprechung des EuGH bezieht sich auf die frühere Datenschutzrichtlinie. Die Auslegungen des EuGH finden jedoch auf die in der Datenschutz-Grundverordnung festgesetzten entsprechenden Rechte und Pflichten weiterhin Anwendung.

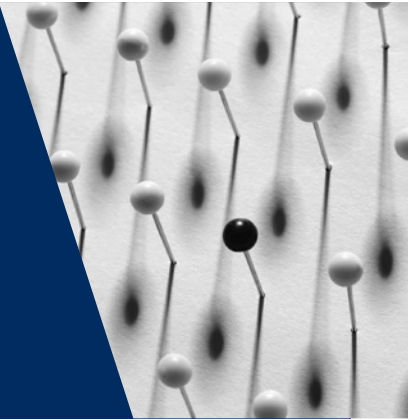
Darüber hinaus werden in Textkästchen mit blauem Hintergrund praktische Hinweise zu hypothetischen Szenarien gegeben. Diese dienen der näheren Illustration der Anwendung der europäischen Datenschutzvorschriften in der Praxis, insbesondere zu Themen, zu denen es keine einschlägige Rechtsprechung des EGMR oder des EuGH gibt. Die Textkästchen mit grauem Hintergrund liefern Beispiele aus anderen Quellen als der Rechtsprechung des EGMR und des EuGH, wie beispielsweise der Rechtsprechung und den Stellungnahmen der Artikel-29-Datenschutzgruppe.

Das Handbuch enthält eine Einführung, in der die Rolle der beiden Rechtssysteme, die auf dem EU-Recht und der EMRK gründen, kurz vorgestellt wird ([Kapitel 1](#)). Die [Kapitel 2](#) bis 10 befassen sich mit folgenden Themen:

- Datenschutzterminologie;
- Kerngrundsätze des europäischen Datenschutzrechts;
- Vorschriften des europäischen Datenschutzrechts;
- unabhängige Aufsicht;
- Rechte betroffener Personen und ihre Durchsetzung;
- grenzüberschreitende Übermittlung und grenzüberschreitender Verkehr personenbezogener Daten;
- Datenschutz in den Bereichen Polizei und Strafjustiz;
- sonstige europäische Datenschutzvorschriften für spezifische Bereiche;
- moderne Herausforderungen beim Schutz personenbezogener Daten.

1

Kontext und Hintergrund des europäischen Datenschutzrechts



EU	Behandelte Themen	Europarat
Das Recht auf Datenschutz		
Vertrag über die Arbeitsweise der Europäischen Union, Artikel 16 Charta der Grundrechte der Europäischen Union (die Charta), Artikel 8 (Recht auf Schutz personenbezogener Daten) Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie), ABl. L 281 vom 23.11.1995 (bis Mai 2018 in Kraft) Rahmenbeschluss 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12.2008 (bis Mai 2018 in Kraft) Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO), ABl. L 119 vom 4.5.2016		EMRK, Artikel 8 (Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz) Modernisiertes Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Modernisiertes Übereinkommen Nr. 108)

EU	Behandelte Themen	Europarat
Richtlinie (EU) 2016/680 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 (Datenschutz für Polizei- und Strafverfolgungsbehörden), ABl. L 119 vom 4.5.2016 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 31.7.2002 Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (Datenschutzverordnung der EU-Organe), ABl. L 8 vom 12.1.2001		
Einschränkungen des Rechts auf Schutz personenbezogener Daten		
Die Charta, Artikel 52 Absatz 1 DSGVO, Artikel 23 EuGH, Verbundene Rechtssachen C-92/09 und C-93/09, <i>Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen</i> [GK], 2010		EMRK, Artikel 8 Absatz 2 Modernisiertes Übereinkommen Nr. 108, Artikel 9 EGMR, <i>S. und Marper / Vereinigtes Königreich</i> [GK], Nrn. 30562/04 und 30566/04, 2008
Abwägen von Rechten		
EuGH, Verbundene Rechtssachen C-92/09 und C-93/09, <i>Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen</i> [GK], 2010	Allgemein	

EU	Behandelte Themen	Europarat
EuGH, C-73/07, <i>Tietosuoja ja valtuutus / Satakunnan Markkinapörssi Oy und Satamedia Oy</i>, 2008 EuGH, C-131/12, <i>Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [GK], 2014	Freiheit der Meinungsäußerung	EGMR, <i>Axel Springer AG / Deutschland</i> [GK], Nr. 39954/08, 2012 EGMR, <i>Mosley / Vereinigtes Königreich</i>, Nr. 48009/08, 2011 EGMR, <i>Bohlen / Deutschland</i>, Nr. 53495/09, 2015
EuGH, C-28/08 P, <i>Europäische Kommission / The Bavarian Lager Co. Ltd.</i> [GK], 2010 EuGH, C-615/13P, <i>ClientEarth, PAN Europe / EFSA</i>, 2015	Zugang zu Dokumenten	EGMR, <i>Magyar Helsinki Bizottság / Ungarn</i> [GK], Nr. 18030/11, 2016
DSGVO, Artikel 90	Berufsgeheimnis	EGMR, <i>Pruteanu / Rumänien</i>, Nr. 30181/05, 2015
DSGVO, Artikel 91	Religions- und Weltanschauungsfreiheit	
	Freiheit von Kunst und Wissenschaft	EGMR, <i>Vereinigung bildender Künstler / Österreich</i>, Nr. 68345/01, 2007
EuGH, C-275/06, <i>Productores de Música de España (Promusicae) / Telefónica de España SAU</i> [GK], 2008	Schutz des Eigentums	
EuGH, C-131/12, <i>Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [GK], 2014. EuGH, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni</i>, 2017	Wirtschaftliche Rechte	

1.1. Das Recht auf Schutz personenbezogener Daten

Kernpunkte

- Gemäß Artikel 8 EMRK ist das Recht einer Person auf Schutz bei der Verarbeitung personenbezogener Daten Teil des Rechts auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz.
- Das Übereinkommen Nr. 108 des Europarates ist das erste und bislang einzige international verbindliche Instrument, das sich mit dem Datenschutz beschäftigt. Das Übereinkommen wurde einem Modernisierungsprozess unterzogen, der mit der Annahme des Änderungsprotokolls SE Nr. 223 abgeschlossen wurde.
- Nach EU-Recht ist das Recht auf Datenschutz als eigenständiges Grundrecht anerkannt. Es ist in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union und in Artikel 8 der Charta der Grundrechte der EU bekräftigt.
- Im EU-Recht wurde der Datenschutz erstmals 1995 in der Datenschutzrichtlinie geregelt.
- In Anbetracht der schnellen technologischen Entwicklungen nahm die EU 2016 eine neue Gesetzgebung zur Anpassung der Datenschutzvorschriften an das digitale Zeitalter an. Die Datenschutz-Grundverordnung trat im Mai 2018 in Kraft und hob die Datenschutzrichtlinie auf.
- Zusammen mit der Datenschutz-Grundverordnung nahm die EU eine Gesetzgebung in Bezug auf die Verarbeitung personenbezogener Daten durch staatliche Behörden zu Strafverfolgungszwecken an. Die Richtlinie (EU) 2017/680 setzt die Datenschutzvorschriften und Datenschutzgrundsätze fest, die die Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung regeln.

1.1.1. Das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten: eine kurze Einführung

Obgleich das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten eng miteinander verbunden sind, handelt es sich dabei um eigenständige Rechte. Das Recht auf Privatsphäre, das im europäischen Recht als Recht auf Achtung des Privatlebens bezeichnet wird, tauchte in den internationalen Menschenrechtsnormen in der im Jahre 1948 angenommenen

Allgemeinen Erklärung der Menschenrechte (AEMR) als eines der grundlegend geschützten Menschenrechte auf. Kurz nach der Annahme der AEMR bekräftigte auch Europa dieses Recht in der Europäischen Menschenrechtskonvention (EMRK), einem Vertrag, der für seine Vertragsparteien rechtsverbindlich ist und im Jahre 1950 verfasst wurde. Die EMRK sieht vor, dass jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz hat. Das Eingreifen in dieses Recht seitens einer Behörde ist verboten, es sei denn der Eingriff ist gesetzlich vorgesehen, verfolgt wichtige und berechtigte öffentliche Interessen und ist in einer demokratischen Gesellschaft notwendig.

Die Annahme der AEMR und der EMRK erfolgte lange vor der Entwicklung von Computern und des Internets und dem Aufkommen der Informationsgesellschaft. Diese Entwicklungen brachten für die Menschen und die Gesellschaft erhebliche Vorteile mit sich, durch die die Lebensqualität, die Leistungsfähigkeit und die Produktivität verbessert wurden. Gleichzeitig stellen sie jedoch auch neue Risiken für das Recht auf Achtung des Privatlebens dar. Als Reaktion auf den Bedarf nach speziellen Vorschriften zur Regelung der Erhebung und Verwendung personenbezogener Informationen kam ein neues Konzept der Privatsphäre auf, das in einigen Rechtsprechungen als „informationelle Selbstbestimmung“ und in anderen als „Recht auf informationelle Selbstbestimmung“ bekannt ist.² Dieses Konzept führte zur Entwicklung spezieller Rechtsvorschriften für den Schutz personenbezogener Daten.

Der Datenschutz in Europa begann in den 1970er Jahren mit der in einigen Staaten erfolgten Annahme von Rechtsvorschriften zur Überwachung der Verarbeitung personenbezogener Informationen seitens Behörden und großer Firmen.³ Danach wurden auf europäischer Ebene Datenschutzinstrumente eingerichtet⁴

- 2 In einem Urteil aus dem Jahr 1983 bestätigte das deutsche Bundesverfassungsgericht ein Recht auf informationelle Selbstbestimmung, *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Das Gericht war der Ansicht, dass sich die informationelle Selbstbestimmung von dem im deutschen Grundgesetz geschützten Grundrecht auf Achtung der Persönlichkeit ableitet. Der EGMR erkannte in einem Urteil aus dem Jahr 2017 an, dass Artikel 8 EMRK „das Recht auf eine Form der informationellen Selbstbestimmung vorsieht“. Siehe EGMR, *Satakunnan Markkinapörssi Oy und Satamedia Oy / Finland*, Nr. 931/13, 27. Juni 2017, Randnr. 137.
- 3 Das deutsche Bundesland Hessen nahm im Jahr 1970 das erste Gesetz zum Datenschutz an, das nur in diesem Bundesland galt. Schweden nahm 1973 das weltweit erste nationale Datenschutzgesetz an. Bis Ende der 1980er Jahre hatten mehrere europäische Staaten (Frankreich, Deutschland, die Niederlande und das Vereinigte Königreich) ebenfalls Rechtsvorschriften zum Datenschutz angenommen.
- 4 Das Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) wurde 1981 angenommen. Die EU nahm 1995 ihr erstes umfassendes Datenschutzinstrument an: Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

und im Laufe der Jahre entwickelte sich der Datenschutz zu einem eigenständigen Wert, der nicht mehr lediglich unter dem Recht auf Achtung der Privatsphäre subsumiert wurde. Das Rechtssystem der EU erkennt den Datenschutz neben dem Grundrecht auf Achtung des Privatlebens als eigenständiges Grundrecht an. Diese Trennung wirft die Frage nach der Beziehung und den Unterschieden zwischen diesen beiden Rechten auf.

Das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten sind eng miteinander verbunden. Beide streben nach dem Schutz ähnlicher Werte, sprich der Autonomie und der menschlichen Würde der Personen, indem sie ihnen eine persönliche Sphäre zugestehen, in der sie ihre Persönlichkeiten frei entwickeln, denken und sich ihre Meinungen bilden können. Folglich stellen sie eine wesentliche Voraussetzung für die Ausübung anderer Grundfreiheiten dar, wie der Freiheit der Meinungsäußerung, der Versammlungs- und Vereinigungsfreiheit und der Religionsfreiheit.

Die beiden Rechte unterscheiden sich in ihrer Formulierung und in ihrem Anwendungsbereich. Das Recht auf Achtung des Privatlebens besteht aus einem allgemeinen Eingriffsverbot, vorbehaltlich einiger Kriterien des öffentlichen Interesses, die das Eingreifen in bestimmten Fällen rechtfertigen können. Der Schutz personenbezogener Daten wird als modernes und aktives Recht betrachtet,⁵ das ein System von „checks and balances“ einrichtet, um die Personen bei jeder Verarbeitung der sie betreffenden personenbezogenen Daten zu schützen. Die Verarbeitung muss mit den wesentlichen Bestandteilen des Schutzes personenbezogener Daten übereinstimmen, und zwar mit der unabhängigen Aufsicht und der Achtung der Rechte der betroffenen Person.⁶

Artikel 8 der Charta der Grundrechte der EU (die Charta) bekräftigt nicht nur das Recht auf Schutz personenbezogener Daten, sondern legt auch die mit diesem Recht verbundenen zentralen Werte dar. Er sieht vor, dass die Verarbeitung personenbezogener Daten nach Treu und Glauben, für festgelegte Zwecke

5 Generalanwältin Sharpston beschrieb die Rechtssache so, dass es dabei um zwei verschiedene Rechte geht: ein „klassisches Recht“ auf den Schutz der Privatsphäre und ein eher „modernes“ Recht, das Recht auf Datenschutz. Siehe EuGH, Verbundene Rechtssachen C-92/09 und C-93/02, *Volker und Markus Schecke GbR / Land Hessen, Schlussanträge der Generalanwältin Eleanor Sharpston*, 17. Juni 2010, Randnr. 71.

6 Hustinx, P., EDSB Vorträge & Artikel, *EU-Datenschutzrecht: Die Überprüfung der Richtlinie 95/46/EG und die vorgeschlagene Datenschutz-Grundverordnung*, Juli 2013.

und mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage erfolgen muss. Personen müssen das Recht haben, Auskunft über ihre personenbezogenen Daten zu erhalten und die Berichtigung der Daten zu erwirken, und die Einhaltung dieses Rechts ist von einer unabhängigen Stelle zu überwachen.

Das Recht auf Schutz personenbezogener Daten kommt immer dann zum Tragen, wenn personenbezogene Daten verarbeitet werden; folglich ist es weiter gefasst als das Recht auf Achtung des Privatlebens. Jede Verarbeitung personenbezogener Daten unterliegt einem angemessenen Schutz. Der Datenschutz betrifft alle Arten von personenbezogenen Daten und Datenverarbeitung, unabhängig von deren Zusammenhang mit der Privatsphäre und deren Auswirkungen auf diese. Wie in den nachstehenden Beispielen verdeutlicht, kann die Verarbeitung personenbezogener Daten auch das Recht auf Privatleben verletzen. Gleichwohl muss eine Verletzung des Privatlebens nicht nachgewiesen werden, um die Datenschutzvorschriften auszulösen.

Das Recht auf Privatsphäre betrifft Situationen, in denen ein privates Interesse oder das „Privatleben“ einer Person beeinträchtigt wurde. Wie im gesamten Handbuch dargelegt, wurde das Konzept des „Privatlebens“ in der Rechtsprechung weit ausgelegt und umfasst intime Situationen, sensible oder vertrauliche Informationen, Informationen, die die Wahrnehmung einer Person seitens der Öffentlichkeit beeinträchtigen könnten, und selbst Aspekte des Berufslebens und des Verhaltens einer Person in der Öffentlichkeit. Die Beurteilung, ob ein Eingriff in das „Privatleben“ vorliegt oder vorlag, hängt jedoch vom Kontext und den Sachverhalten jedes Einzelfalls ab.

Jeder Vorgang, der die Bearbeitung personenbezogener Daten beinhaltet, könnte hingegen in den Anwendungsbereich der Datenschutzvorschriften fallen und das Recht auf Schutz personenbezogener Daten auslösen. Wenn ein Arbeitgeber beispielsweise Informationen über die Namen und die Vergütung seiner Beschäftigten aufzeichnet, kann die bloße Aufzeichnung dieser Informationen nicht als Eingriff in das Privatleben betrachtet werden. Ein solcher Eingriff könnte jedoch geltend gemacht werden, sofern der Arbeitgeber die personenbezogenen Informationen der Beschäftigten beispielsweise an Dritte übermittelt. In jedem Fall müssen Arbeitgeber die Datenschutzvorschriften befolgen, da die Aufzeichnung von Informationen über die Beschäftigten eine Datenverarbeitung darstellt.

Beispiel: In der Rechtssache *Digital Rights Ireland*⁷ musste der EuGH über die Gültigkeit der Richtlinie 2006/24/EG in Anbetracht der in der Charta der Grundrechte der EU bekräftigten Grundrechte auf Schutz personenbezogener Daten und Achtung des Privatlebens entscheiden. Die Richtlinie verpflichtete die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder die Betreiber öffentlicher Kommunikationsnetze, die Telekommunikationsdaten der Bürger über einen Zeitraum von bis zu zwei Jahren auf Vorrat zu speichern, um zu gewährleisten, dass diese Daten zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Die Maßnahme betraf ausschließlich Metadaten, Standortdaten und Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind. Sie galt nicht für den Inhalt elektronischer Nachrichtenübermittlungen.

Nach Ansicht des EuGH griff die Richtlinie in das Grundrecht auf Schutz personenbezogener Daten ein, „da sie eine Verarbeitung personenbezogener Daten vorsieht“.⁸ Darüber hinaus stellte er fest, dass die Richtlinie in das Recht auf Achtung des Privatlebens eingriff.⁹ Aus der Gesamtheit der gemäß der Richtlinie auf Vorrat gespeicherten personenbezogenen Daten, die den zuständigen Behörden zugänglich gemacht werden könnten, könnten „sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.“¹⁰ Der Eingriff in die beiden Rechte sei von großem Ausmaß und besonders schwerwiegend.

Der EuGH erklärte die Richtlinie 2006/24/EG für ungültig und stellte fest, dass obgleich die Richtlinie ein berechtigtes Ziel verfolge, der Eingriff in das Recht auf Schutz personenbezogener Daten und in das Recht auf Achtung des Privatlebens schwerwiegend und nicht auf das absolut Notwendige beschränkt sei.

7 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere* und *Kärntner Landesregierung und andere* [GK], 8 April 2014.

8 a.a.O., Randnr. 36.

9 a.a.O., Randnrn. 32–35.

10 a.a.O., Randnr. 27.

1.1.2. Internationaler Rechtsrahmen: Vereinte Nationen

Der Rechtsrahmen der Vereinten Nationen erkennt den Schutz personenbezogener Daten nicht als Grundrecht an, obgleich das Recht auf Privatsphäre im internationalen Rechtssystem ein seit langem bestehendes Grundrecht ist. Das Recht einer Person auf den Schutz ihrer Privatsphäre vor dem Eindringen anderer, insbesondere des Staates, wurde völkerrechtlich zum ersten Mal in Artikel 12 AEMR über die Wahrung von Privat- und Familienleben verankert.¹¹ Obgleich es sich bei der AEMR um eine unverbindliche Erklärung handelt, verfügt sie über einen hohen Stellenwert als Gründungsinstrument der internationalen Menschenrechtsnormen und beeinflusste die Entwicklung anderer Menschenrechtsinstrumente in Europa. Der im Jahre 1976 in Kraft getretene Internationale Pakt über bürgerliche und politische Rechte (IPBPR) proklamiert, dass niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden darf. Der IPBPR ist ein internationaler Vertrag, der 169 Parteien zur Achtung und zur Gewährleistung der Ausübung der bürgerlichen Rechte der Einzelnen verpflichtet, zu denen auch die Privatsphäre zählt.

Seit 2013 nahmen die Vereinten Nationen als Reaktion auf die Entwicklung neuer Technologien und die Enthüllungen über die in einigen Staaten erfolgende Massenüberwachung (Snowden-Enthüllungen) zwei Resolutionen zum Thema Privatsphäre mit dem Titel „das Recht auf Privatsphäre im digitalen Zeitalter“¹² an. Sie verurteilen die Massenüberwachung auf das Schärfste und heben die Auswirkungen hervor, die eine solche Überwachung auf die Grundrechte auf Privatsphäre und auf die Freiheit der Meinungsäußerung sowie auf die Funktionsweise einer lebendigen und demokratischen Gesellschaft haben kann. Wenngleich diese Resolutionen nicht rechtsverbindlich sind, entfachten sie weltweit eine bedeutende hochkarätige politische Debatte zum Thema Privatsphäre, neue Technologien und Überwachung. Sie führten auch zur Einrichtung eines Sonderberichterstatters über das Recht auf Privatsphäre, dessen Auftrag in der Förderung und im Schutz dieses Rechtes besteht. Zu den konkreten Aufgaben des Berichterstatters zählen die Sammlung von Informationen

11 Vereinte Nationen (UN), *Allgemeine Erklärung der Menschenrechte (AEMR)*, 10. Dezember 1948.

12 Siehe UN, Generalversammlung, *Resolution on the right to privacy in the digital age*, A/RES/68/167, New York, 18. Dezember 2013; und UN, Generalversammlung, *Revised draft resolution on the right to privacy in the digital age*, A/C.3/69/L.26/Rev.1, New York, 19. November 2014.

über die nationalen Praktiken und Erfahrungen im Zusammenhang mit der Privatsphäre und den aus den neuen Technologien entstehenden Herausforderungen, der Austausch und die Förderung von bewährten Vorgehensweisen und die Ermittlung potentieller Hindernisse.

Während sich die früheren Resolutionen auf die negativen Auswirkungen der Massenüberwachung und die Verantwortung der Staaten zur Einschränkung der Befugnisse der Nachrichtendienste konzentrierten, spiegeln die neueren Resolutionen eine entscheidende Entwicklung in der Debatte um die Privatsphäre in den Vereinten Nationen wider.¹³ Die in den Jahren 2016 und 2017 angenommenen Resolutionen bekräftigen das Erfordernis zur Einschränkung der Befugnisse der Nachrichtendienste und verurteilen die Massenüberwachung. Sie geben jedoch auch ausdrücklich an, dass „die zunehmenden Möglichkeiten der Unternehmen zur Erhebung, Verarbeitung und Verwendung personenbezogener Daten im digitalen Zeitalter eine Gefahr für den Genuss des Rechts auf Privatsphäre darstellen können“. Zusätzlich zur Verantwortung der staatlichen Behörden weisen die Resolutionen deshalb auf die Verantwortung des privaten Sektors zur Achtung der Menschenrechte hin und fordern die Unternehmen dazu auf, die Nutzer über die Erhebung, die Verwendung, den Austausch und die Vorratsspeicherung personenbezogener Daten zu informieren und transparente Verarbeitungsmethoden einzuführen.

1.1.3. Europäische Menschenrechtskonvention

Der Europarat wurde nach dem Zweiten Weltkrieg gegründet, um die Staaten Europas mit dem Ziel zusammenzubringen, Rechtsstaatlichkeit, Demokratie, Menschenrechte und soziale Entwicklung zu fördern. Zu diesem Zweck verabschiedete er im Jahr 1950 die [EMRK](#), die 1953 in Kraft trat.

Die Vertragsparteien sind völkerrechtlich zur Einhaltung der EMRK verpflichtet. Seitdem haben alle Mitgliedstaaten des Europarates die EMRK in ihr nationales Recht übernommen oder umgesetzt, weshalb sie verpflichtet sind, im Einklang mit den Bestimmungen der Konvention zu handeln. Die Vertragsparteien müssen sich bei der Ausübung jeder Tätigkeit oder Befugnis an die in der Konvention festgesetzten Rechte halten. Dies umfasst auch Tätigkeiten, die für

¹³ UN, Generalversammlung, [Revised draft resolution on the right to privacy in the digital age](#), A/C.3/71/L.39/Rev.1, New York, 16. November 2016; UN, Menschenrechtsrat, „The right to privacy in the digital age“, A/HRC/34/L.7/Rev.1, 22. März 2017.

die nationale Sicherheit durchgeführt werden. Grundsatzurteile des Europäischen Gerichtshofs für Menschenrechte (EGMR) befassten sich mit staatliche Tätigkeiten in den sensiblen Bereichen des nationalen Sicherheitsrechts und den damit verbundenen Praktiken.¹⁴ Das Gericht zögerte nicht zu bekräftigen, dass Überwachungstätigkeiten einen Eingriff in die Achtung des Privatlebens darstellen.¹⁵

Um zu gewährleisten, dass die Vertragsparteien ihren Verpflichtungen aus der EMRK nachkommen, wurde 1959 in Straßburg (Frankreich) der EGMR eingerichtet. Der EGMR stellt mit Individualbeschwerden von natürlichen Personen, Personengruppen, Nichtregierungsorganisationen oder juristischen Personen wegen behaupteter Verletzungen des Übereinkommens sicher, dass Staaten ihre Verpflichtungen aus dem Übereinkommen erfüllen. Der EGMR kann auch im Rahmen einer Staatenbeschwerde angerufen werden, die von einem oder mehreren Mitgliedstaaten des Europarates gegen einen anderen Mitgliedstaat eingebracht wird.

2018 gehören dem Europarat 47 Mitgliedstaaten an, von denen 28 auch EU-Mitgliedstaaten sind. Ein Beschwerdeführer vor dem EGMR muss nicht Staatsbürger einer der Vertragsparteien sein, obgleich mutmaßliche Verletzungen innerhalb der Rechtsordnung einer der Vertragsparteien stattfinden müssen.

Das Recht auf Schutz personenbezogener Daten gehört zu den gemäß Artikel 8 EMRK geschützten Rechten; dieser Artikel garantiert das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz und legt die Bedingungen fest, unter denen Einschränkungen dieses Rechts zulässig sind.¹⁶

Der EGMR hat sich mit vielen Fällen befasst, in denen es um Datenschutzfragen ging; etwa im Zusammenhang mit dem Abhören des Datenverkehrs,¹⁷ verschiedenen Formen der Überwachung seitens des privaten und öffentlichen

14 Vgl. beispielsweise: EGMR, *Klass und andere / Deutschland*, Nr. 5029/71, 6. September 1978; EGMR, *Rotaru / Rumänien* [GK], Nr. 28341/95, 4. Mai 2000 und EGMR, *Szabó und Vissy / Ungarn*, Nr. 37138/14, 12. Januar 2016.

15 a.a.O.

16 Europarat, *Europäische Menschenrechtskonvention*, SEV Nr. 005, 1950.

17 Vgl. beispielsweise: EGMR, *Malone / Vereinigtes Königreich*, Nr. 8691/79, 2. August 1984; EGMR, *Copland / Vereinigtes Königreich*, Nr. 62617/00, 3. April 2007, oder EGMR, *Mustafa Sezgin Tanrıkulu / Türkei*, Nr. 27473/06, 18. Juli 2017.

Sektors,¹⁸ und dem Schutz gegen die Speicherung personenbezogener Daten durch Behörden.¹⁹ Die Achtung des Privatlebens stellt kein absolutes Recht dar, da dessen Ausübung andere Rechte wie die Freiheit der Meinungsäußerung und den Zugang zu Informationen beeinträchtigen könnte und umgekehrt. Daher versucht der Gerichtshof, zwischen den verschiedenen betroffenen Rechten abzuwägen. Er hat klargestellt, dass Artikel 8 EMRK nicht nur Staaten dazu verpflichtet, Aktionen zu unterlassen, die gegen dieses im Übereinkommen festgeschriebene Recht verstoßen, sondern sie unter bestimmten Umständen dazu verpflichtet, sich sogar aktiv für einen wirksamen Schutz des Privat- und Familienlebens einzusetzen.²⁰ In den entsprechenden Kapiteln sind viele dieser Fälle detailliert beschrieben.

1.1.4. Übereinkommen Nr. 108 des Europarates

Mit dem Aufkommen der Informationstechnologie in den 1960er Jahren trat zunehmend Bedarf an detaillierten Vorschriften über den Schutz natürlicher Personen in Bezug auf ihre personenbezogenen Daten auf. Mitte der 1970er Jahre verabschiedete das Ministerkomitee des Europarates mehrere Entschlüsse zum Schutz personenbezogener Daten, in denen auf Artikel 8 EMRK verwiesen wurde.²¹ 1981 wurde ein [Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten \(Übereinkommen Nr. 108\)](#)²² zur Unterzeichnung aufgelegt. Das Übereinkommen Nr. 108 war und ist noch immer das einzige rechtsverbindliche völkerrechtliche Instrument im Bereich des Datenschutzes.

Das Übereinkommen Nr. 108 gilt für die Verarbeitung jeglicher personenbezogener Daten, sei es im privatwirtschaftlichen oder öffentlichen Sektor, einschließlich der Datenverarbeitung durch Justiz- und Strafverfolgungsbehörden. Das Übereinkommen

18 Vgl. beispielsweise: EGMR, *Klass und andere / Deutschland*, Nr. 5029/71, 6. September 1978; EGMR, *Uzun / Deutschland*, Nr. 35623/05, 2. September 2010.

19 Vgl. beispielsweise: EGMR, *Roman Zakharov / Russland* [GK], Nr. 47143/06, 4. Dezember 2015; EGMR, *Szabó und Vissy / Ungarn*, Nr. 37138/14, 12. Januar 2016.

20 Siehe beispielsweise: EGMR, *I / Finnland*, Nr. 20511/03, 17. Juli 2008; EGMR, *K.U. / Finnland*, Nr. 2872/02, 2. Dezember 2008.

21 Europarat, Ministerkomitee (1973), *EntschlieÙung (73) 22* über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im nicht-öffentlichen Sektor, 26. September 1973; Europarat, Ministerkomitee (1974), *EntschlieÙung (74) 29* über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im öffentlichen Bereich, 20. September 1974.

22 Europarat, Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, Europarat, SEV Nr. 108, 1981.

schützt Menschen vor Missbrauch bei der Verarbeitung personenbezogener Daten und strebt gleichzeitig eine Regulierung des grenzüberschreitenden Verkehrs personenbezogener Daten an. Im Hinblick auf die Verarbeitung personenbezogener Daten enthält das Übereinkommen Grundsätze insbesondere bezüglich der nach Treu und Glauben zu erfolgenden rechtmäßigen Erhebung der Daten und der automatischen Verarbeitung von Daten zu konkreten rechtmäßigen Zwecken. Das bedeutet, dass die Daten weder für Ziele verwendet werden dürfen, die mit diesen Zwecken nicht vereinbar sind, noch länger als erforderlich aufbewahrt werden dürfen. Die Grundsätze betreffen auch die Qualität der Daten; diese müssen insbesondere den Zwecken entsprechen, für die sie erhoben werden, dafür erheblich sein, dürfen nicht darüber hinausgehen (Verhältnismäßigkeit) und müssen sachlich richtig sein.

Das Übereinkommen enthält Garantien für die Verarbeitung personenbezogener Daten und Verpflichtungen in Bezug auf die Datensicherheit, verbietet aber darüber hinaus, sofern keine angemessenen rechtlichen Schutzklauseln vorhanden sind, die Verarbeitung so genannter „sensibler“ Daten, wie Daten zu Rasse, politischer Einstellung, Gesundheit, Konfession, Sexualleben oder Vorstrafen einer Person.

Im Übereinkommen ist ferner das Recht einer Person verankert, über die sie betreffenden Daten Auskunft zu erhalten und sie bei Bedarf berichtigen zu lassen. Einschränkungen der im Übereinkommen festgelegten Rechte sind nur bei übergeordneten Interessen wie Sicherheit des Staats oder Verteidigung möglich. Darüber hinaus sieht das Übereinkommen den freien Verkehr personenbezogener Daten zwischen den Vertragsparteien des Übereinkommens vor und enthält auch einige Einschränkungen für diesen Datenverkehr mit Staaten, in denen die Rechtsvorschriften keinen gleichwertigen Schutz bieten.

An dieser Stelle sei anzumerken, dass das Übereinkommen Nr. 108 für die Ratifizierungsstaaten verbindlich ist. Es untersteht nicht der richterlichen Aufsicht des EGMR, wurde jedoch in der Rechtsprechung des EGMR im Zusammenhang mit Artikel 8 EMGK berücksichtigt. Im Laufe der Jahre hat das Gericht entschieden, dass der Schutz personenbezogener Daten ein wichtiger Bestandteil des Rechts auf Achtung des Privatlebens (Artikel 8) ist und wurde bei der Entscheidung in Bezug auf das Vorliegen oder Nichtvorliegen eines Eingriffs in dieses Grundrecht von den Grundsätzen des Übereinkommens Nr. 108 geleitet.²³

23 Vgl. beispielsweise: EGMR, *Z / Finnland*, Nr. 22009/93, 25. Februar 1997.

Zur Weiterentwicklung der im Übereinkommen Nr. 108 niedergelegten allgemeinen Grundsätze und Vorschriften hat das Ministerkomitee des Europarates mehrere Empfehlungen angenommen, die allerdings nicht rechtsverbindlich sind. Diese Empfehlungen haben die Entwicklung des Datenschutzrechts in Europa beeinflusst. So war die Polizei-Empfehlung beispielsweise jahrelang das einzige Instrument in Europa, das eine Orientierungshilfe in Bezug auf die Nutzung personenbezogener Daten im Polizeibereich bot.²⁴ Die in der Empfehlung enthaltenen Grundsätze, wie die Mittel zur Vorratsspeicherung von Daten und die Notwendigkeit zur Einführung klarer Vorschriften in Bezug auf die Personen, denen Zugang zu diesen Dateien gewährt wird, wurden weiterentwickelt und spiegeln sich in der späteren EU-Gesetzgebung wider.²⁵ Neuere Empfehlungen bemühen sich um die Behandlung der Herausforderungen des digitalen Zeitalters, wie beispielsweise im Zusammenhang mit der Verarbeitung von Daten im Beschäftigungskontext (siehe [Kapitel 9](#)).

Alle EU-Mitgliedstaaten haben das Übereinkommen Nr. 108 ratifiziert. 1999 wurden Änderungen zum Übereinkommen Nr. 108 vorgeschlagen, damit die EU Vertragspartei werden konnte; die Änderungen traten jedoch nie in Kraft.²⁶ 2001 wurde ein Zusatzprotokoll zum Übereinkommen Nr. 108 angenommen. Es enthält Bestimmungen über die grenzüberschreitende Übermittlung von Daten an Nicht-Vertragsparteien, so genannte Drittländer, und die Pflicht zur Errichtung nationaler Datenschutzaufsichtsbehörden.²⁷

Der Beitritt zum Übereinkommen Nr. 108 steht auch Nicht-Vertragsparteien des Europarates offen. Das Potenzial des Übereinkommens als universeller Standard und sein offener Charakter sind die Grundlage für die Förderung des Datenschutzes weltweit. Bis heute sind 51 Länder Vertragsparteien des

24 Europarat, Ministerkomitee (1987), Empfehlung Rec (87)15 an die Mitgliedstaaten über die Nutzung personenbezogener Daten im Polizeibereich, Straßburg, 17. September 1987.

25 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ABl. L 281 vom 23. November 1995.

26 Europarat, Änderungen des Übereinkommens zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108), angenommen vom Ministerkomitee in Straßburg am 15. Juni 1999.

27 Europarat, Zusatzprotokoll zum Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitendem Datenverkehr, SEV Nr. 181, 2001. Mit der Überarbeitung des Übereinkommens 108 wird dieses Protokoll nicht länger angewandt, da seine Bestimmungen aktualisiert und in das Modernisierte Übereinkommen 108 integriert wurden.

Übereinkommens Nr. 108. Dazu zählen alle Mitgliedstaaten des Europarates (47 Länder). Uruguay, das erste außereuropäische Land, trat im August 2013 bei, und Mauritius, Senegal und Tunesien traten 2016 und 2017 bei.

Vor Kurzem wurde das Übereinkommen einer **Modernisierung** unterzogen. Eine im Jahre 2011 abgehaltene öffentliche Konsultation bekräftigte die beiden Hauptziele dieser Arbeit: besserer Schutz der Privatsphäre im digitalen Bereich und Ausbau des Folgemechanismus des Übereinkommens. Der Modernisierungsprozess konzentrierte sich auf diese Ziele und wurde mit der Annahme eines Protokolls, das das Übereinkommen 108 ändert, abgeschlossen (Protokoll SEV Nr. 223). Die Durchführung der Arbeit erfolgte parallel zu anderen Reformen an internationalen Datenschutzinstrumenten und neben der 2012 eingeleiteten Reform der Datenschutzvorschriften der EU. Die Regulierungsbehörden auf Ebene des Europarates und der EU haben sich größte Mühe gegeben, die Kohärenz und Vereinbarkeit der beiden Rechtsrahmen zu gewährleisten. Durch die Modernisierung wird der allgemeine und flexible Charakter des Übereinkommens beibehalten und sein Potenzial als universelles Instrument des Datenschutzrechts verstärkt. Wichtige Grundsätze werden erneut bekräftigt und gefestigt und den Einzelnen werden neue Rechte zuerkannt, während den Stellen, die personenbezogene Daten verarbeiten, gleichzeitig mehr Verantwortung übertragen wird und eine verstärkte Verantwortlichkeit gewährleistet ist. Personen, deren personenbezogene Daten verarbeitet werden, sind beispielsweise dazu berechtigt, Informationen über den Grund dieser Datenverarbeitung zu erhalten und dieser Verarbeitung zu widersprechen. Um der verstärkten Anwendung des Profiling in der Online-Welt entgegenzuwirken, schreibt das Übereinkommen auch das Recht des Einzelnen fest, keinen Entscheidungen unterworfen zu werden, die ausschließlich auf der automatischen Verarbeitung gründen und ihren eigenen Standpunkt nicht berücksichtigen. Die wirksame Durchsetzung der Datenschutzvorschriften seitens unabhängiger Aufsichtsbehörden in den Staaten der Vertragsparteien gilt als wesentlicher Faktor für die praktische Umsetzung des Übereinkommens. Zu diesem Zweck unterstreicht das Modernisierte Übereinkommen das Erfordernis, dass die Aufsichtsbehörden mit wirksamen Befugnissen und Funktionen ausgestattet sind und bei der Ausübung ihrer Aufgaben echte Unabhängigkeit genießen.

1.1.5. Das Datenschutzrecht der Europäischen Union

Das EU-Recht setzt sich aus dem primären und dem sekundären EU-Recht zusammen. Die Verträge, insbesondere der [Vertrag über die Europäische Union \(EUV\)](#) und der Vertrag über die Arbeitsweise der Europäischen Union (AEUV), wurden von allen EU-Mitgliedstaaten ratifiziert und stellen das „primäre EU-Recht“ dar. Die Verordnungen, Richtlinien und Beschlüsse der EU wurden von den EU-Organen angenommen, denen diese Befugnis in den Verträgen übertragen wurde; sie stellen das „sekundäre EU-Recht“ dar.

Datenschutz im primären EU-Recht

Die ursprünglichen Verträge der Europäischen Gemeinschaften beinhalteten keinerlei Verweis auf Menschenrechte oder deren Schutz, da die Europäische Wirtschaftsgemeinschaft anfänglich als regionale Organisation mit Schwerpunkt auf wirtschaftlicher Integration und der Errichtung eines gemeinsamen Marktes vorgesehen war. Ein fundamentaler Grundsatz, der die Gründung und Entwicklung der Europäischen Gemeinschaften untermauert und heute noch gleichermaßen gilt, ist der Grundsatz der begrenzten Einzelermächtigung. Diesem Grundsatz zufolge wird die EU nur innerhalb der Grenzen der Zuständigkeiten tätig, die die Mitgliedstaaten ihr in den EU-Verträgen übertragen haben. Im Gegensatz zu den Europaratsverträgen enthalten die EU-Verträge keine ausdrückliche Zuständigkeit für Grundrechtsangelegenheiten.

Als jedoch Rechtssachen vor den EuGH gebracht wurden, in denen es um die behauptete Verletzung von Menschenrechten im Geltungsbereich des Unionsrechts ging, lieferte der EuGH eine wichtige Auslegung der Verträge. Um den Schutz von Personen zu gewährleisten, wurden die Grundrechte in die so genannten allgemeinen Rechtsgrundsätze des EU-Rechts aufgenommen. Nach Auffassung des EuGH tragen diese allgemeinen Grundsätze dem Inhalt der Bestimmungen zum Schutz der Menschenrechte Rechnung, die in den nationalen Verfassungen und Menschenrechtsverträgen, insbesondere in der EMRK, verankert sind. Der EuGH hielt fest, er werde dafür Sorge tragen, dass das Unionsrecht mit diesen Grundsätzen in Einklang steht.

In Anerkennung der Tatsache, dass ihre Politik Auswirkungen auf die Menschenrechte haben kann, und in dem Bemühen, die Nähe der Bürger zur EU zu stärken, verkündete die EU im Jahr 2000 die Charta der Grundrechte der Europäischen Union (Charta). Sie umfasst die gesamte Bandbreite der bürgerlichen,

politischen, wirtschaftlichen und sozialen Rechte europäischer Bürger und fasst damit die gemeinsamen verfassungsrechtlichen Traditionen und internationalen Verpflichtungen der Mitgliedstaaten zusammen. Die in der Charta verankerten Rechte lassen sich in sechs Kategorien unterteilen: Würde, Freiheiten, Gleichheit, Solidarität, Bürgerrechte und justizielle Rechte.

Ursprünglich war die Charta nur ein politisches Dokument, doch wurde sie mit dem Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 rechtsverbindliches EU-Primärrecht²⁸ (siehe Artikel 6 Absatz 1 EUV²⁹). Die Bestimmungen der Charta richten sich an die Organe und Einrichtungen der EU und verpflichten diese zur Einhaltung der darin angegebenen Rechte bei der Erfüllung ihrer Aufgaben. Die Bestimmungen der Charta sind auch für die Mitgliedstaaten bei der Vollziehung des Unionsrechts verpflichtend.

Die Charta gewährleistet nicht nur die Achtung des Privat- und Familienlebens (Artikel 7), sondern sieht auch das Recht auf Schutz personenbezogener Daten vor (Artikel 8) und hebt damit ausdrücklich das Niveau dieses Schutzes im EU-Recht auf das eines Grundrechts an. Die Organe und Einrichtungen der EU haben dieses Recht ebenso zu gewährleisten und zu achten wie die Mitgliedstaaten bei der Vollziehung des Unionsrechts (Artikel 51 der Charta). Artikel 8 der Charta, der mehrere Jahre nach der Datenschutzrichtlinie formuliert wurde, ist als Ausdruck bereits bestehenden EU-Datenschutzrechts zu verstehen. In der Charta wird also nicht nur ausdrücklich in Artikel 8 Absatz 1 das Recht auf Datenschutz erwähnt, sondern es wird in Artikel 8 Absatz 2 auch auf die Grundsätze des Datenschutzes verwiesen. Schließlich erfordert Artikel 8 Absatz 3 der Charta, dass die Umsetzung dieser Grundsätze von einer unabhängigen Stelle überwacht wird.

Die Annahme des Vertrags von Lissabon stellt einen Meilenstein in der Entwicklung des Datenschutzrechts dar, und dies nicht nur deswegen, weil er der Charta den Status eines verbindlichen Rechtsdokuments auf Ebene des Primärrechts verliehen hat, sondern auch, weil er das Recht auf Schutz personenbezogener Daten vorsieht. Dieses Recht ist in Artikel 16 AEUV ausdrücklich vorgesehen, in dem Teil des Vertrags, der den allgemeinen Grundsätzen der EU gewidmet ist. Artikel 16 schafft auch eine neue Rechtsgrundlage, indem er der EU die

²⁸ EU (2012), Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26. Oktober 2012.

²⁹ Siehe konsolidierte Fassungen von Europäische Gemeinschaften (2012), Vertrag über die Europäische Union, ABl. C 326 vom 26. Oktober 2012, und von Europäische Gemeinschaften (2012), Vertrag über die Arbeitsweise der Europäischen Union, ABl. C 326 vom 26. Oktober 2012.

Zuständigkeit einräumt, in Datenschutzangelegenheiten gesetzgeberisch tätig zu werden. Dies stellt eine bedeutende Entwicklung dar, da die Datenschutzvorschriften der EU und insbesondere die Datenschutzrichtlinie anfangs auf der Rechtsgrundlage des Binnenmarkts und auf dem Erfordernis zur Angleichung der nationalen Gesetze basierten, um den freien Datenverkehr innerhalb der EU nicht einzuschränken. Artikel 16 AEUV liefert nun eine unabhängige Rechtsgrundlage für ein modernes und umfassendes Konzept für den Datenschutz, das sämtliche unter die Zuständigkeit der EU fallende Angelegenheiten abdeckt, einschließlich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Artikel 16 AEUV bekräftigt darüber hinaus, dass die Einhaltung der nach Maßgabe dieses Artikels angenommenen Datenschutzvorschriften von unabhängigen Aufsichtsbehörden überwacht werden muss. Artikel 16 diente als Rechtsgrundlage für die Annahme der umfassenden Reform der Datenschutzvorschriften im Jahr 2016, d. h. der Datenschutz-Grundverordnung und der Datenschutzrichtlinie für Polizei- und Strafverfolgungsbehörden (siehe unten).

Die Datenschutz-Grundverordnung

Von 1995 bis Mai 2018 war die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie) das Hauptrechtsinstrument der EU für den Datenschutz.³⁰ Sie wurde 1995 angenommen, zu einem Zeitpunkt, zu dem mehrere Mitgliedstaaten bereits nationale Datenschutzgesetze verabschiedet hatten,³¹ und entstand aus der Notwendigkeit zur Harmonisierung dieser Gesetze zur Gewährleistung eines hohen Schutzniveaus und eines ungehinderten Verkehrs personenbezogener Daten zwischen den verschiedenen Mitgliedstaaten. Der freie Waren-, Kapital- und Dienstleistungsverkehr und die Personenfreizügigkeit machten einen ungehinderten Datenverkehr erforderlich, der nur möglich war, wenn sich die Mitgliedstaaten auf ein einheitlich hohes Datenschutzniveau verlassen konnten.

30 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995.

31 Das deutsche Bundesland Hessen nahm im Jahr 1970 das erste Gesetz zum Datenschutz an, das nur in diesem Bundesland galt. Schweden nahm 1973 das *Datalagen* an; Deutschland nahm das *Bundesdatenschutzgesetz* 1976 an und Frankreich nahm 1977 das *Loi relatif à l'informatique, aux fichiers et aux libertés* an. Im Vereinigten Königreich wurde der *Data Protection Act* 1984 angenommen. Die Niederlande nahmen schließlich 1989 das *Wet Persoonregistraties* an.

Die Datenschutzrichtlinie spiegelte die in den nationalen Gesetzen und im Übereinkommen Nr. 108 bereits enthaltenen Datenschutzgrundsätze wider und dehnte diese oft noch aus. Sie nutzte die in Artikel 11 des Übereinkommens Nr. 108 eingeräumte Möglichkeit, weitere Schutzinstrumente hinzuzufügen. So hat sich insbesondere die in die Richtlinie erfolgte Einführung einer unabhängigen Aufsicht als Instrument zur Verbesserung der Einhaltung der Datenschutzvorschriften als wichtiger Beitrag zu einem effizienten Funktionieren des europäischen Datenschutzrechts erwiesen. Folglich wurde dieses Merkmal 2001 mit dem Zusatzprotokoll zum Übereinkommen Nr. 108 in das Recht des Europarates übernommen. Dies verdeutlicht das enge Zusammenwirken und den positiven Einfluss, den die beiden Instrumente im Laufe der Jahre aufeinander hatten.

Die Datenschutzrichtlinie errichtete ein detailliertes und umfassendes Datenschutzsystem in der EU. In Übereinstimmung mit dem Rechtssystem der EU finden Richtlinien jedoch keine direkte Anwendung und müssen in die nationalen Rechtsvorschriften der Mitgliedstaaten umgesetzt werden. Bei der Umsetzung der in der Richtlinie enthaltenen Bestimmungen verfügen die Mitgliedstaaten unweigerlich über einen Ermessensspielraum. Obgleich die Richtlinie zu einer umfassenden Harmonisierung³² (und zu einem vollständigen Schutzniveau) führen sollte, wurde sie in der Praxis in den Mitgliedstaaten unterschiedlich umgesetzt. Dies führte zur Einführung verschiedener Datenschutzvorschriften innerhalb der EU, mit in den nationalen Rechtsvorschriften unterschiedlich ausgelegten Begriffsbestimmungen und Vorschriften. Auch der Grad der Durchsetzung und der Schweregrad der Sanktionen unterschieden sich in den Mitgliedstaaten. Schließlich fanden seit der Abfassung der Richtlinie Mitte der 1990er Jahre auch bedeutende Veränderungen in der Informationstechnologie statt. Zusammengenommen veranlassten diese Gründe die Reform der Datenschutzvorschriften der EU.

Nach Jahren intensiver Diskussionen führte die Reform im April 2016 zur Annahme der Datenschutz-Grundverordnung. Die Debatten über die Notwendigkeit der Modernisierung der Datenschutzvorschriften der EU begannen 2009, als die Kommission eine öffentliche Konsultation über den künftigen Rechtsrahmen für das Grundrecht auf Schutz personenbezogener Daten in Gang setzte. Der Vorschlag für die Verordnung wurde von der Kommission

32 EuGH, Verbundene Rechtssachen C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECEDM) / Administración del Estado*, 24. November 2011, Randnr. 29.

im Januar 2012 veröffentlicht und löste einen langen Verhandlungsprozess zwischen dem Europäischen Parlament und dem Rat der EU aus. Nach der Annahme sah die Datenschutz-Grundverordnung einen zweijährigen Übergangszeitraum vor. Am 25. Mai 2018 trat sie mit der Aufhebung der Datenschutzrichtlinie vollständig in Kraft.

Durch die Annahme der Datenschutz-Grundverordnung im Jahre 2016 wurden die Datenschutzvorschriften der EU modernisiert und für den Schutz der Grundrechte im Kontext der wirtschaftlichen und sozialen Herausforderungen des digitalen Zeitalters tauglich gemacht. Die DSGVO behält die in der Datenschutzrichtlinie vorgesehenen wichtigsten Grundsätze und Rechte der betroffenen Person bei und baut diese weiter aus. Darüber hinaus führte sie neue Verpflichtungen ein, die Organisationen die Einführung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, die unter bestimmten Voraussetzungen erfolgende Ernennung eines Datenschutzbeauftragten, die Einhaltung eines neuen Rechts auf Datenübertragbarkeit und die Einhaltung des Grundsatzes der Verantwortlichkeit vorschreiben. Nach EU-Recht gelten Verordnungen unmittelbar und bedürfen keiner nationalen Umsetzung. Die Datenschutz-Grundverordnung sieht folglich für die gesamte EU ein einziges Datenschutzregelwerk vor. Dadurch werden die Datenschutzvorschriften innerhalb der gesamten EU kohärent, wodurch ein von Rechtssicherheit geprägtes Umfeld entsteht, das den Wirtschaftsakteuren und den Einzelnen als „betroffene Personen“ zugutekommen kann.

Auch wenn die Datenschutz-Grundverordnung unmittelbar anwendbar ist, wird von den Mitgliedstaaten erwartet, dass sie ihre bestehenden nationalen Datenschutzvorschriften im Hinblick auf deren vollständige Angleichung an die Verordnung aktualisieren und gleichzeitig auch über einen Ermessensspielraum für bestimmte in Erwägungsgrund 10 genannte Bestimmungen nachdenken. Die in der Verordnung festgesetzten wichtigsten Vorschriften und Grundsätze und die starken Rechte, die sie den Einzelnen einräumt, stellen einen Großteil des Handbuchs dar und werden in den nachstehenden Kapiteln vorgestellt. Die Verordnung enthält umfassende Vorschriften zum räumlichen Anwendungsbe-
reich. Sie gilt für in der EU niedergelassene Unternehmen und auch für nicht in der EU niedergelassene Verantwortliche und Auftragsverarbeiter, die betroffenen Personen, die sich in der EU befinden, Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten. Da etliche Technologieunternehmen aus Übersee über einen bedeutenden Anteil am europäischen Markt und Millionen Kunden aus der EU verfügen, ist es wichtig, dass diese Organisationen den

Datenschutzvorschriften der EU unterworfen werden, um den Schutz der Einzelnen und gleiche Wettbewerbsbedingungen zu gewährleisten.

Datenschutz im Bereich der Strafverfolgung – Richtlinie 2016/680

Die aufgehobene Datenschutzrichtlinie sah eine umfangreiche Datenschutzregelung vor. Diese Regelung wurde nun durch die Annahme der Datenschutz-Grundverordnung noch weiter verbessert. Wenngleich der Anwendungsbereich der aufgehobenen Datenschutzrichtlinie umfassend war, so war er dennoch auf Tätigkeiten beschränkt, die unter den Binnenmarkt fallen, sowie auf Behördentätigkeiten mit Ausnahme der Strafverfolgung. Folglich mussten konkrete Instrumente angenommen werden, um die erforderliche Klarheit und Abwägung zwischen dem Datenschutz und anderen berechtigten Interessen zu erzielen und für bestimmte Bereiche besonders relevante Herausforderungen zu meistern. Dazu gehören die Vorschriften zur Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden.

Der Rahmenbeschluss 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, war das erste Rechtsinstrument der EU zur Regelung dieser Thematik. Seine Vorschriften fanden ausschließlich auf zwischen Mitgliedstaaten ausgetauschte polizeiliche und justizielle Daten Anwendung. Die innerstaatliche Verarbeitung personenbezogener Daten seitens Strafverfolgungsbehörden war von seinem Anwendungsbereich ausgeschlossen.

Die als Datenschutzrichtlinie für Polizei- und Strafverfolgungsbehörden bezeichnete Richtlinie 2016/680 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 Datenverkehr³³ behob diese Situation. Die parallel zur Datenschutz-Grundverordnung angenommene Richtlinie hob den Rahmenbeschluss 2008/977/JI auf, führte ein umfangreiches System für den Schutz personenbezogener Daten im Kontext der Strafverfolgung ein

33 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, ABl. L 119 vom 4.5.2016.

und erkannte gleichzeitig die Besonderheiten der öffentlichen Verarbeitung sicherheitsrelevanter Daten an. Während die Datenschutz-Grundverordnung allgemeine Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten und zur Gewährleistung des freien Datenverkehrs innerhalb der EU festschreibt, setzt die Richtlinie konkrete Vorschriften zum Datenschutz im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit fest. Wenn eine zuständige Behörde personenbezogene Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten verarbeitet, findet die Richtlinie 2016/680 Anwendung. Wenn die zuständigen Behörden personenbezogene Daten für andere als die oben genannten Zwecke verarbeiten, findet die allgemeine Regelung nach Maßgabe der Datenschutz-Grundverordnung Anwendung. Im Unterschied zu ihrem Vorgänger (dem Rahmenbeschluss 2008/977/JI des Rates), erstreckt sich der Anwendungsbereich der Richtlinie 2016/680 auf die innerstaatliche Verarbeitung personenbezogener Daten seitens Strafverfolgungsbehörden und ist nicht auf den Austausch solcher Daten zwischen den Mitgliedstaaten beschränkt. Darüber hinaus soll durch die Richtlinie eine Abwägung zwischen den Rechten natürlicher Personen und den berechtigten Zielsetzungen einer sicherheitsrelevanten Verarbeitung erzielt werden.

Zu diesem Zweck bekräftigt die Richtlinie unter genauer Befolgung der in der Datenschutz-Grundverordnung verankerten Vorschriften und Grundsätze das Recht auf Schutz personenbezogener Daten und die wichtigsten Grundsätze, denen die Datenverarbeitung unterliegen sollte. Die Rechte natürlicher Personen und die den Verantwortlichen beispielsweise in Bezug auf die Datensicherheit, den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen und die Meldung von Verletzungen des Schutzes personenbezogener Daten auferlegten Pflichten ähneln den in der Datenschutz-Grundverordnung enthaltenen Rechten und Pflichten. Die Richtlinie berücksichtigt überdies die aufkommenden großen technologischen Herausforderungen, die sich auf die Einzelnen besonders belastend auswirken können, und versucht, diese anzugehen. Dazu zählt beispielsweise der Einsatz von Profiling-Techniken seitens der Strafverfolgungsbehörden Grundsätzlich müssen ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungen – einschließlich Profiling – verboten werden.³⁴ Überdies dürfen sie nicht auf sensible Daten gründen. Diese Grundsätze unterliegen bestimmten Ausnahmen, die in der Richtlinie dargelegt sind. Darüber hinaus darf eine solche Verarbeitung nicht zur Folge haben, dass Personen diskriminiert werden.³⁵

34 Datenschutzrichtlinie für Polizei- und Strafverfolgungsbehörden, Artikel 11 Absatz 1.

35 *a.a.O.*, Artikel 11 Absatz 2 und 3.

Die Richtlinie enthält auch Vorschriften zur Gewährleistung der Rechenschaftspflicht der Verantwortlichen. Sie müssen einen Datenschutzbeauftragten ernennen, der die Einhaltung der Datenschutzvorschriften überwacht, die Stelle und die Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten unterrichtet und berät, und mit der Aufsichtsbehörde zusammenarbeitet. Die Verarbeitung personenbezogener Daten im Polizei- und Strafverfolgungsbereich unterliegt nun der Aufsicht unabhängiger Aufsichtsbehörden. Sowohl der Rechtsrahmen zum allgemeinen Datenschutz als auch die besondere Datenschutzregelung für die Strafverfolgung und für Strafsachen müssen zudem den Anforderungen der Charta der Grundrechte der Europäischen Union entsprechen.

Die durch die Datenschutzrichtlinie für Polizei- und Strafverfolgungsbehörden eingeführten Sonderregelungen zur Datenverarbeitung im Kontext der polizeilichen und justiziellen Zusammenarbeit werden in [Kapitel 8](#) detailliert beschrieben.

Datenschutzrichtlinie für elektronische Kommunikation

Auch im Bereich der elektronischen Kommunikation wurde die Einführung von speziellen Datenschutzvorschriften für notwendig erachtet. Mit der Entwicklung des Internets und der Festnetz- und Mobiltelefonie war es wichtig, die Achtung der Rechte der Nutzer auf Privatsphäre und Vertraulichkeit sicherzustellen. Die Richtlinie 2002/58/EG³⁶ über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation oder ePrivacy-Richtlinie) enthält Vorschriften in Bezug auf die Sicherheit personenbezogener Daten in diesen Netzwerken, die Anzeige von Verletzungen des Schutzes personenbezogener Daten und die Vertraulichkeit der Kommunikation.

In Bezug auf die Sicherheit müssen die Anbieter elektronischer Kommunikationsdienste unter anderem sicherstellen, dass der Zugriff auf personenbezogene Daten ausschließlich auf ermächtigte Personen beschränkt ist, und Maßnahmen ergreifen, um die Zerstörung, den Verlust oder die unbeabsichtigte Beschädigung personenbezogener Daten zu verhindern.³⁷ Besteht ein besonderes Risiko der Verletzung der Sicherheit des öffentlichen Kommunikationsnetzes, müssen

36 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 201 vom 31.7.2002 (Datenschutzrichtlinie für elektronische Kommunikation oder ePrivacy-Richtlinie).

37 Datenschutzrichtlinie für elektronische Kommunikation, Artikel 4 Absatz 1.

die Anbieter die Teilnehmer über dieses Risiko unterrichten.³⁸ Sollte trotz der umgesetzten Sicherheitsmaßnahmen eine Verletzung der Sicherheit auftreten, müssen die Anbieter die mit der Umsetzung und Durchsetzung der Richtlinie betraute nationale Behörde von der Verletzung des Schutzes personenbezogener Daten in Kenntnis setzen. In manchen Fällen müssen die Anbieter auch die Personen über die Verletzung personenbezogener Daten benachrichtigen, und zwar wenn anzunehmen ist, dass durch die Verletzung deren personenbezogene Daten oder deren Privatsphäre beeinträchtigt werden.³⁹ Die Vertraulichkeit der Kommunikation erfordert, dass das Mithören, Abhören und Speichern sowie andere Arten des Überwachens oder Abfangens von Nachrichten und Metadaten grundsätzlich untersagt ist. Die Richtlinie untersagt auch unerbetene Nachrichten (häufig als „Spam“ bezeichnet), es sei denn, die Nutzer haben ihre Einwilligung erteilt, und enthält Vorschriften in Bezug auf die Speicherung von „Cookies“ auf Computern und Geräten. Diese wichtigen Unterlassungspflichten lassen deutlich erkennen, dass die Vertraulichkeit der Kommunikation maßgeblich mit dem Schutz des in Artikel 7 der Charta verankerten Rechts auf Achtung des Privatlebens und des in Artikel 8 der Charta verankerten Rechts auf Schutz personenbezogener Daten verknüpft ist.

Im Januar 2017 veröffentlichte die Kommission einen Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation, die die Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie) ersetzen soll. Ziel der Reform ist die Angleichung der Vorschriften für die elektronische Kommunikation an die durch die Datenschutz-Grundverordnung eingeführte neue Datenschutzregelung. Die neue Verordnung wird in der gesamten EU unmittelbar gelten; alle Personen kommen in den Genuss desselben Schutzniveaus ihrer elektronischen Kommunikation, während die Telekommunikationsanbieter und Unternehmen von der Klarheit, der Rechtssicherheit und dem Bestehen eines einzigen EU-weiten Regelwerks profitieren werden. Die vorgeschlagenen Vorschriften über die Vertraulichkeit der elektronischen Kommunikation werden auch auf neue Marktteilnehmer Anwendung finden, die elektronische Kommunikationsdienste anbieten, die nicht unter die ePrivacy-Richtlinie fallen. Letztere deckte nur die Anbieter traditioneller Telekommunikationsdienste ab. Aufgrund des massiven Anstiegs der Nutzung von Diensten wie Skype, WhatsApp, Facebook Messenger und Viber zum Nachrichtenversand oder zur Tätigkeit

38 a.a.O., Artikel 4 Absatz 2.

39 a.a.O., Artikel 4 Absatz 3.

von Anrufen, werden diese Over-the-Top-Dienste (OTT-Dienste) nun in den Anwendungsbereich der Verordnung fallen und müssen deren Anforderungen in Bezug auf Datenschutz, Privatsphäre und Sicherheit erfüllen. Zum Zeitpunkt der Veröffentlichung dieses Handbuchs war das Gesetzgebungsverfahren in Bezug auf die ePrivacy-Vorschriften noch im Gange.

Verordnung (EG) Nr. 45/2001

Da sich die Datenschutzrichtlinie nur an die Mitgliedstaaten richten konnte, war ein weiteres Rechtsinstrument für die Organisation des Datenschutzes bei der Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der EU erforderlich. Diese Aufgabe erfüllt die Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (Datenschutzverordnung für die EU-Organe).⁴⁰

Die Verordnung (EG) Nr. 45/2001 befolgt genau die Grundsätze der allgemeinen Datenschutzregelung der EU und wendet diese auf die seitens der Organe und Einrichtungen der EU im Rahmen der Ausübung ihrer Aufgaben durchgeführte Datenverarbeitung an. Darüber hinaus richtet sie mit dem Europäischen Datenschutzbeauftragten (EDSB) eine unabhängige Aufsichtsbehörde zur Überwachung der Anwendung ihrer Bestimmungen ein. Der EDSB ist mit Kontrollbefugnissen ausgestattet und hat die Aufgabe, die Verarbeitung personenbezogener Daten in den Organen und Einrichtungen der EU zu überwachen und Beschwerden in Bezug auf behauptete Verstöße gegen die Datenschutzvorschriften anzuhören und zu prüfen. Darüber hinaus berät er die Organe und Einrichtungen der EU bei sämtlichen Angelegenheiten in Bezug auf den Schutz personenbezogener Daten, angefangen bei Vorschlägen für neue Rechtsvorschriften bis hin zur Ausarbeitung interner Vorschriften in Bezug auf die Datenverarbeitung.

Im Januar 2017 legte die Europäische Kommission einen Vorschlag für eine neue Verordnung über die Datenverarbeitung durch die EU-Organe vor, die die derzeitige Verordnung aufheben wird. Ebenso wie die Reform der ePrivacy-Richtlinie wird auch die Reform der Verordnung (EG) Nr. 45/2001 die darin enthaltenen Vorschriften modernisieren und an die durch die Datenschutz-Grundverordnung eingeführten neuen Datenschutzregelungen angleichen.

⁴⁰ Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 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. Januar 2001.

Die Rolle des EuGH

Der EuGH ist dafür zuständig, zu entscheiden, ob ein Mitgliedstaat seinen Verpflichtungen aus dem Datenschutzrecht der EU nachgekommen ist oder nicht, und die Rechtsvorschriften der EU auszulegen, um deren wirksame und einheitliche Anwendung in den Mitgliedstaaten zu gewährleisten. Seit der Annahme der Datenschutzrichtlinie im Jahre 1995 hat sich eine umfangreiche Rechtsprechung angesammelt, die den Anwendungsbereich und die Bedeutung der Datenschutzgrundsätze und des in Artikel 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten verdeutlicht. Obgleich die Richtlinie ersetzt wurde und mit der Datenschutz-Grundverordnung nun ein neues Rechtsinstrument in Kraft ist, bleibt diese bereits bestehende Rechtsprechung für die Auslegung und Anwendung der Datenschutzgrundsätze der EU maßgeblich und gültig, soweit die wichtigsten Grundsätze und Konzepte der Datenschutzrichtlinie in der DSGVO beibehalten wurden.

1.2. Einschränkungen des Rechts auf Schutz personenbezogener Daten

Kernpunkte

- Das Recht auf Schutz personenbezogener Daten ist kein absolutes Recht; bei Bedarf kann es für eine Zielsetzung von allgemeinem Interesse oder für den Schutz der Rechte und Freiheiten anderer eingeschränkt werden.
- Die Bedingungen für die Einschränkung des Rechts auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten sind in Artikel 8 EMRK und in Artikel 52 Absatz 1 der Charta aufgelistet. Sie wurden durch die Rechtsprechung des EGMR und des EuGH entwickelt und interpretiert.
- Nach Maßgabe des Datenschutzrechtes des Europarates stellt die Verarbeitung personenbezogener Daten einen rechtmäßigen Eingriff in das Recht auf Achtung des Privatlebens dar und darf nur ausgeführt werden, wenn
 - sie im Gesetz vorgesehen ist,
 - ein rechtmäßiges Ziel verfolgt,
 - den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und
 - in einer demokratischen Gesellschaft für das Erreichen eines rechtmäßigen Zwecks notwendig und verhältnismäßig ist:

- Das Rechtssystem der EU stellt ähnliche Bedingungen an Einschränkungen der Ausübung der durch die Charta geschützten Grundrechte. Jedwede Einschränkung eines Grundrechts, einschließlich des Grundrechts auf Schutz personenbezogener Daten, kann nur dann rechtmäßig sein, wenn
 - sie im Gesetz vorgesehen ist,
 - den Wesensgehalt des Rechts achtet,
 - unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich ist, und
 - sie eine von der Union anerkannte dem Gemeinwohl dienende Zielsetzung oder das Erfordernis des Schutzes der Rechte anderer verfolgt.

Das Grundrecht auf Schutz personenbezogener Daten gemäß Artikel 8 der Charta ist kein absolutes Recht, „sondern muss im Hinblick auf seine gesellschaftliche Funktion gesehen werden“.⁴¹ Artikel 52 Absatz 1 der Charta erkennt folglich an, dass Einschränkungen der Ausübung der Rechte wie derjenigen, die in Artikel 7 und 8 der Charta verankert sind, auferlegt werden können, sofern diese Einschränkungen gesetzlich vorgesehen sind, den Wesensgehalt dieser Rechte und Freiheiten achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und den von der EU anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.⁴² Ebenso wird der Datenschutz im System der EMRK durch Artikel 8 gewährleistet, und die Ausübung dieses Rechts kann bei Bedarf eingeschränkt werden, sofern dies zur Verfolgung eines rechtmäßigen Zwecks erforderlich ist. Dieser Abschnitt befasst sich sowohl mit den Eingriffsvoraussetzungen gemäß der EMRK, wie sie in der Rechtsprechung des EGMR ausgelegt werden, als auch mit den Bedingungen für rechtmäßige Einschränkungen gemäß Artikel 52 der Charta.

1.2.1. Anforderungen an einen rechtmäßigen Eingriff gemäß EMRK

Die Verarbeitung personenbezogener Daten kann ein Eingriff in das durch Artikel 8 EMRK geschützte Recht auf Achtung des Privatlebens der betroffenen

41 Siehe beispielsweise EuGH, Verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen* [GK], 9. November 2010, Randnr. 48.

42 a.a.O., Randnr. 50.

Person sein.⁴³ Wie oben erläutert (siehe [Abschnitt 1.1.1](#) und [Abschnitt 1.1.4](#)), erkennt die EMRK im Gegensatz zur Rechtsordnung der EU den Schutz personenbezogener Daten nicht als eigenständiges Grundrecht an. Vielmehr stellt der Schutz personenbezogener Daten einen Bestandteil der nach Maßgabe des Rechts auf Achtung des Privatlebens geschützten Rechte dar. Folglich kann nicht jede Tätigkeit, die die Verarbeitung personenbezogener Daten umfasst, unter den Anwendungsbereich von Artikel 8 EMRK fallen. Damit Artikel 8 anwendbar wird, muss zunächst bestimmt werden, ob ein privates Interesse oder das Privatleben einer Person beeinträchtigt wurden. Der EGMR behandelte den Begriff des „Privatlebens“ in seiner Rechtsprechung als weites Konzept, das selbst Aspekte des Berufslebens und des Verhaltens einer Person in der Öffentlichkeit umfasst. Er entschied auch, dass der Schutz personenbezogener Daten einen wichtigen Bestandteil des Rechts auf Achtung des Privatlebens darstellt. Trotz der weiten Auslegung des Privatlebens würden nicht alle Arten der Verarbeitung per se die gemäß Artikel 8 geschützten Rechte beeinträchtigen.

Wenn der EGMR der Ansicht ist, dass die betreffende Verarbeitung das Recht der Personen auf Achtung des Privatlebens beeinträchtigt, prüft er, ob der Eingriff gerechtfertigt ist. Das Recht auf Achtung des Privatlebens ist jedoch kein absolutes Recht, sondern muss mit anderen berechtigten Interessen abgewogen und in Einklang gebracht werden, seien sie nun die anderer Personen (private Interessen) oder die der Gesellschaft insgesamt (öffentliche Interessen).

Ein Eingriff könnte gerechtfertigt sein, wenn die folgenden kumulativen Bedingungen erfüllt sind:

Er muss im Gesetz vorgesehen sein

Gemäß der Rechtsprechung des EGMR steht ein Eingriff im Einklang mit dem Gesetz, wenn er sich auf eine Bestimmung des innerstaatlichen Rechts stützt, das bestimmte Merkmale aufweist. Das Gesetz muss „den betroffenen Personen zugänglich und in seinen Wirkungen vorhersehbar sein“.⁴⁴ Eine Vorschrift ist vorhersehbar, „wenn sie mit hinreichender Bestimmtheit formuliert ist, so dass

43 EGMR, *S. und Marper / Vereinigtes Königreich* [GK], Nrn. 30562/04 und 30566/04, 8. Dezember 2008, Randnr. 67.

44 EGMR, *Amann / Schweiz* [GK], Nr. 27798/95, 16. Februar 2000, Randnr. 50; siehe auch EGMR, *Kopp / Schweiz*, Nr. 23224/94, 25. März 1998, Randnr. 55 und ECtHR, *Iordachi und andere / Republik Moldau*, Nr. 25198/02, 10. Februar 2009, Randnr. 50.

ein jeder – bei Bedarf mit angemessener Beratung – in der Lage ist, sich entsprechend zu verhalten“.⁴⁵ Überdies gilt: „Der von „dem Gesetz“ in diesem Zusammenhang verlangte Detailgrad hängt vom jeweiligen Thema ab.“⁴⁶

Beispiele: In der Rechtssache *Rotaru gegen Rumänien*⁴⁷ machte der Beschwerdeführer eine Verletzung seines Rechts auf Achtung seines Privatlebens geltend, da der rumänische Geheimdienst eine Datei mit seinen personenbezogenen Informationen besaß und verwendete. Der EGMR stellte fest, dass nach rumänischem Recht die Sammlung, Aufzeichnung und Archivierung von Informationen, die die nationale Sicherheit berühren, in Geheimakten zwar zulässig sei, für die Ausübung dieser Befugnisse jedoch keine Grenzen festgelegt waren; diese lagen im Ermessen der Behörden. So war im innerstaatlichen Recht beispielsweise nicht festgelegt, welche Art von Informationen verarbeitet werden durfte, gegen welche Personenkategorien Überwachungsmaßnahmen ergriffen werden konnten, unter welchen Umständen solche Maßnahmen ergriffen werden durften und welche Verfahren galten. Folglich befand der Gerichtshof, dass das innerstaatliche Recht nicht dem Erfordernis der Vorhersehbarkeit gemäß Artikel 8 EMRK Genüge tat und dass eine Verletzung dieses Artikels vorlag.

In der Rechtssache *Taylor-Sabori gegen Vereinigtes Königreich*⁴⁸ war der Beschwerdeführer Ziel polizeilicher Überwachung gewesen. Unter Zuhilfenahme einer „Kopie“ des Pagers des Beschwerdeführers konnte die Polizei an ihn gesendete Nachrichten abhören. Der Beschwerdeführer wurde festgenommen und der Verschwörung zur Lieferung kontrollierter Drogen beschuldigt. Die Anklage gegen ihn stützte sich teilweise auf Niederschriften der Pager-Nachrichten, die von der Polizei angefertigt worden waren. Zum Zeitpunkt des Verfahrens gegen den Beschwerdeführer

45 EGMR, *Amann / Schweiz* [GK], Nr. 27798/95, 16. Februar 2000, Randnr. 56; siehe auch EGMR, *Malone / Vereinigtes Königreich*, Nr. 8691/79, 2. August 1984, Randnr. 66; EGMR, *Silver und andere / Vereinigtes Königreich*, Nrn. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. März 1983, Randnr. 88.

46 EGMR, *The Sunday Times / Vereinigtes Königreich*, Nr. 6538/74, 26. April 1979, Randnr. 49; siehe auch EGMR, *Silver und andere / Vereinigtes Königreich*, Nrn. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. März 1983, Randnr. 88.

47 EGMR, *Rotaru / Rumänien* [GK], Nr. 28341/95, 4. Mai 2000, Randnr. 57; siehe auch EGMR, *Association for European Integration and Human Rights und Ekimdzhiev / Bulgarien*, Nr. 62540/00, 28. Juni 2007; EGMR, *Shimovolos / Russland*, Nr. 30194/09, 21. Juni 2011; und EGMR, *Vetter / Frankreich*, Nr. 59842/00, 31. Mai 2005.

48 EGMR, *Taylor-Sabori / Vereinigtes Königreich*, Nr. 47114/99, 22. Oktober 2002.

gab es jedoch im britischen Recht keine Bestimmung zur Regelung des Abhörens von Gesprächen über ein privates Telekommunikationssystem. Der Eingriff in seine Rechte war somit „nicht im Gesetz vorgesehen“. Der EGMR befand, dass dadurch eine Verletzung von Artikel 8 EMRK vorlag.

In der Rechtssache *Vukota-Bojić gegen Schweiz*⁴⁹ ging es um die geheime Überwachung einer Sozialversicherungsempfängerin durch seitens ihres Versicherungsunternehmens beauftragte Privatdetektive. Der EGMR befand, dass die den Gegenstand der Beschwerde darstellende Sicherheitsmaßnahme zwar seitens eines privaten Versicherungsunternehmens angeordnet wurde, dieses Unternehmen jedoch vom Staat dazu berechtigt worden war, Leistungen aus Pflichtkrankenversicherungen bereitzustellen und Versicherungsbeiträge einzuziehen. Ein Staat könne sich nicht von der ihm nach Maßgabe des Übereinkommens zukommenden Haftung befreien, indem er seine Pflichten an private Einrichtungen oder Personen überträgt. Das innerstaatliche Recht habe für hinreichende Garantien gegen Missbrauch zu sorgen, damit der Eingriff in die Rechte gemäß Artikel 8 EMRK als „im Gesetz vorgesehen“ betrachtet werden kann. In der vorliegenden Rechtssache befand der EGMR, dass eine Verletzung von Artikel 8 EMRK vorlag, da das innerstaatliche Recht nicht mit ausreichender Klarheit das Ausmaß und die Art und Weise der Ausübung des dem Versicherungsunternehmen übertragenen Ermessens angab, wenn dieses als Behörde bei Versicherungsstreitigkeiten die geheime Überwachung von Versicherten veranlasste. Insbesondere enthielt das innerstaatliche Recht keine hinreichenden Garantien gegen Missbrauch.

Er muss ein rechtmäßiges Ziel verfolgen

Das rechtmäßige Ziel kann im Zusammenhang mit einem der genannten öffentlichen Interessen oder mit dem Schutz der Rechte und Freiheiten anderer stehen. Bei rechtmäßigen Zielen, die einen Eingriff rechtfertigen könnten, handelt es sich gemäß Artikel 8 Absatz 2 EMRK um die nationale oder öffentliche Sicherheit, das wirtschaftliche Wohl eines Landes, die Aufrechterhaltung der Ordnung, die Verhütung von Straftaten, den Schutz der Gesundheit oder der Moral und den Schutz der Rechte und Freiheiten anderer.

⁴⁹ EGMR, *Vukota-Bojić / Schweiz*, Nr. 61838/10, 18. Oktober 2016, Randnr. 77.

Beispiel: In der Rechtssache *Peck gegen Vereinigtes Königreich*⁵⁰ versuchte der Beschwerdeführer, auf der Straße durch Aufschneiden seiner Pulsadern Selbstmord zu begehen, hatte jedoch nicht bemerkt, dass er bei diesem Versuch von einer Überwachungskamera gefilmt worden war. Die Polizei, die die Aufnahmen der Überwachungskamera gesehen hatte, rettete ihn und gab das Filmmaterial der Überwachungskamera anschließend an die Medien weiter, die es veröffentlichten, ohne das Gesicht des Beschwerdeführers unkenntlich zu machen. Nach Auffassung des EGMR lagen keine stichhaltigen oder hinreichenden Gründe für eine direkte Weitergabe des Filmmaterials durch die Behörden an die Öffentlichkeit vor, ohne vorher die Einwilligung des Beschwerdeführers eingeholt oder sein Gesicht unkenntlich gemacht zu haben. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Er muss in einer demokratischen Gesellschaft notwendig sein

Der EGMR stellt hierzu fest: „Der Begriff der Notwendigkeit impliziert, dass der Eingriff einem dringenden gesellschaftlichen Bedürfnis entspricht und vor allem, dass er zu dem angestrebten rechtmäßigen Ziel in einem angemessenen Verhältnis steht“.⁵¹ Bei der Beurteilung, ob eine Maßnahme erforderlich ist, um einem dringenden gesellschaftlichen Bedürfnis gerecht zu werden, untersucht der EGMR deren Bedeutung und Eignung in Bezug auf das verfolgte Ziel. Dazu kann er berücksichtigen, ob mit dem Eingriff auf ein Problem eingegangen werden soll, das ansonsten schädliche Auswirkungen auf die Gesellschaft haben könnte, ob belegt ist, dass der Eingriff diese schädlichen Auswirkungen abmildern kann, und welche Auffassungen die Gesellschaft allgemein zu dem betreffenden Problem vertritt.⁵² Die durch Sicherheitsdienste erfolgende Erhebung und Speicherung personenbezogener Daten bestimmter Personen, bei denen Zusammenhänge mit terroristischen Bewegungen festgestellt wurden, würde einen Eingriff in das Recht auf Achtung des Privatlebens der Person darstellen, der gleichwohl einem dringenden gesellschaftlichen Bedürfnis entspricht, das in der nationalen Sicherheit und in der Terrorismusbekämpfung besteht. Um die Notwendigkeitsprüfung zu bestehen, muss der Eingriff auch verhältnismäßig sein. In der Rechtsprechung des EGMR wird die Verhältnismäßigkeit im Rahmen des Konzepts der Notwendigkeit behandelt.

50 EGMR, *Peck / Vereinigtes Königreich*, Nr. 44647/98, 28. Januar 2003, Randnr. 85.

51 EGMR, *Leander / Schweden*, Nr. 9248/81, 26. März 1987, Randnr. 58.

52 Artikel-29-Datenschutzgruppe (2014), *Stellungnahme zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung*, WP 211, Brüssel, 27. Februar 2014, S. 7-8.

Die Verhältnismäßigkeit erfordert, dass sich ein Eingriff in die nach Maßgabe der EMRK geschützten Rechte auf das zur Erfüllung des angestrebten rechtmäßigen Ziels erforderliche Maß beschränkt. Wichtige Faktoren, die es bei der Durchführung der Verhältnismäßigkeitsprüfung zu berücksichtigen gilt, sind der Geltungsbereich des Eingriffs, und insbesondere die Anzahl der betroffenen Personen und die eingerichteten Schutzvorkehrungen oder Vorbehalte zur Begrenzung seines Geltungsbereichs oder der nachteiligen Auswirkungen auf die Rechte der Personen.⁵³

Beispiel: In der Rechtssache *Khelili gegen Schweiz*⁵⁴ wurden bei einer Polizeikontrolle bei der Beschwerdeführerin Visitenkarten mit folgendem Aufdruck gefunden: „Nette, hübsche Frau, Ende dreißig, sucht einen Mann, mit dem sie gelegentlich ein Gläschen trinken oder ausgehen kann. Tel.-Nr. [...]“. Die Beschwerdeführerin gab an, dass die Polizei sie daraufhin in ihren Akten als Prostituierte führte, einer Beschäftigung, der nachzugehen sie stets verneinte. Die Beschwerdeführerin verlangte die Streichung des Wortes „Prostituierte“ aus den Computerverzeichnissen der Polizei. Der EGMR räumte grundsätzlich ein, dass die Speicherung der personenbezogenen Daten einer Person aus dem Grund, dass diese Person eine andere Straftat begehen könnte, unter gewissen Umständen verhältnismäßig sein kann. Im Falle der Beschwerdeführerin sei jedoch die Behauptung illegaler Prostitution zu vage und allgemein, werde nicht durch konkrete Fakten gestützt, da sie nie wegen illegaler Prostitution verurteilt worden sei, und könne daher nicht als Antwort auf ein „dringendes gesellschaftliches Bedürfnis“ im Sinne von Artikel 8 EMRK angesehen werden. Der Gerichtshof betrachtete es als Aufgabe der Behörden, die sachliche Richtigkeit der über die Beschwerdeführerin gespeicherten Daten nachzuweisen, und befand in seinem Urteil bezüglich der Schwere des Eingriffs in die Rechte der Beschwerdeführerin, dass die jahrelange Speicherung des Worts „Prostituierte“ in den Polizeiakten in einer demokratischen Gesellschaft nicht notwendig gewesen sei. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Beispiel: In der Rechtssache *S. und Marper gegen Vereinigtes Königreich*⁵⁵ waren die beiden Beschwerdeführer bestimmter Straftaten angeklagt. Wie im „Police and Criminal Evidence Act“ (Polizei- und Beweismittelgesetz)

53 a.a.O., S. 9–11.

54 EGMR, *Khelili / Schweiz*, Nr. 16188/07, 18. Oktober 2011.

55 EGMR, *S. und Marper / Vereinigtes Königreich* [GK], Nrn. 30562/04 und 30566/04, 4. Dezember 2008.

vorgesehen, nahm die Polizei ihre Fingerabdrücke und DNA-Profile auf. Die Beschwerdeführer wurden für die Straftaten nie verurteilt. Einer wurde vor Gericht freigesprochen und das Strafverfahren gegen den zweiten Beschwerdeführer wurde eingestellt. Dessen ungeachtet bewahrte die Polizei ihre Fingerabdrücke, DNA-Profile und Zellproben weiter in einer Datenbank auf und die innerstaatliche Gesetzgebung erlaubte deren unbefristete Speicherung. Obgleich das Vereinigte Königreich argumentierte, dass die Speicherung die Ermittlung künftiger Straftäter erleichtere und folglich das rechtmäßige Ziel der Verhütung und Aufdeckung von Straftaten anstrebe, befand der EGMR den Eingriff in das Recht des Beschwerdeführers auf Achtung des Privatlebens ungerechtfertigt. Er erinnerte daran, dass die Kerngrundsätze des Datenschutzes erfordern, dass die Speicherung von personenbezogenen Daten in einem angemessenen Verhältnis zum Zweck der Erhebung steht und die Speicherzeiten befristet sein müssen. Der Gerichtshof stimmte zu, dass die Erweiterung der Datenbank durch DNA-Profile, die nicht nur von verurteilten Personen stammen, sondern auch von verdächtigen Personen, die nicht verurteilt wurden, zur Aufdeckung und Verhütung von Straftaten im Vereinigten Königreich hätte beitragen können. Er war jedoch „von der pauschalen und unterschiedslosen Art der Speicherbefugnis schockiert“⁵⁶

In Anbetracht der Fülle der in den Zellproben enthaltenen genetischen und gesundheitsbezogenen Informationen sei der Eingriff in das Recht des Beschwerdeführers auf Achtung seines Privatlebens besonders einschneidend. Fingerabdrücke und Proben könnten von verhafteten Personen erfasst und auf unbestimmte Zeit in der Polizeidatenbank gespeichert werden, unabhängig von der Art und Schwere der Straftat, und selbst im Falle kleinerer Vergehen, die nicht mit einer Freiheitsstrafe bestraft werden. Darüber hinaus seien die Möglichkeiten freigesprochener Personen zur Entfernung ihrer Daten aus der Datenbank beschränkt. Schließlich berücksichtigte der EGMR ganz besonders die Tatsache, dass ein Beschwerdeführer bei seiner Festnahme erst elf Jahre alt war. Die Speicherung personenbezogener Daten nicht verurteilter Minderjähriger kann sich in Anbetracht ihrer Verletzlichkeit und der Wichtigkeit ihrer Entwicklung und Eingliederung in die Gesellschaft als besonders gefährlich erweisen.⁵⁷ Der Gerichtshof entschied einstimmig, dass die

⁵⁶ a.a.O., Randnr. 119.

⁵⁷ a.a.O., Randnr. 124.

Speicherung einen unverhältnismäßigen Eingriff in das Recht auf Privatleben darstellte, der in einer demokratischen Gesellschaft nicht als erforderlich erachtet werden konnte.

Beispiel: In der Rechtssache *Leander gegen Schweden*⁵⁸ stellte der EGMR fest, dass die geheime Überprüfung von Personen, die sich um einen für die nationale Sicherheit wichtigen Arbeitsplatz bewerben, an sich nicht dem Erfordernis widerspricht, in einer demokratischen Gesellschaft notwendig zu sein. Aufgrund der im innerstaatlichen Recht vorgesehenen besonderen Garantien für den Schutz der Interessen der betroffenen Person, beispielsweise Kontrolle durch Parlament und Justizministerium, befand der EGMR, dass das schwedische System für Personalkontrolle den Anforderungen von Artikel 8 Absatz 2 EMRK Genüge tut. In Anbetracht seines großen Ermessensspielraums sei der beklagte Staat zu der Auffassung befugt, im Falle des Beschwerdeführers den Interessen der nationalen Sicherheit Vorrang vor denen dieser Person einzuräumen. Der Gerichtshof befand, dass keine Verletzung von Artikel 8 EMRK vorlag.

1.2.2. Bedingungen für rechtmäßige Einschränkungen gemäß der EU-Charta

Struktur und Wortlaut der Charta unterscheiden sich von denen der EMRK. Die Charta verwendet nicht den Begriff des Eingriffs in garantierte Rechte, sondern enthält eine Bestimmung über die Einschränkung(en) der Ausübung der in der Charta anerkannten Rechte und Freiheiten.

Gemäß Artikel 52 Absatz 1 dürfen Einschränkungen der Ausübung der in der Charta anerkannten Rechte und Freiheiten und damit auch des Rechts auf Wahrnehmung des Rechts auf Datenschutz nur vorgenommen werden, wenn sie

- gesetzlich vorgesehen sind;
- den Wesensgehalt des Rechts auf Datenschutz achten;
- unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind⁵⁹ und

⁵⁸ EGMR, *Leander / Schweden*, Nr. 9248/81, 26. März 1987, Randnrn. 59 und 67.

⁵⁹ Zur Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken, siehe: EDSB (2017), *Necessity Toolkit*, Brüssel, 11. April 2017.

- den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer entsprechen.

Da es sich beim Schutz personenbezogener Daten in der Rechtsordnung der EU um ein separates und eigenständiges Grundrecht handelt, das gemäß Artikel 8 der Charta geschützt ist, stellt jedwede Verarbeitung personenbezogener Daten an sich bereits einen Eingriff in dieses Recht dar. Dabei spielt es keine Rolle, ob sich die betreffenden personenbezogenen Daten auf das Privatleben einer Person beziehen, sensibel sind, oder ob die betroffenen Personen auf irgendeine Weise belästigt wurden. Um rechtmäßig zu sein, muss der Eingriff mit sämtlichen in Artikel 52 Absatz 1 der Charta aufgelisteten Bedingungen übereinstimmen.

Gesetzlich vorgesehen sein

Einschränkungen des Rechts auf Schutz personenbezogener Daten müssen gesetzlich vorgesehen sein. Dieses Erfordernis besagt, dass Einschränkungen auf eine Rechtsgrundlage gestützt sein müssen, die hinreichend zugänglich und vorhersehbar und hinreichend bestimmt formuliert ist, dass die betroffenen Personen ihre Verpflichtungen verstehen und ihr Verhalten steuern können. Überdies muss die Rechtsgrundlage auch eine eindeutige Definition des Umfangs und der Art der Ausübung der Befugnisse der zuständigen Behörden enthalten, um die Personen vor willkürlichen Eingriffen zu schützen. Diese Auslegung ähnelt dem in der Rechtsprechung des EGMR enthaltenen Erfordernis eines „rechtmäßigen Eingriffs“,⁶⁰ und es wurde argumentiert, dass dem in der Charta verwendeten Ausdruck „gesetzlich vorgesehen“ dieselbe Bedeutung beigemessen werden sollte, wie sie dieser Ausdruck im Zusammenhang der EMRK hat.⁶¹ Die Rechtsprechung des EGMR und insbesondere der von ihm im Laufe der Jahre entwickelte Begriff der „Qualität des Gesetzes“ ist eine wichtige Überlegung, die es vom EuGH bei der Auslegung der Tragweite von Artikel 52 Absatz 1 der Charta zu berücksichtigen gilt.⁶²

60 EDSB (2017), *Necessity Toolkit*, Brüssel, 11. April 2017, S. 4; siehe auch EuGH, *Gutachten 1/15 des Gerichtshofs* [GK], 26. Juli 2017.

61 EuGH, Verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB / Post- och telestyrelsen und Secretary of State for the Home Department / Tom Watson, Peter Brice, Geoffrey Lewis*, Schlussanträge des Generalanwalts Henrik Saugmandsgaard Øe vom 19. Juli 2016, Randnr. 140.

62 EuGH, C-70/10, *Scarlet Extended SA / Société belge des auteurs compositeurs et éditeurs (SABAM)*, Schlussanträge des Generalanwalts Cruz Villalón vom 14. April 2011, Randnr. 100.

Den Wesensgehalt des Rechts achten

In der Rechtsordnung der EU muss jedwede Einschränkung der gemäß der Charta geschützten Grundrechte den Wesensgehalt dieser Rechte achten. Dies bedeutet, dass Einschränkungen, die so weitreichend und einschneidend sind, dass sie einem Grundrecht dessen grundlegenden Inhalt entziehen, nicht gerechtfertigt sein können. Wenn der Wesensgehalt des Rechts gefährdet ist, ist die Einschränkung als unrechtmäßig zu betrachten, ohne dass darüber hinaus zu beurteilen ist, ob sie einer Zielsetzung von allgemeinem Interesse dient und die Kriterien in Bezug auf die Erforderlichkeit und Verhältnismäßigkeit erfüllt.

Beispiel: In der Rechtssache *Schrems*⁶³ ging es um den Schutz natürlicher Personen bei der Übermittlung ihrer personenbezogenen Daten in Drittländer – im vorliegenden Fall in die Vereinigten Staaten. Schrems, ein österreichischer Staatsbürger, der seit einigen Jahren Facebook nutzte, reichte eine Beschwerde bei der irischen Datenschutzaufsichtsbehörde ein, um die Übermittlung seiner personenbezogenen Daten von der irischen Tochtergesellschaft von Facebook an Facebook Inc. und die sich in den Vereinigten Staaten befindenden Server anzuprangern, wo diese Daten verarbeitet wurden. Er argumentierte, dass das Recht und die Praxis der USA angesichts der 2013 erfolgten Enthüllungen des amerikanischen Whistleblowers Edward Snowden über die Überwachungstätigkeiten der US-Nachrichtendienste keinen ausreichenden Schutz der in das Hoheitsgebiet der USA übermittelten personenbezogenen Daten gewährleiste. Snowden hatte enthüllt, dass die National Security Agency die Server von Firmen wie Facebook direkt anzapfte und auf diese Weise die Inhalte von Chats und privaten Nachrichten lesen konnte.

Die Datenübermittlungen in die Vereinigten Staaten gründeten auf einer im Jahr 2000 angenommenen Angemessenheitsentscheidung der Kommission, die die Datenübermittlungen an US-Unternehmen erlaubte, die bescheinigten, aus der EU übermittelte personenbezogene Daten zu schützen und die sogenannten Grundsätze des „sicheren Hafens“ einzuhalten. Als die Rechtssache vor den EuGH gebracht wurde, prüfte dieser die Gültigkeit der Entscheidung der Kommission im Lichte der Charta. Er erinnerte daran, dass der Schutz der Grundrechte in der EU verlangt, dass sich die Ausnahmen und Einschränkungen auf das absolut Notwendige

63 EuGH, Rechtssache C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015.

beschränken. Eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, „verletzt“ nach Ansicht des EuGH „den Wesensgehalt des durch Artikel 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens“. Das Recht würde seiner Tragweite völlig beraubt, wenn den US-Behörden gestattet würde, auf die Kommunikation in beliebiger Weise, ohne jede auf konkrete Erwägungen der nationalen Sicherheit oder der Verbrechensverhütung, die speziell mit den betroffenen Personen in Zusammenhang stünden, basierende objektive Rechtfertigung und ohne begleitende angemessene Schutzmechanismen gegen den Machtmissbrauch zuzugreifen.

Überdies merkte der EuGH an, dass „eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken“, mit dem Grundrecht auf wirksamen gerichtlichen Rechtsschutz unvereinbar ist (Artikel 47 der Charta). Demnach konnte die Entscheidung in Bezug auf den „sicheren Hafen“ in den Vereinigten Staaten keinen Schutz gewährleisten, der dem in der Union nach Maßgabe der Richtlinie im Licht der Charta garantierten Schutz der Sache nach gleichwertig ist. Folglich erklärte der EuGH die Entscheidung für ungültig.⁶⁴

Beispiel: In der Rechtssache *Digital Rights Ireland*⁶⁵ untersuchte der EuGH die Vereinbarkeit der Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten) mit Artikel 7 und 8 der Charta. Die Richtlinie verpflichtete die Anbieter elektronischer Kommunikationsdienste, Verkehrs- und Standortdaten über einen Zeitraum von mindestens sechs Monaten und höchstens 24 Monaten zu speichern, und den zuständigen nationalen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von schweren Straftaten Zugang zu diesen Daten zu ermöglichen. Die Richtlinie gestattete keine Vorratsspeicherung des Inhalts der elektronischen Kommunikation. Der EuGH stellte fest, dass die Daten,

64 Die Entscheidung des EuGH zur Ungültigerklärung der Entscheidung 2000/520/EG der Kommission basierte auch auf anderen Gründen, die in anderen Abschnitten des vorliegenden Handbuchs untersucht werden. Insbesondere war der EuGH der Ansicht, dass die Entscheidung die Befugnisse der nationalen Datenschutzaufsichtsbehörden auf unrechtmäßige Weise beschränkte. Darüber hinaus gab es unter dem System des „sicheren Hafens“ für die Personen keine Rechtsbehelfe, die es ihnen erlaubten, Zugang zu den sie betreffenden personenbezogenen Daten zu erhalten und/oder deren Berichtigung oder Löschung zu erwirken. Folglich war auch der Wesensgehalt des in Artikel 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz gefährdet.

65 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014.

zu deren Speicherung die Anbieter nach Maßgabe der Richtlinie verpflichtet waren, Daten beinhalteten, die zur Rückverfolgung und Identifizierung der Quelle und der Adressaten einer Nachricht benötigt wurden, Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung, die Rufnummern des anrufenden und des angerufenen Anschlusses und die IP-Adressen. „Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.“

Folglich stellte die Vorratsspeicherung personenbezogener Daten nach Maßgabe der Richtlinie einen besonders schwerwiegenden Eingriff in die Rechte auf Privatsphäre und den Schutz personenbezogener Daten dar. Der EuGH entschied jedoch, dass der Eingriff den Wesensgehalt dieser Rechte nicht antastete. Was das Recht auf Privatsphäre betrifft, so wurde dessen Wesensgehalt nicht gefährdet, da die Richtlinie die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattete. Gleichermäßen wurde auch der Wesensgehalt des Rechts auf Schutz personenbezogener Daten nicht gefährdet, da die Richtlinie von den Anbietern elektronischer Kommunikationsdienste die Einhaltung bestimmter Grundsätze des Datenschutzes und der Datensicherheit und die zu diesem Zweck erfolgende Ergreifung geeigneter technischer und organisatorischer Maßnahmen verlangte.

Notwendigkeit und Verhältnismäßigkeit

Artikel 52 Absatz 1 der Charta besagt, dass Einschränkungen der Ausübung der von der Charta anerkannten Grundrechte und Grundfreiheiten unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden dürfen, wenn sie notwendig sind.

Eine Einschränkung kann **notwendig** sein, wenn Maßnahmen für das im öffentlichen Interesse verfolgte Ziel angenommen werden müssen, doch Notwendigkeit bedeutet gemäß der Auslegung des EuGH auch, dass die angenommenen Maßnahmen im Vergleich zu anderen Optionen für die Erreichung desselben Ziels weniger einschneidend sein müssen. In Bezug auf Einschränkungen des Rechts auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten wendet der EuGH eine strenge Notwendigkeitsprüfung an und

führt aus, dass „sich Ausnahmen und Einschränkungen auf das absolut Notwendige beschränken müssen“. Sofern eine Einschränkung als absolut notwendig erachtet wird, ist auch zu beurteilen, ob sie verhältnismäßig ist.

Verhältnismäßigkeit bedeutet, dass die sich aus der Einschränkung ergebenden Vorteile die Nachteile aufwiegen sollten, die Letztere auf die Ausübung der betreffenden Grundrechte hat.⁶⁶ Zur Senkung der Nachteile und Risiken in Bezug auf die Wahrnehmung der Rechte auf Privatsphäre und Datenschutz ist es wichtig, dass die Einschränkungen angemessene Garantien enthalten.

Beispiel: In der Rechtssache *Volker und Markus Schecke*⁶⁷ befand der EuGH, dass der Rat und die Kommission durch die Auferlegung einer Verpflichtung zur Veröffentlichung der personenbezogenen Daten aller natürlichen Personen, die Empfänger von Beihilfen aus bestimmten Landwirtschaftsfonds sind, ohne nach einschlägigen Kriterien wie den Zeiträumen, während deren sie solche Beihilfen erhalten haben, der Häufigkeit oder auch Art und Umfang dieser Beihilfen zu unterscheiden, die durch den Grundsatz der Verhältnismäßigkeit vorgegebenen Grenzen überschritten hätten.

Daher erachtete es der EuGH als erforderlich, bestimmte Bestimmungen der Verordnung (EG) Nr. 1290/2005 des Rates und die Verordnung Nr. 259/2008 in ihrer Gesamtheit für ungültig zu erklären.⁶⁸

Beispiel: In der Rechtssache *Digital Rights Ireland*⁶⁹ gefährdete der durch die Richtlinie über die Vorratsspeicherung von Daten verursachte Eingriff in das Recht auf Privatsphäre nach Auffassung des EuGH nicht den Wesensgehalt dieses Rechts, da die Richtlinie die Vorratsspeicherung des Inhalts der elektronischen Kommunikation verbot. Der EuGH befand jedoch, dass die

66 EDSB (2017), *Necessity Toolkit*, S. 5.

67 EuGH, Verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen* [GK], 9. November 2010, Randnm. 89 und 86.

68 Verordnung (EG) Nr. 1290/2005 des Rates vom 21. Juni 2005 über die Finanzierung der Gemeinsamen Agrarpolitik, ABl. L 209 vom 11.8.2005; Verordnung (EG) Nr. 259/2008 der Kommission vom 18. März 2008 mit Durchführungsbestimmungen zur Verordnung (EG) Nr. 1290/2005 des Rates hinsichtlich der Veröffentlichung von Informationen über die Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER), ABl. L 76 vom 19.3.2008.

69 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014, Randnr. 39.

Richtlinie mit Artikel 7 und 8 der Charta unvereinbar sei und erklärte sie für ungültig. Da die Gesamtheit der angesammelten Verkehrs- und Standortdaten analysiert werden und ein detailliertes Bild des Privatlebens des Einzelnen aufzeigen können, stelle sie einen schwerwiegenden Eingriff in diese Rechte dar. Der EuGH berücksichtigte, dass die Richtlinie die Vorratsspeicherung sämtlicher Metadaten betreffend Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie vorschrieb und somit für alle elektronischen Kommunikationsmittel galt, deren Nutzung im täglichen Leben jedes Einzelnen stark verbreitet ist. Sie stelle daher einen Eingriff dar, der fast die gesamte europäische Bevölkerung betreffe. In Anbetracht des Ausmaßes und der Schwere dieses Eingriffs könne die Vorratsspeicherung von Verkehrs- und Standortdaten nach Auffassung des EuGH ausschließlich zum Zwecke der Bekämpfung schwerer Kriminalität gerechtfertigt sein. Darüber hinaus sehe die Richtlinie keine objektiven Kriterien vor, die gewährleisten würden, den Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten auf das absolut Notwendige zu beschränken. Überdies enthalte sie keine materiell- und verfahrensrechtlichen Voraussetzungen, die den Zugang zu den auf Vorrat gespeicherten Daten und deren Nutzung seitens der nationalen Behörden regeln, die keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegen.

In den verbundenen Rechtssachen *Tele2 Sverige AB gegen Post- och telestyrelsen* und *Secretary of State for the Home Department gegen Tom Watson und andere* gelangte der EuGH zu einer ähnlichen Schlussfolgerung.⁷⁰ In diesen Rechtssachen ging es um die Vorratsspeicherung von Verkehrs- und Standortdaten „aller Teilnehmer und registrierten Nutzer und aller elektronischen Kommunikationsmittel sowie sämtlicher Verkehrsdaten“ ohne „Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel“.⁷¹ Im vorliegenden Fall stellte es keine Bedingung für die Vorratsspeicherung der Daten dar, ob eine Person direkt oder indirekt mit schweren Straftaten in Verbindung stand oder nicht oder ob ihre Kommunikation für die nationale Sicherheit maßgeblich war oder nicht. Angesichts des Fehlens eines erforderlichen Zusammenhangs zwischen den auf Vorrat gespeicherten Daten und einer Bedrohung für die öffentliche

70 EuGH, Verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB / Post- och telestyrelsen und Secretary of State for the Home Department / Tom Watson und andere*, 21. Dezember 2016, Randnr. 105–106.

71 a.a.O., Randnr. 105.

Sicherheit oder Beschränkungen in Bezug auf den Zeitraum oder ein geografisches Gebiet, befand der EuGH, dass die nationale Regelung die Grenzen des für die Bekämpfung schwerer Straftaten absolut Notwendigen übersteige.⁷²

Der Europäische Datenschutzbeauftragte verfolgt in seinem *Necessity Toolkit* („*Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken – Ein Toolkit*“) einen vergleichbaren Ansatz in Bezug auf die Notwendigkeit.⁷³ Das Toolkit ist als Hilfestellung bei der Beantwortung der Frage gedacht, ob vorgeschlagene Maßnahmen mit dem EU-Datenschutzrecht in Einklang stehen. Es wurde als Rüstzeug für Entscheidungsträger und Gesetzgeber der EU erarbeitet, die für die Ausarbeitung oder Prüfung von Maßnahmen zuständig sind, die die Verarbeitung personenbezogener Daten beinhalten und das Recht auf Schutz personenbezogener Daten oder andere in der Charta niedergelegte Rechte und Freiheiten einschränken.

Dem Gemeinwohl dienende Zielsetzungen

Um gerechtfertigt zu sein, muss jedwede Einschränkung der Ausübung der seitens der Charta anerkannten Rechte auch den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Was das Erfordernis des Schutzes der Rechte und Freiheiten anderer betrifft, so interagiert das Recht auf Schutz personenbezogener Daten häufig mit anderen Grundrechten. [Abschnitt 1.3](#) enthält eine detaillierte Analyse dieser Interaktionen. Was die dem Gemeinwohl dienenden Zielsetzungen betrifft, so umfassen diese die in Artikel 3 des Vertrags über die Europäische Union (EUV) bestätigten allgemeinen Ziele der EU wie die Förderung des Friedens und des Wohlergehens ihrer Völker, soziale Gerechtigkeit und sozialen Schutz und die Errichtung eines Raums der Freiheit, der Sicherheit und des Rechts, in dem – in Verbindung mit geeigneten Maßnahmen in Bezug auf die Verhütung und Bekämpfung der Kriminalität – der freie Personenverkehr gewährleistet ist, sowie andere durch spezifische Bestimmungen der Verträge geschützte Ziele und Interessen.⁷⁴ Die Datenschutz-Grundverordnung enthält diesbezüglich eine weitere Präzisierung

⁷² a.a.O., Randnr. 107.

⁷³ EDSB (2017), *Necessity Toolkit*, Brüssel, 11. April 2017.

⁷⁴ Erläuterungen zur Charta der Grundrechte (2007/C 303/02), ABL C 303 vom 14.12.2007, S. 17–35.

von Artikel 52 Absatz 1 der Charta: Artikel 23 Absatz 1 der Verordnung führt eine Reihe von dem Gemeinwohl dienenden Zielsetzungen an, die als rechtmäßige Einschränkung der Rechte der Einzelnen betrachtet werden, sofern die Einschränkung den Wesensgehalt des Rechts auf Schutz personenbezogener Daten achtet und notwendig und verhältnismäßig ist. Die nationale Sicherheit und die Landesverteidigung, die Verhütung von Straftaten, der Schutz wichtiger wirtschaftlicher und finanzieller Interessen der EU oder der Mitgliedstaaten, die öffentliche Gesundheit und die soziale Sicherheit zählen zu den darin genannten Zielsetzungen des öffentlichen Interesses.

Es ist wichtig, die dem Gemeinwohl dienende Zielsetzung, die durch die Einschränkung verfolgt wird, so detailliert wie möglich zu definieren und zu erläutern, da die Notwendigkeit der Einschränkung vor diesem Hintergrund beurteilt wird. Eine klare und detaillierte Beschreibung der Zielsetzung der Einschränkung und der vorgeschlagenen Maßnahmen ist von wesentlicher Bedeutung, damit festgestellt werden kann, ob sie erforderlich ist.⁷⁵ Die verfolgte Zielsetzung und die Notwendigkeit und Verhältnismäßigkeit der Einschränkung sind eng miteinander verbunden.

Beispiel: In der Rechtssache *Schwarz gegen Stadt Bochum*⁷⁶ ging es um Einschränkungen des Rechts auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten, die sich aus der Erfassung und Speicherung von Fingerabdrücken im Rahmen der Erteilung von Reisepässen durch die Behörden der Mitgliedstaaten ergeben.⁷⁷ Der Kläger beantragte bei der Stadt Bochum die Erteilung eines Reisepasses, verweigerte jedoch die Erfassung seiner Fingerabdrücke, woraufhin die Stadt Bochum seinen Antrag auf Erteilung eines Reisepasses ablehnte. Im Anschluss daran erhob er vor einem deutschen Gericht eine Klage mit dem Begehren, einen Reisepass ausgestellt zu bekommen, ohne Fingerabdrücke von ihm zu erfassen. Das deutsche Gericht verwies den Fall an den EuGH mit der Frage, ob Artikel 1 Absatz 2 der Verordnung (EG) Nr. 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten als gültig zu betrachten sei.

75 EDSB (2017), *Necessity Toolkit*, Brüssel, 11. April 2017, S. 4.

76 EuGH, C-291/12, *Michael Schwarz / Stadt Bochum*, 17. Oktober 2013.

77 a.a.O., Randnrn. 33–36.

Der EuGH wies darauf hin, dass Fingerabdrücke **personenbezogene Daten darstellen**, da sie objektiv unverwechselbare Informationen über natürliche Personen enthalten, die deren genaue Identifizierung ermöglichen, und die Erfassung und Speicherung von Fingerabdrücken eine Verarbeitung darstellt. Diese Verarbeitung, die in Artikel 1 Absatz 2 der Verordnung Nr. 2252/2004 geregelt ist, stellt einen Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten dar.⁷⁸ Nach Artikel 52 Absatz 1 der Charta sind jedoch Einschränkungen der Ausübung dieser Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit müssen sie erforderlich sein und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Im vorliegenden Fall stellte der EuGH erstens fest, dass die Einschränkung, die sich aus der Erfassung und Speicherung von Fingerabdrücken im Rahmen der Erteilung von Reisepässen ergibt, **gesetzlich vorgesehen ist**, da Artikel 1 Absatz 2 der Verordnung Nr. 2252/2004 dies vorsieht. Zweitens ist diese Verordnung auf den Schutz vor Fälschung von Pässen und die Verhinderung ihrer betrügerischen Verwendung ausgerichtet. Demnach bezweckt Artikel 1 Absatz 2 unter anderem, die illegale Einreise von Personen in das Unionsgebiet zu verhindern und verfolgt somit eine von der Union anerkannte dem Gemeinwohl dienende Zielsetzung. Drittens war weder den dem Gerichtshof vorliegenden Angaben zu entnehmen, noch war im Übrigen vorgetragen worden, dass im vorliegenden Fall durch die Einschränkungen der Ausübung dieser Rechte der Wesensgehalt dieser Rechte nicht geachtet worden wäre. Viertens erfordert die Speicherung von Fingerabdrücken auf einem Speichermedium mit hohem Sicherheitsstandard, wie sie in dieser Bestimmung vorgesehen ist, einen hohen technischen Entwicklungsstand. Sie ist daher geeignet, die Gefahr der Fälschung von Pässen zu verringern und die Aufgabe der mit der Überprüfung der Authentizität der Pässe an den Grenzen betrauten Stellen zu erleichtern. Es kommt nicht entscheidend darauf an, dass die genannte Methode nicht völlig zuverlässig ist. Zum einen reicht es nämlich aus, dass diese Methode, auch wenn sie die Akzeptanz unbefugter Personen nicht völlig ausschließt, die Gefahr solcher Akzeptanzen doch erheblich vermindert. In Anbetracht der vorstehenden Ausführungen stellte der EuGH fest, dass die Erfassung und die Speicherung von Fingerabdrücken, die in Artikel 1 Absatz 2

⁷⁸ a.a.O., Randnrn. 27–30.

der Verordnung Nr. 2252/2004 vorgesehen sind, geeignet sind, die mit dieser Verordnung angestrebten Ziele und damit das Ziel der Verhinderung der illegalen Einreise von Personen in das Unionsgebiet zu erreichen.⁷⁹

Im Anschluss daran prüfte der EuGH die **Erforderlichkeit** einer solchen Verarbeitung und stellte fest, dass die betreffende Erfassung nur in der Abnahme der Abdrücke zweier Finger besteht. Diese Finger sind auch normalerweise den Blicken anderer Personen ausgesetzt, so dass die Erfassung kein Vorgang intimer Natur ist. Ebenso wie die Aufnahme des Gesichtsbildes führt auch sie nicht zu einer besonderen körperlichen oder psychischen Unannehmlichkeit für den Betroffenen. Es ist darauf hinzuweisen, dass die einzige im Lauf des Verfahrens vor dem EuGH angesprochene echte Alternative zur Erfassung der Fingerabdrücke in der Erfassung eines Bildes der Iris des Auges bestand. Nichts in den dem EuGH vorgelegten Akten deutete indessen darauf hin, dass dieses Verfahren weniger stark in die durch die Artikel 7 und 8 der Charta anerkannten Rechte eingreife als die Erfassung der Fingerabdrücke. Außerdem ist, was die Wirksamkeit dieser beiden Methoden betrifft, das Verfahren der Iris-Erkennung unstreitig technisch noch nicht so ausgereift wie das der Erfassung von Fingerabdrücken, ist gegenwärtig deutlich kostspieliger als das des Abgleichs von Fingerabdrücken und deshalb für eine allgemeine Anwendung weniger geeignet. Demgemäß wurde dem Gerichtshof nicht zur Kenntnis gebracht, dass es Maßnahmen gäbe, die hinreichend wirksam zum Ziel des Schutzes vor betrügerischer Verwendung von Reisepässen beitragen könnten und dabei weniger schwerwiegend in die durch die Artikel 7 und 8 der Charta anerkannten Rechte eingriffen als das auf den Fingerabdrücken beruhende Verfahren.⁸⁰

Der EuGH stellte fest, dass Artikel 4 Absatz 3 der Verordnung Nr. 2252/2004 ausdrücklich vorsieht, dass die Fingerabdrücke nur zu dem Zweck verwendet werden dürfen, die Authentizität des Passes und die Identität seines Inhabers zu überprüfen, während Artikel 1 Absatz 2 der Verordnung die Speicherung der Fingerabdrücke nur im Reisepass selbst vorsieht, der im ausschließlichen Besitz seines Inhabers bleibt. Folglich stellte die Verordnung keine Rechtsgrundlage für eine etwaige Zentralisierung der auf ihrer Grundlage erfassten Daten oder für eine Nutzung dieser Daten zu anderen Zwecken als der Verhinderung der illegalen Einreise von Personen in das

79 a.a.O., Randnrn. 35–45.

80 EuGH, C-291/12, *Michael Schwarz / Stadt Bochum*, 17. Oktober 2013, Randnrn. 46–53.

Unionsgebiet dar.⁸¹ Nach alledem befand der EuGH, dass die Prüfung der Vorlagefrage nichts ergeben habe, was die Gültigkeit von Artikel 1 Absatz 2 der Verordnung Nr. 2252/2004 beeinträchtigen könnte.

Beziehung zwischen der Charta und der EMRK

Trotz Verwendung eines anderen Wortlauts erinnern die Bedingungen für rechtmäßige Einschränkungen der in Artikel 52 Absatz 1 der Charta enthaltenen Rechte an Artikel 8 Absatz 2 der EMRK über das Recht auf Achtung des Privatlebens. Der EuGH und der EGMR verweisen in ihrer Rechtsprechung häufig auf die Urteile des jeweils anderen Gerichtshofs, was Teil des kontinuierlichen Dialogs zwischen den beiden Gerichtshöfen ist, der auf den Erhalt einer harmonischen Auslegung der Datenschutzvorschriften abzielt. Artikel 52 Absatz 3 der Charta setzt fest: „Soweit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird.“ Artikel 8 der Charta entspricht jedoch nicht unmittelbar einem Artikel der EMRK.⁸² Artikel 52 Absatz 3 der Charta betrifft den Inhalt und die Tragweite der durch jedes Rechtssystem geschützten Rechte und nicht die Bedingungen für deren Einschränkung. In Anbetracht des weiter gefassten Rahmens des Dialogs und der Zusammenarbeit zwischen den beiden Gerichtshöfen kann der EuGH bei seinen Analysen jedoch die Kriterien für rechtmäßige Einschränkungen gemäß Artikel 8 EMRK in deren Auslegung durch den EGMR berücksichtigen. Auch das entgegengesetzte Szenario ist möglich, in dem der EGMR auf die Bedingungen für rechtmäßige Einschränkungen nach Maßgabe der Charta verweisen kann. In jedem Fall sollte auch berücksichtigt werden, dass die EMRK kein perfektes Gegenstück zu Artikel 8 der Charta enthält, der sich auf den Schutz personenbezogener Daten bezieht und insbesondere auf die Rechte der betroffenen Person, die berechtigten Gründe für die Verarbeitung und die Aufsicht durch eine unabhängige Stelle. Einige Bestandteile von Artikel 8 der Charta können in der seitens des EGMR zu Artikel 8 EMRK entwickelten Rechtsprechung in Bezug auf das Übereinkommen Nr. 108 begründet sein.⁸³ Diese Verbindung gewährleistet die gegenseitige Inspiration zwischen dem EuGH und dem EGMR im Hinblick auf Angelegenheiten im Bereich des Datenschutzes.

81 a.a.O., Randnrn. 56–61.

82 EDSB (2017), *Necessity Toolkit*, Brussels, 11. April 2017, S. 6.

83 Erläuterungen zur Charta der Grundrechte (2007/C 303/02), Artikel 8.

1.3. Interaktion mit anderen Rechten und berechtigten Interessen

Kernpunkte

- Das Recht auf Datenschutz interagiert häufig mit anderen Rechten wie der Freiheit der Meinungsäußerung und dem Recht zum Empfang und zur Offenlegung von Informationen.
- Diese Interaktion ist häufig ambivalent: während es Situationen gibt, in denen das Recht auf Schutz personenbezogener Daten mit einem bestimmten Recht in Konflikt steht, gibt es auch Situationen, in denen das Recht auf Schutz personenbezogener Daten die Achtung desselben konkreten Rechts wirksam gewährleistet. Dies trifft beispielsweise auf die Freiheit der Meinungsäußerung zu, da das Berufsgeheimnis ein Bestandteil des Rechts auf Achtung des Privatlebens ist.
- Das Erfordernis zum Schutz der Rechte und Freiheiten anderer ist eines der Kriterien, das für die Bewertung der rechtmäßigen Einschränkung des Rechts auf Schutz personenbezogener Daten herangezogen wird.
- Wenn unterschiedliche Rechte betroffen sind, müssen die Gerichte zwischen den Rechten abwägen, um diese in Einklang zu bringen.
- Die Datenschutz-Grundverordnung verpflichtet die Mitgliedstaaten, das Recht auf Schutz personenbezogener Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.
- Die Mitgliedstaaten können auch konkrete Bestimmungen in ihr innerstaatliches Recht aufnehmen, um das Recht auf Schutz personenbezogener Daten mit dem öffentlichen Zugang zu amtlichen Dokumenten und den Verpflichtungen des Berufsgeheimnisses in Einklang zu bringen.

Das Recht auf Schutz personenbezogener Daten ist kein absolutes Recht; die Bedingungen für die rechtmäßige Einschränkung dieses Rechts wurden oben dargelegt. Eines der sowohl im Recht des Europarates als auch im EU-Recht anerkannten Kriterien für rechtmäßige Einschränkungen von Rechten besteht darin, dass der Eingriff in den Datenschutz für den Schutz der Rechte und Freiheiten anderer erforderlich ist. In Fällen, in denen der Datenschutz mit anderen Rechten interagiert, haben sowohl der EGMR als auch der EuGH wiederholt ausgeführt, dass bei der Anwendung und Auslegung von Artikel 8 EMRK

und Artikel 8 der Charta ein Abwägen mit anderen Rechten erforderlich ist.⁸⁴ Wir werden anhand mehrerer wichtiger Beispiele veranschaulichen, wie dieses Abwägen erzielt wird.

Zusätzlich zu dem seitens dieser Gerichte durchgeführten Abwägen, können die Staaten bei Bedarf Rechtsvorschriften erlassen, um das Recht auf Schutz personenbezogener Daten mit anderen Rechten in Einklang zu bringen. Aus diesem Grund sieht die Datenschutz-Grundverordnung eine Reihe von Bereichen vor, in denen nationale Abweichungen möglich sind.

In Bezug auf die Freiheit der Meinungsäußerung verpflichtet die DSGVO die Mitgliedstaaten, „das Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken“ durch Rechtsvorschriften in Einklang zu bringen.⁸⁵ Die Mitgliedstaaten können auch Rechtsvorschriften erlassen, um den Datenschutz mit dem Zugang der Öffentlichkeit zu amtlichen Dokumenten und dem als Bestandteil des Rechts auf Achtung des Privatlebens geschützten Berufsgeheimnis in Einklang zu bringen.⁸⁶

1.3.1. Freiheit der Meinungsäußerung

Eines der Rechte, das am stärksten mit dem Recht auf Datenschutz interagiert, ist das Recht auf freie Meinungsäußerung.

Die Freiheit der Meinungsäußerung wird geschützt durch Artikel 11 der Charta („Freiheit der Meinungsäußerung und Informationsfreiheit“). Dieses Recht „schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben“. Die Informationsfreiheit gemäß Artikel 11 der Charta und Artikel 10 EMRK schützt nicht nur das Recht, Informationen mitzuteilen, sondern auch zu *empfangen*.

84 EGMR, *Von Hannover / Deutschland (Nr. 2)* [GK], Nrn. 40660/08 und 60641/08, 7. Februar 2012; EuGH, Verbundene Rechtssachen C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECMD) / Administración del Estado*, 24. November 2011, Randnr. 48; EuGH, C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, 29. Januar 2008, Randnr. 68.

85 Datenschutz-Grundverordnung, Artikel 85.

86 a.a.O., Artikel 86 und 90.

Einschränkungen der Freiheit der Meinungsäußerung müssen die in Artikel 52 Absatz 1 der Charta vorgesehenen und oben beschriebenen Kriterien erfüllen. Außerdem entspricht Artikel 11 Artikel 10 EMRK. Gemäß Artikel 52 Absatz 3 der Charta gilt: Soweit diese Charta Rechte enthält, die den durch die EMRK garantierten Rechten entsprechen, „haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird“. Die Einschränkungen, die rechtmäßig auf das in Artikel 11 der Charta festgeschriebene Recht angewandt werden können, dürfen daher über die in Artikel 10 Absatz 2 EMRK vorgesehenen Einschränkungen nicht hinausgehen, müssen also gesetzlich vorgesehen sein und in einer demokratischen Gesellschaft „zum Schutz [...] des guten Rufes oder der Rechte anderer“ notwendig sein. Solche Rechte umfassen insbesondere das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten.

Die Beziehung zwischen dem Schutz personenbezogener Daten und der Meinungsfreiheit ist in Artikel 85 der Datenschutz-Grundverordnung mit dem Titel „Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit“ geregelt. Nach Maßgabe dieses Artikels bringen die Mitgliedstaaten das Recht auf Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang. Ausnahmen und Abweichungen von bestimmten Kapiteln der Datenschutz-Grundverordnung sind insbesondere zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken vorzusehen, sofern dies erforderlich ist, um das Recht auf Schutz personenbezogener Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

Beispiel: In der Rechtssache *Tietosuojaalvutettu gegen Satakunnan Markkinapörssi Oy und Satamedia Oy*⁸⁷ war der EuGH aufgefordert, die Beziehung zwischen Datenschutz und Pressefreiheit festzulegen.⁸⁸ Er hatte die über einen SMS-Dienst erfolgte Verbreitung von Steuerdaten über rund 1,2 Millionen natürliche Personen zu prüfen, die ein Unternehmen

87 EuGH, C-73/07, *Tietosuojaalvutettu / Satakunnan Markkinapörssi Oy und Satamedia Oy* [GK], 16. Dezember 2008, Randnrn. 56, 61 und 62.

88 Die Rechtssache betraf die Auslegung von Artikel 9 der Datenschutzrichtlinie - nunmehr ersetzt durch Artikel 85 der Datenschutz-Grundverordnung - der wie folgt lautet: „Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von diesem Kapitel sowie von den Kapiteln IV und VI nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen“.

auf legalem Wege von den finnischen Steuerbehörden erhalten hatte. Die finnische Datenschutzaufsichtsbehörde hatte eine Entscheidung erlassen, in der sie das Unternehmen zur Beendigung der Verbreitung dieser Daten aufforderte. Das Unternehmen legte gegen diese Entscheidung Widerspruch vor einem innerstaatlichen Gericht ein, das den EuGH um die Klärung der Auslegung der Datenschutzrichtlinie ersuchte. Der EuGH hatte insbesondere der Frage nachzugehen, ob die Verarbeitung personenbezogener Daten, die die Steuerbehörden zur Verfügung gestellt hatten, damit Nutzer von Mobiltelefonen Steuerdaten anderer natürlicher Personen erhalten können, als eine Tätigkeit anzusehen ist, die allein journalistischen Zwecken dient. Nachdem der EuGH zu dem Schluss gekommen war, die Tätigkeiten des Unternehmens seien „Verarbeitung personenbezogener Daten“ im Sinne von Artikel 3 Absatz 1 der Datenschutzrichtlinie, wandte er sich der Auslegung von Artikel 9 der Richtlinie (über die Verarbeitung personenbezogener Daten und die Meinungsfreiheit) zu. Er wies zunächst auf die Bedeutung des Rechts auf freie Meinungsäußerung in jeder demokratischen Gesellschaft hin und vertrat die Auffassung, dass die damit zusammenhängenden Begriffe, zu denen auch der Journalismus gehört, weit auszulegen sind. Weiter führte er aus, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Datenschutz auf das absolut Notwendige beschränken müssen, um ein Gleichgewicht zwischen den beiden Grundrechten herzustellen. Der EuGH vertrat die Auffassung, dass Tätigkeiten wie die von den betreffenden Unternehmen, die Daten aus Dokumenten betreffen, die nach den nationalen Rechtsvorschriften öffentlich sind, als „journalistische Tätigkeiten“ eingestuft werden können, wenn sie zum Zweck haben, Informationen, Meinungen oder Ideen, mit welchem Übertragungsmittel auch immer, in der Öffentlichkeit zu verbreiten. Er befand ferner, dass diese Tätigkeiten nicht Medienunternehmen vorbehalten sind und mit der Absicht verbunden sein können, Gewinn zu erzielen. Der EuGH überließ es jedoch dem innerstaatlichen Gericht, zu prüfen, ob dies auf die speziellen Umstände dieses Falls zutrifft.

Dieselbe Rechtssache wurde auch vom EGMR geprüft, nachdem das innerstaatliche Gericht auf Grundlage der Orientierungshilfe des EuGH entschied, dass die Anordnung der Aufsichtsbehörde in Bezug auf die Einstellung der Veröffentlichung sämtlicher Steuerdaten einen gerechtfertigten Eingriff in die Freiheit der Meinungsäußerung des Unternehmens darstellte. Der EGMR hielt diesen Ansatz aufrecht.⁸⁹ Er stellte fest, dass trotz des

89 EGMR, *Satakunnan Markkinapörssi Oy und Satamedia Oy / Finland*, Nr. 931/13, 27. Juni 2017.

Vorliegens eines Eingriffs in das Recht des Unternehmens zur Erteilung von Informationen, dieser Eingriff gesetzlich vorgesehen war, ein berechtigtes Ziel verfolgte und in einer demokratischen Gesellschaft notwendig war.

Der Gerichtshof erinnerte an die Rechtsprechungskriterien, die die nationalen Behörden und den EGMR selbst beim Abwägen der Freiheit der Meinungsäußerung mit dem Recht auf Achtung des Privatlebens leiten sollten. Wenn es um politische Reden oder eine Debatte über ein Thema von öffentlichem Interesse geht, gibt es nur einen geringen Spielraum für die Einschränkung des Rechts auf das Empfangen und Weitergeben von Informationen, da die Öffentlichkeit das Recht darauf hat, informiert zu werden, „und dies ist in einer demokratischen Gesellschaft ein unerlässliches Recht“.⁹⁰ Presseartikel, die allein darauf abzielen, die Neugier einer bestimmten Leserschaft in Bezug auf Einzelheiten aus dem Privatleben einer Person zu stillen, können jedoch nicht als Beitrag zu einer Debatte von öffentlichem Interesse betrachtet werden. Die zu journalistischen Zwecken erfolgende Ausnahme von den Datenschutzvorschriften soll Journalisten den Zugang zu, die Erhebung und die Verarbeitung von Daten ermöglichen, damit diese ihren journalistischen Tätigkeiten nachkommen können. Folglich bestand in der Tat ein öffentliches Interesse daran, den Zugang zu den großen Mengen an Steuerdaten bereitzustellen und den beschwerdeführenden Unternehmen deren Erhebung und Verarbeitung zu ermöglichen. Der Gerichtshof stellte hingegen fest, dass an der in unveränderter Form und ohne jedweden analytischen Beitrag erfolgten Massenverbreitung dieser Rohdaten seitens der Zeitungen kein öffentliches Interesse bestand. Die Informationen über die Besteuerung hätten neugierigen Bürgern möglicherweise die Einstufung von Personen nach Maßgabe ihrer wirtschaftlichen Lage ermöglicht und den Durst der Öffentlichkeit nach Informationen über das Privatleben anderer gestillt. Dies könne nicht als Beitrag zu einer Debatte von öffentlichem Interesse betrachtet werden.

Beispiel: In der Rechtssache *Google Spain*⁹¹ prüfte der EuGH, ob Google zur Löschung veralteter Informationen über die finanziellen Schwierigkeiten des Beschwerdeführers aus seiner Suchergebnisliste verpflichtet war. Bei der unter Eingabe des Namens des Beschwerdeführers erfolgenden Durchführung einer Suche in der Google Suchmaschine, lieferten die Suchergebnisse Links zu alten Zeitungsartikeln, aus denen dessen Verbindung zu Konkursverfahren

90 a.a.O., Randnr. 169.

91 EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014, Randnrn. 81–83.

hervorging. Nach Ansicht des Beschwerdeführers stelle dies eine Verletzung seiner Rechte auf Achtung des Privatlebens und Schutz personenbezogener Daten dar, da die Verfahren vor Jahren abgeschlossen wurden und diese Verweise demnach nicht erheblich seien.

Der EuGH legte zunächst dar, dass Internetsuchmaschinen und Suchergebnisse, die personenbezogene Daten liefern, ein detailliertes Profil einer Person erstellen können. Um den Einzelnen ein hohes Datenschutzniveau zu gewährleisten, ist es vor dem Hintergrund einer zunehmend digitalisierten Gesellschaft von grundlegender Bedeutung, dass personenbezogene Daten sachlich richtig sind und deren Veröffentlichung nicht über das erforderliche Maß der Information der Öffentlichkeit hinausgeht. Der „für die Verarbeitung Verantwortliche muss in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür sorgen, dass die Verarbeitung den Anforderungen“ des EU-Rechts „genügt“, damit die eingerichteten gesetzlichen Garantien ihre volle Wirkung entfalten. Dies bedeutet, dass das Recht auf Löschung seiner personenbezogenen Daten im Falle einer nicht länger erforderlichen oder veralteten Verarbeitung auch Suchmaschinen umfasst, in Bezug auf die festgestellt wurde, dass es sich dabei um für die Verarbeitung Verantwortliche und nicht lediglich um Auftragsverarbeiter handelt (siehe [Abschnitt 2.3.1](#)).

Im Rahmen der Prüfung, ob Google zur Entfernung der mit dem Beschwerdeführer im Zusammenhang stehenden Links verpflichtet war, befand der EuGH, dass natürliche Personen unter bestimmten Voraussetzungen das Recht auf die Löschung ihrer personenbezogenen Daten aus den Suchergebnissen einer Internetsuchmaschine haben. Dieses Recht kann geltend gemacht werden, wenn Informationen in Bezug auf eine natürliche Person sachlich unrichtig sind oder den Zwecken der Datenverarbeitung nicht entsprechen, dafür nicht erheblich sind oder darüber hinausgehen. Der EuGH erkannte an, dass es sich dabei nicht um ein absolutes Recht handelt; es muss gegen andere Rechte abgewogen werden, und hierbei insbesondere gegen das Interesse und das Recht der breiten Öffentlichkeit auf Zugang zu dieser Information. Jede beantragte Löschung erfordert eine individuelle Beurteilung, um ein Gleichgewicht zwischen den Grundrechten auf Schutz personenbezogener Daten und auf Achtung des Privatlebens der betroffenen Person einerseits und den berechtigten Interessen aller Internetnutzer andererseits anzustreben.

Der EuGH stellte eine Orientierungshilfe in Bezug auf die im Zuge des Abwägens zu berücksichtigenden Faktoren bereit. Bei der Art der betreffenden Informationen handelt es sich um einen besonders wichtigen Faktor. Sofern es sich um Informationen handelt, die für das Privatleben der natürlichen Person sensibel sind, und kein öffentliches Interesse an der Verfügbarkeit der Informationen besteht, überwiegen der Datenschutz und die Privatsphäre gegenüber dem Recht der breiten Öffentlichkeit auf Zugang zu den Informationen. Stellt sich hingegen heraus, dass es sich bei der betroffenen Person um eine Persönlichkeit des öffentlichen Lebens handelt, oder die Informationen derart sind, dass sie die Gewährung des Zugangs der breiten Öffentlichkeit zu diesen Informationen rechtfertigen, ist der Eingriff in die Grundrechte auf Datenschutz und auf Achtung der Privatsphäre gerechtfertigt.

Im Anschluss an das Urteil nahm die Artikel-29-Datenschutzgruppe Leitlinien zur Umsetzung der Entscheidung des EuGH an. Die Leitlinien umfassen eine Liste der gemeinsamen Kriterien, die seitens der Aufsichtsbehörden für die Bearbeitung von Beschwerden in Bezug auf Löschungsanträge natürlicher Personen zu verwenden sind und diese beim Abwägen von Rechten leiten sollen.⁹²

Zur Frage der Vereinbarkeit des Rechts auf Datenschutz mit dem Recht auf freie Meinungsäußerung hat der EGMR mehrere Grundsatzurteile gesprochen.

Beispiel: In der Rechtssache *Axel Springer AG gegen Deutschland*⁹³ befand der EGMR, dass eine einstweilige Verfügung, die das beschwerdeführende Unternehmen von der Veröffentlichung eines Artikels über die Verhaftung und Verurteilung eines bekannten Schauspielers abhielt, eine Verletzung von Artikel 10 EMRK darstelle. Der EGMR verwies erneut auf die in seiner Rechtsprechung festgelegten Kriterien, die bei der Abwägung zwischen dem Recht auf Freiheit der Meinungsäußerung und dem Recht auf Achtung des Privatlebens zu berücksichtigen sind:

- Handelt es sich bei dem Ereignis, um das es in dem betreffenden Artikel ging, um ein Ereignis von allgemeinem Interesse?

92 Artikel-29-Datenschutzgruppe (2014), *Leitlinien für die Umsetzung des Urteils des Gerichtshofs der Europäischen Union in der Rechtssache C-131/12 „Google Spanien und Inc/Agencia Española de Protección de Datos (AEPD) und Mario Costeja González“*, WP 225, Brüssel, 26. November 2014.

93 EGMR, *Axel Springer AG / Deutschland* [GK], Nr. 39954/08, 7. Februar 2012, Randnrn. 90 und 91.

- Handelt es sich bei der betreffenden Person um eine Person öffentlichen Interesses?
- Wie wurden die Informationen beschafft und waren sie zuverlässig?

Der EGMR stellte fest, dass die Verhaftung und Verurteilung des Schauspielers eine öffentliche juristische Tatsache und damit von öffentlichem Interesse war, dass der Schauspieler hinreichend bekannt und damit eine Person öffentlichen Interesses war, und dass die Informationen von der Staatsanwaltschaft stammten und deren Richtigkeit zwischen den Parteien unstrittig war. Daher standen die dem Unternehmen auferlegten Einschränkungen bezüglich der Veröffentlichung in keinem angemessenen Verhältnis zu dem legitimen Ziel des Schutzes des Privatlebens des Beschwerdeführers. Der Gerichtshof befand, dass eine Verletzung von Artikel 10 EMRK vorlag.

Beispiel: Die Rechtssache *Coudec und Hachette Filipacchi Associés gegen Frankreich*⁹⁴ betraf die seitens einer französischen Wochenzeitschrift erfolgte Veröffentlichung eines Interviews mit Frau Coste, die behauptete, dass Fürst Albert von Monaco der Vater ihres Sohnes sei. Das Interview beschrieb auch die Beziehung zwischen Frau Coste und dem Fürsten und die Art und Weise, auf die dieser auf die Geburt des Kindes reagierte. Begleitet war der Artikel von Fotos des Fürsten mit dem Kind. Fürst Albert verklagte den Verlag wegen Verletzung seines Rechts auf Schutz des Privatlebens. Die französischen Gerichte waren der Auffassung, dass die Veröffentlichung des Artikels für Fürst Albert zu einem unwiderruflichen Schaden geführt habe und verurteilten den Verlag zur Entrichtung von Schadensersatz und zur Veröffentlichung der Einzelheiten des Urteils auf dem Titelblatt der Zeitschrift.

Die Herausgeber der Zeitschrift brachten die Rechtssache vor den EGMR und behaupteten, dass das Urteil der französischen Gerichte einen ungerechtfertigten Eingriff in ihr Recht auf freie Meinungsäußerung darstelle. Der EGMR musste Fürst Alberts Recht auf Achtung seines Privatlebens gegen das Recht des Herausgebers auf freie Meinungsäußerung und das Recht der breiten Öffentlichkeit auf Erhalt der Information abwägen. Auch das

94 EGMR, *Coudec und Hachette Filipacchi Associés / Frankreich* [GK], Nr. 40454/07, 10. November 2015.

Recht von Frau Coste, ihre Geschichte mit der Öffentlichkeit zu teilen, und das Interesse des Kindes an einer amtlichen Anerkennung der Vater-Kind-Beziehung waren wichtige Aspekte.

Der EGMR befand, dass die Veröffentlichung des Interviews einen Eingriff in das Privatleben des Fürsten darstelle und prüfte daraufhin, ob der Eingriff notwendig war. Er vertrat die Auffassung, dass die Veröffentlichung eine Persönlichkeit des öffentlichen Lebens und eine Angelegenheit des öffentlichen Interesses betreffe, da die Bürger von Monaco Interesse daran hatten, über die Existenz eines Kindes des Fürsten informiert zu werden, da die Zukunft einer Erbmonarchie „untrennbar mit der Existenz von Nachkommen verbunden“ und demnach eine Angelegenheit von öffentlichem Interesse sei.⁹⁵ Der Gerichtshof hob auch hervor, dass der Artikel Frau Coste und ihrem Kind die Ausübung ihres Rechts auf freie Meinungsäußerung ermöglicht habe. Die innerstaatlichen Gerichte hätten die in der Rechtsprechung des EGMR für die Abwägung des Rechts auf Achtung des Privatlebens und des Rechts auf Meinungsäußerungsfreiheit dargelegten Grundsätze und Kriterien nicht ausreichend berücksichtigt. Er befand, dass Frankreich Artikel 10 EMRK über die Freiheit der Meinungsäußerung verletzt habe.

In der Rechtsprechung des EGMR gehört zu den zentralen Kriterien bei der Abwägung dieser Rechte die Frage, ob die fragliche Äußerung einen Beitrag zu einer Debatte von allgemeinem Interesse leistet.

Beispiel: In der Rechtssache *Mosley gegen Vereinigtes Königreich*⁹⁶ veröffentlichte eine nationale Wochenzeitung intime Fotos des Beschwerdeführers, einer bekannten Persönlichkeit, der den Herausgeber im Anschluss daran mit Erfolg verklagte und Schadensersatz gewährt bekam. Trotz der gewährten finanziellen Entschädigung beschwerte er sich darüber, einer Verletzung seines Rechts auf Privatsphäre zum Opfer gefallen zu sein, da ihm die Möglichkeit verweigert wurde, vor der Veröffentlichung der betreffenden Fotos eine Unterlassungsklage anzustrengen, da für die Zeitung keine gesetzliche Pflicht zur Vorabnotifizierung der Veröffentlichung besteht.

⁹⁵ a.a.O., Randnrn. 104–116.

⁹⁶ EGMR, *Mosley / Vereinigtes Königreich*, Nr. 48009/08, 10. Mai 2011, Randnrn. 129 und 130.

Der EGMR hob hervor, dass wenngleich die Verbreitung dieses Materials generell eher der Unterhaltung als der Erziehung diene, sie zweifelsohne in den Genuss des Schutzes von Artikel 10 EMRK kam, der möglicherweise hinter die Anforderungen von Artikel 8 EMRK zu stellen ist, wenn die Information von privater und intimer Natur war und an ihrer Verbreitung kein öffentliches Interesse bestand. Besondere Sorgfalt war jedoch bei der Prüfung von Einschränkungen geboten, die als eine Art Zensur vor der Veröffentlichung wirken könnten. In Anbetracht der potenziell abschreckenden Wirkung einer Vorabnotifizierungspflicht, der Zweifel an deren Wirksamkeit und des großen Ermessensspielraums in diesem Bereich merkte der EGMR an, dass Artikel 8 keine rechtlich verbindliche Vorabnotifizierungspflicht verlangt. Folglich befand der Gerichtshof, dass keine Verletzung von Artikel 8 vorlag.

Beispiel: In der Rechtssache *Bohlen gegen Deutschland*⁹⁷ hatte der Beschwerdeführer, ein bekannter Sänger und Musikproduzent, eine Autobiographie veröffentlicht und wurde im Anschluss daran dazu gezwungen, einige Passagen aufgrund von Gerichtsentscheidungen zu streichen. Über die Geschichte wurde in den nationalen Medien umfangreich berichtet und ein Tabakunternehmen startete eine humoristische Werbekampagne in Bezug auf dieses Ereignis, in deren Rahmen sie den Vornamen des Beschwerdeführers ohne dessen Einwilligung verwendete. Der Beschwerdeführer machte eine Verletzung seiner Rechte gemäß Artikel 8 EMRK geltend und forderte vom Werbeunternehmen erfolglos Schadensersatz. Der EGMR verwies erneut auf die Kriterien, die bei der Abwägung zwischen dem Recht auf Achtung des Privatlebens und dem Recht auf freie Meinungsäußerung zu berücksichtigen sind und befand, dass keine Verletzung von Artikel 8 vorlag. Beim Beschwerdeführer handelte es sich um eine Persönlichkeit des öffentlichen Lebens und die Werbung bezog sich nicht auf die Einzelheiten seines Privatlebens sondern auf ein öffentliches Ereignis, über das in den Medien bereits berichtet worden war und das Bestandteil einer öffentlichen Auseinandersetzung war. Darüber hinaus war die Werbung humorvoll und enthielt keinerlei abwertende oder negative Inhalte in Bezug auf den Beschwerdeführer.

Beispiel: In der Rechtssache *Biriuk gegen Litauen*⁹⁸ argumentierte die Beschwerdeführerin vor dem EGMR, dass Litauen seiner Pflicht zur Gewährleistung der Achtung ihres Rechts auf Privatleben nicht

97 EGMR, *Bohlen / Deutschland*, Nr. 53495/09, 19. Februar 2015, Randnrn. 45–60.

98 EGMR, *Biriuk / Litauen*, Nr. 23373/03, 25. November 2008.

nachgekommen sei, da ihr seitens der innerstaatlichen Gerichte, die die Rechtssache geprüft hatten, ein finanzieller Schadensersatz in Höhe einer lächerlichen Summe gewährt worden sei, obgleich eine große Zeitung ihre Privatsphäre schwer verletzt habe. Bei der Gewährung des immateriellen Schadensersatzes hatten die innerstaatlichen Gerichte die Bestimmungen des nationalen Gesetzes über die Bereitstellung von Informationen an die Öffentlichkeit angewandt, die eine niedrige Obergrenze für die Entschädigung immaterieller Schäden auferlegten, die durch die unrechtmäßige öffentliche Verbreitung von Informationen über das Privatleben einer Person durch die Medien verursacht wurden. Die Rechtssache gründete auf der auf der Titelseite der größten litauischen Tageszeitung erfolgten Veröffentlichung eines Artikels, der darüber berichtete, dass die Beschwerdeführerin HIV-positiv sei. Der Artikel kritisierte auch das Verhalten der Beschwerdeführerin und stellte ihre moralischen Werte in Frage.

Der EGMR rief in Erinnerung, dass der Schutz personenbezogener Daten und nicht zuletzt medizinischer Daten nach Maßgabe der EMRK von grundlegender Bedeutung für das Recht auf Achtung des Privatlebens sei. Die Vertraulichkeit von Gesundheitsdaten ist dabei von besonderer Bedeutung, da die Offenlegung medizinischer Daten (im vorliegenden Fall der HIV-Status der Beschwerdeführerin) das Privat- und Familienleben einer Person, ihre Beschäftigungssituation und ihre Einbeziehung in die Gesellschaft erheblich beeinträchtigen kann. Besonderes Gewicht maß der Gerichtshof der Tatsache bei, dass laut Zeitungsbericht ärztliches Personal des Krankenhauses die Informationen über den HIV-Status der Beschwerdeführerin weitergegeben und damit ganz offensichtlich gegen die ärztliche Schweigepflicht verstoßen hatte. Folglich stellte dies keinen berechtigten Eingriff in das Recht der Beschwerdeführerin auf Achtung ihres Privatlebens dar.

Der Artikel wurde von der Presse veröffentlicht und auch die Freiheit der Meinungsäußerung ist nach Maßgabe der EMRK ein Grundrecht. Bei der Prüfung, ob das Vorliegen eines öffentlichen Interesses die Veröffentlichung dieser Art von Informationen über die Beschwerdeführerin rechtfertige, stellte der Gerichtshof jedoch fest, dass der Hauptzweck der Veröffentlichung in der Steigerung der Verkaufszahlen der Zeitung durch die Befriedigung der Neugier der Leser bestand. Ein solcher Zweck konnte nicht als Beitrag zu einer Debatte von allgemeinem Interesse für die Gesellschaft anzusehen sein. Da es sich hier um einen Fall des „ungeheuerlichen Missbrauchs der Pressefreiheit“ handelte, bedeuteten die strengen Einschränkungen in Bezug auf die Entschädigung des

Schadens und der durch das innerstaatliche Recht vorgesehene geringe Betrag des immateriellen Schadensersatzes, dass es Litauen nicht gelungen war, seiner positiven Verpflichtung zum Schutz des Rechts der Beschwerdeführerin auf Achtung ihres Privatlebens nachzukommen. Der EGMR befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Das Recht auf freie Meinungsäußerung und das Recht auf Schutz personenbezogener Daten kollidieren nicht immer. Es gibt Fälle, in denen der wirksame Schutz personenbezogener Daten die Freiheit der Meinungsäußerung garantiert.

Beispiel: In der Rechtssache *Tele2 Sverige* befand der EuGH, dass der mit der Richtlinie 2006/24 (Richtlinie über die Vorratsspeicherung von Daten) verbundene Eingriff in die in Artikel 7 und Artikel 8 der Charta verankerten Grundrechte „von großem Ausmaß und als besonders schwerwiegend anzusehen ist. Außerdem ist der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist“. Der EuGH befand auch, dass die allgemeine Vorratsspeicherung der Verkehrs- und Standortdaten Auswirkungen auf die Nutzung der elektronischen Kommunikationsmittel und „infolgedessen auf die Ausübung der in Artikel 11 der Charta gewährleisteten Freiheit der Meinungsäußerung durch die Nutzer dieser Mittel“ haben könne.⁹⁹ In diesem Sinne tragen die Datenschutzvorschriften durch das Erfordernis strenger Garantien für eine nicht allgemein erfolgende Vorratsdatenspeicherung schließlich zur Ausübung der freien Meinungsäußerung bei.

Was das Recht auf den Empfang von Informationen betrifft, das ebenfalls Teil der freien Meinungsäußerung ist, so wächst das Bewusstsein für die Bedeutung einer transparent handelnden Regierung für das Funktionieren einer demokratischen Gesellschaft. Transparenz ist eine dem Gemeinwohl dienende Zielsetzung, die – sofern erforderlich und verhältnismäßig – folglich einen

⁹⁹ EuGH, Verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB / Post- och telestyrelsen und Secretary of State for the Home Department / Tom Watson und andere* [GK], 21. Dezember 2016, Randnrn. 37 und 101; EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014, Randnr. 28.

Eingriff in das Recht auf Datenschutz rechtfertigen könnte, wie in [Abschnitt 1.2](#) erläutert. In den beiden letzten Jahrzehnten wurde das Recht auf Zugang zu sich im Besitz von Behörden befindenden Dokumenten als ein wichtiges Recht eines jeden Unionsbürgers und jeder natürlichen oder juristischen Person mit Wohnsitz oder satzungsgemäßem Sitz in einem Mitgliedstaat anerkannt.

Im Recht des Europarates wäre hier auf die Grundsätze zu verweisen, die in der Empfehlung zum Zugang zu amtlichen Dokumenten verankert sind, von der sich wiederum die Verfasser des Übereinkommens über den Zugang zu amtlichen Dokumenten (Übereinkommen Nr. 205) inspirieren ließen.¹⁰⁰

Im EU-Recht wird das Recht auf Zugang zu Dokumenten durch die Verordnung (EG) Nr. 1049/2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (Verordnung über den Zugang zu Dokumenten) gewährleistet.¹⁰¹ Artikel 42 der Charta und Artikel 15 Absatz 3 AEUV haben dieses Recht noch erweitert; es umfasst jetzt den Zugang „zu den Dokumenten der Organe, Einrichtungen und sonstigen Stellen der Union, unabhängig von der Form der für diese Dokumente verwendeten Träger“.

Dieses Recht könnte mit dem Recht auf Datenschutz kollidieren, wenn beim Zugang zu Dokumenten personenbezogene Daten anderer Personen offengelegt werden. Artikel 86 der Datenschutz-Grundverordnung sieht eindeutig vor, dass personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz von Behörden oder öffentlichen Einrichtungen befinden, von der betreffenden Behörde oder Einrichtung gemäß dem Unionsrecht¹⁰² oder dem Recht des Mitgliedstaats offengelegt werden können, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten gemäß der Verordnung in Einklang zu bringen.

Bei Anträgen auf Zugang zu Dokumenten oder Informationen im Besitz von Behörden kann es daher erforderlich sein, das Recht auf Datenschutz von Personen, deren Daten sich in den angeforderten Dokumenten befinden, angemessen zu berücksichtigen.

¹⁰⁰ Europarat, Ministerkomitee (2002), Empfehlung Rec(81) 19 und Empfehlung Rec(2002)2 an die Mitgliedstaaten über die Einsicht in amtliche Dokumente, 21. Februar 2002; Europarat, Übereinkommen über den Zugang zu amtlichen Dokumenten, SEV Nr. 205, 18. Juni 2009. Das Übereinkommen ist noch nicht in Kraft getreten.

¹⁰¹ Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission, ABl. L 145 vom 31.5.2001.

¹⁰² Artikel 42 der Charta, Artikel 15 Absatz 3 AEUV und Verordnung (EG) Nr. 1049/2009.

Beispiel: In der Rechtssache *Volker und Markus Schecke und Hartmut Eifert gegen Land Hessen*,¹⁰³ hatte der EuGH über die Verhältnismäßigkeit der von EU-Rechtsvorschriften geforderten Veröffentlichung der Namen von Empfängern von EU-Agrarsubventionen und der von ihnen erhaltenen Beträge zu befinden. Mit der Veröffentlichung sollte die Transparenz erhöht und zur öffentlichen Kontrolle der angemessenen Verwendung öffentlicher Mittel durch die Verwaltung beigetragen werden. Mehrere Empfänger forchten die Verhältnismäßigkeit dieser Veröffentlichung an.

Der EuGH stellte fest, dass das Recht auf Datenschutz kein absolutes Recht ist, dass aber die Veröffentlichung von Daten mit den Namen der Empfänger von Mitteln aus den beiden EU-Fonds und den genauen Beträgen auf einer Internetseite einen Eingriff in ihr Privatleben im Allgemeinen und in den Schutz ihrer personenbezogenen Daten im Besonderen darstellt.

Nach Auffassung des EuGH sind solche Verletzungen der durch Artikel 7 und 8 der Charta anerkannten Rechte gesetzlich vorgesehen und entsprechen einer von der Union anerkannten dem Gemeinwohl dienenden Zielsetzung, nämlich die Transparenz in Bezug auf die Verwendung der Gemeinschaftsmittel zu erhöhen. Der EuGH stellte allerdings fest, dass die Veröffentlichung der Namen natürlicher Personen, die Empfänger von Agrarbeihilfen der EU aus diesen beiden Fonds sind, sowie der genauen erhaltenen Beträge eine unverhältnismäßige Maßnahme darstellte und mit Blick auf Artikel 52 Absatz 1 der Charta nicht gerechtfertigt war. Er erkannte an, dass es in einer demokratischen Gesellschaft wichtig ist, dass die Steuerzahler über die Verwendung der öffentlichen Gelder informiert werden. Da aber „dem Ziel der Transparenz nicht ohne Weiteres Vorrang gegenüber dem Recht auf Schutz der personenbezogenen Daten zuerkannt werden kann“,¹⁰⁴ seien die EU-Organe dazu verpflichtet, das Interesse der Union an Transparenz mit der seitens der Empfänger infolge der Veröffentlichung erlittenen Einschränkung der Ausübung der Rechte auf Privatsphäre und Schutz personenbezogener Daten zum Ausgleich zu bringen.

103 EuGH, Verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen* [GK], 9. November 2010, Randnrn. 47–52, 58, 66–67, 75, 86 und 92.

104 a.a.O., Randnr. 85.

Der EuGH war der Ansicht, dass die EU-Organe keine ausgewogene Gewichtung vorgenommen hätten, da Maßnahmen vorstellbar seien, die die Grundrechte der natürlichen Personen weniger stark beeinträchtigen, den mit der Veröffentlichung verfolgten Transparenzziele aber ebenso in wirksamer Weise dienen. Statt einer allgemeinen Veröffentlichung aller Begünstigten unter Angabe ihres Namens und der von jedem von ihnen erhaltenen genauen Beträge könnte eine Unterscheidung nach einschlägigen Kriterien wie den Zeiträumen, während deren sie solche Beihilfen erhalten haben, der Häufigkeit oder auch Art und Umfang dieser Beihilfen gemacht werden.¹⁰⁵ Der EuGH erklärte somit EU-Rechtsvorschriften über die Veröffentlichung von Informationen über die Empfänger von Mitteln aus europäischen Landwirtschaftsfonds teilweise für ungültig.

Beispiel: In der Rechtssache *Rechnungshof gegen Österreichischer Rundfunk und andere*,¹⁰⁶ überprüfte der EuGH die Übereinstimmung bestimmter österreichischer Rechtsvorschriften mit dem Datenschutzrecht der EU. Die Rechtsvorschriften verpflichteten ein staatliches Organ zur Erhebung und Weiterleitung von Einkommensdaten zum Zweck der Veröffentlichung der Namen und Einkommen der Dienstnehmer verschiedener öffentlicher Stellen in einem der Allgemeinheit zugänglich gemachten Jahresbericht. Einige Personen lehnten die Mitteilung ihrer Daten aus Datenschutzgründen ab.

In seiner Stellungnahme stützte sich der EuGH auf den Schutz der Grundrechte als allgemeinen Grundsatz des EU-Rechts und auf Artikel 8 EMRK, wobei er daran erinnerte, dass die Charta zu diesem Zeitpunkt nicht verbindlich war. Er befand, dass die Erhebung von Daten über die beruflichen Einkünfte Einzelner und insbesondere deren Offenlegung unter den Anwendungsbereich des Rechts auf Achtung des Privatlebens falle und eine Verletzung dieses Rechts darstelle. Der Eingriff könnte gerechtfertigt sein, wenn er gesetzlich vorgesehen gewesen wäre, ein berechtigtes Ziel verfolgt hätte und in einer demokratischen Gesellschaft für die Erreichung dieses Zieles notwendig gewesen wäre. Der EuGH stellte fest, dass die österreichischen Rechtsvorschriften ein berechtigtes Ziel verfolgten, da sie darauf abzielten, die Bezüge in angemessenen Grenzen zu halten - eine Überlegung, die auch

¹⁰⁵ a.a.O., Randnr. 89.

¹⁰⁶ EuGH, Verbundene Rechtssachen C-465/00, C-138/01 und C-139/09, *Rechnungshof / Österreichischer Rundfunk und andere* und *Christa Neukomm und Joseph Lauermann / Österreichischer Rundfunk*, 20. Mai 2003.

mit dem wirtschaftlichen Wohl des Landes verbunden ist. Das Interesse Österreichs an der Gewährleistung der bestmöglichen Verwendung öffentlicher Mittel sei jedoch gegen die Schwere der Beeinträchtigung des Rechts der Betroffenen auf Achtung ihres Privatlebens abzuwägen.

Der EuGH überließ es dem vorlegenden Gericht, zu prüfen, ob die Veröffentlichung von Daten über die Einkünfte Einzelner notwendig ist und in einem angemessenen Verhältnis zu dem mit den Rechtsvorschriften verfolgten Ziel steht, forderte das vorlegende Gericht jedoch dazu auf, zu untersuchen, ob dieses Ziel durch weniger einschneidende Mittel nicht ebenso wirksam erreicht werden könnte. Ein Beispiel wäre die ausschließliche Übermittlung der personenbezogenen Daten an die Kontrollorgane und nicht an die Allgemeinheit.

In späteren Rechtssachen wurde es offensichtlich, dass die Abwägung zwischen dem Datenschutz und dem Zugang zu Dokumenten einer genauen Einzelfallanalyse bedarf. Keines der beiden Rechte kann automatisch das andere aufheben. Der EuGH hatte die Gelegenheit, das Recht auf Zugang zu Dokumenten mit personenbezogenen Daten in zwei Fällen auszulegen.

Beispiel: In der Rechtssache *Europäische Kommission gegen Bavarian Lager*¹⁰⁷ legte der EuGH den Umfang des Schutzes personenbezogener Daten im Zusammenhang mit dem Zugang zu Dokumenten von EU-Organen fest und befasste sich mit der Beziehung zwischen der Verordnung (EG) Nr. 1049/2001 (Verordnung über den Zugang zu Dokumenten) und der Verordnung (EG) Nr. 45/2001 (Datenschutzverordnung der EU-Organe). Bavarian Lager, gegründet 1992, führt deutsches Flaschenbier in das Vereinigte Königreich ein, hauptsächlich für den Ausschank in Gaststätten. Das Unternehmen stieß jedoch auf Schwierigkeiten, weil das britische Recht *de facto* britische Hersteller bevorzugte. Als Reaktion auf die Beschwerde von Bavarian Lager leitete die Europäische Kommission gegen das Vereinigte Königreich ein Vertragsverletzungsverfahren ein; daraufhin änderte das Vereinigte Königreich die angefochtenen Bestimmungen und gleichte sie an das EU-Recht an. Bavarian Lager forderte daraufhin bei der Kommission unter anderem eine Kopie des Protokolls einer Sitzung an, an der Vertreter der Kommission, der britischen Behörden und der *Confédération des Brasseurs*

¹⁰⁷ EuGH, C-28/08 P, *Europäische Kommission / The Bavarian Lager Co. Ltd.* [GK], 29. Juni 2010.

du Marché Commun (CBMC) teilgenommen hatten. Die Kommission stimmte der Verbreitung bestimmter Dokumente im Zusammenhang mit dieser Sitzung zu, schwärzte jedoch im Protokoll fünf Namen, da zwei Personen der Offenlegung ihrer Identität ausdrücklich widersprochen hatten und die Kommission die drei anderen nicht kontaktieren konnte. Mit Entscheidung vom 18. März 2004 lehnte die Kommission den Antrag von Bavarian Lager auf Gewährung des Zugangs zum vollständigen Protokoll insbesondere unter Hinweis auf den Schutz des Privatlebens dieser Personen ab, wie er in der Datenschutzverordnung gewährleistet wird.

Da Bavarian Lager mit dieser Entscheidung nicht einverstanden war, klagte es vor dem Gericht erster Instanz. Dieses Gericht hob die Entscheidung der Kommission mit Urteil vom 8. November 2007 auf (Rechtssache T-194/04, *The Bavarian Lager Co. Ltd gegen Kommission der Europäischen Gemeinschaften*) und führte aus, dass die alleinige Eintragung der Namen der fraglichen Personen in die Liste der Personen, die im Namen ihrer Einrichtungen an der Sitzung teilnahmen, keine Gefährdung des Privatlebens bedeutete und das Privatleben dieser Personen nicht gefährdete.

Auf die Berufung der Kommission hin hob der EuGH das Urteil des Gerichts erster Instanz auf. Nach Auffassung des EuGH enthält die Verordnung über den Zugang zu Dokumenten „eine spezifische, verstärkte Schutzregelung für Personen, deren personenbezogene Daten gegebenenfalls veröffentlicht werden könnten“. Weiter führt der EuGH aus, dass die Bestimmungen der Datenschutzverordnung der EU-Organe in vollem Umfang anwendbar werden, wenn mit einem nach der Verordnung über den Zugang zu Dokumenten gestellten Antrag die Gewährung des Zugangs zu Dokumenten beantragt wird, die personenbezogene Daten enthalten. Nach Auffassung des EuGH hat daher die Kommission den Antrag auf Zugang zum vollständigen Protokoll der Sitzung vom Oktober 1996 zu Recht abgelehnt. Da von fünf Teilnehmern an dieser Sitzung keine Einwilligung vorlag, kam die Kommission durch die Weitergabe einer Fassung des streitigen Dokuments mit fünf geschwärzten Namen hinreichend der ihr obliegenden Pflicht zur Transparenz nach.

Da nach Auffassung des EuGH „Bavarian Lager keine ausdrückliche rechtliche Begründung gegeben und kein überzeugendes Argument über die Notwendigkeit der Übermittlung dieser personenbezogenen Daten vorgetragen hat, war es der Kommission nicht möglich, die verschiedenen Interessen der Beteiligten gegeneinander abzuwägen. Sie konnte auch

nicht prüfen, ob Grund zur Annahme, dass die berechtigten Interessen der Betroffenen beeinträchtigt sein könnten, bestand oder nicht“, wie es die Datenschutzverordnung der EU-Organe verlangt.

Beispiel: In der Rechtssache *Client Earth und PAN Europe gegen EFSA*¹⁰⁸ untersuchte der EuGH, ob die Entscheidung der Europäischen Behörde für Lebensmittelsicherheit (EFSA), den Beschwerdeführern vollständigen Zugang zu Dokumenten zu verweigern, für den Schutz der Privatsphäre und der Datenschutzrechte der Personen erforderlich war, auf die sich die Dokumente bezogen. Die Dokumente betrafen den seitens einer Arbeitsgruppe der EFSA zusammen mit externen Sachverständigen ausgearbeiteten Entwurf eines Leitfadens zum Inverkehrbringen eines Pflanzenschutzmittels. Anfangs gewährte die EFSA den Beschwerdeführern Zugang zu einem Teil der betreffenden Dokumente und verweigerte den Zugang auf einige Versionen des Leitfadenentwurfs. Danach gewährte sie Zugang zur Entwurfsversion, die die individuellen Stellungnahmen der externen Sachverständigen enthielt. Sie machte jedoch die Namen dieser Sachverständigen gemäß Artikel 4 Absatz 1 Buchstabe b der Verordnung Nr. 45/2001 über die Verarbeitung personenbezogener Daten durch die EU-Organe unkenntlich. In erster Instanz bestätigte das Gericht der EU die Entscheidung der EFSA.

Auf die Berufung der Beschwerdeführer revidierte der EuGH das erstinstanzliche Urteil. Er befand, dass die Übermittlung personenbezogener Daten in diesem Fall erforderlich war, um prüfen zu können, ob die einzelnen Sachverständigen bei der Erfüllung ihrer wissenschaftlichen Aufgabe unparteiisch waren und um die Transparenz des Entscheidungsprozesses der EFSA zu gewährleisten. Dem EuGH zufolge gab die EFSA nicht an, inwiefern die Offenbarung der Namen der externen Sachverständigen, die die spezifischen Stellungnahmen im Leitfadenentwurf abgaben, die berechtigten Interessen der Sachverständigen beeinträchtigen würden. Das allgemeine Argument, wonach die Verbreitung die Privatsphäre beeinträchtigen könnte, reicht nicht aus, wenn es nicht für jeden Einzelfall mit Beweisen untermauert ist.

¹⁰⁸ EuGH, C-615/13P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) / Europäische Behörde für Lebensmittelsicherheit (EFSA), Europäische Kommission*, 16. Juli 2015.

Diesen Urteilen zufolge bedarf es für einen Eingriff in das Recht auf Datenschutz im Zusammenhang mit dem Zugang zu Dokumenten einer konkreten und fundierten Begründung. Das Recht auf Zugang zu Dokumenten kann nicht automatisch das Recht auf Datenschutz aufheben.¹⁰⁹

Wie das nachstehende Urteil zeigt, ist dieser Ansatz mit dem seitens des EGMR in Bezug auf Privatsphäre und Zugang zu Dokumenten vertretenen Ansatz vergleichbar. Im Urteil *Magyar Helsinki* stellte der EGMR fest, dass Artikel 10 einem Individuum kein Recht auf Zugang zu Informationen verleiht, die sich im Besitz einer Behörde befinden, oder die Regierung zu deren Offenlegung verpflichtet. Ein solches Recht bzw. eine solche Verpflichtung kann jedoch dann im Raum stehen, wenn erstens eine Offenlegung der Information von einem Gericht rechtskräftig angeordnet wurde, oder zweitens, unter Umständen, wo der Zugang zur Information für die seitens des Einzelnen erfolgende Ausübung des Rechts auf freie Meinungsäußerung - vor allem „die Freiheit auf den Erhalt und die Offenlegung von Informationen“ - maßgeblich war und wo deren Verweigerung einen Eingriff in dieses Recht darstellt.¹¹⁰ Ob und inwieweit die Verweigerung des Zugangs zu Informationen einen Eingriff in das Recht des Beschwerdeführers auf freie Meinungsäußerung darstellt, ist in jedem Einzelfall und im Hinblick auf dessen besondere Umstände zu beurteilen, darunter: (i) der Zweck des Informationsansuchens, (ii) der Charakter der begehrten Informationen, (iii) die Rolle des Beschwerdeführers und (iv) ob die Informationen bereit und verfügbar waren.

Beispiel: In der Rechtssache *Magyar Helsinki Bizottság gegen Ungarn*¹¹¹ forderte die Beschwerdeführerin, eine Menschenrechtsorganisation, bei der Polizei Informationen in Bezug auf die Arbeit amtswegiger Verteidiger an, um eine Studie über die Funktionsweise des Pflichtverteidigersystems in Ungarn fertigzustellen. Die Polizei verweigerte die Bereitstellung der Informationen mit dem Argument, dass diese personenbezogene Daten darstellen, die nicht der Offenlegung unterstehen. Unter Anwendung der obigen Kriterien befand der EGMR, dass ein Eingriff in ein unter Artikel 10 geschütztes Recht vorgelegen habe. Genauer gesagt wollte die Beschwerdeführerin das Recht

¹⁰⁹ Siehe jedoch detaillierte Ausführungen in EDSB (2011), *Öffentlicher Zugang zu Dokumenten mit personenbezogenen Daten nach dem Urteil in der Rechtssache „Bavarian Lager“*, Brüssel, 24. März 2011.

¹¹⁰ EGMR, *Magyar Helsinki Bizottság / Ungarn* [GK], Nr. 18030/11, 8. November 2016, Randnr. 156.

¹¹¹ a.a.O., Randnrn. 181, 187–200.

auf Offenlegung von Informationen über eine Angelegenheit von öffentlichem Interesse ausüben, beantragte diesbezüglich Zugang zu Informationen, und die Informationen waren für die Ausübung des Rechts der Beschwerdeführerin auf freie Meinungsäußerung erforderlich. Die Informationen über die Bestellung von Pflichtverteidigern waren für die Öffentlichkeit von Interesse. Es gab keinen Grund, daran zu zweifeln, dass die betreffende Studie Informationen enthielt, zu deren Offenlegung sich die Beschwerdeführerin verpflichtete und auf deren Erhalt die Öffentlichkeit ein Recht hatte. Der Gerichtshof war folglich davon überzeugt, dass der Zugang zu den angeforderten Informationen für die Beschwerdeführerin zur Erledigung der Aufgabe erforderlich war. Schließlich waren die Informationen bereit und verfügbar.

Der EGMR befand, dass die Verweigerung des Zugangs zu den Informationen in diesem Fall den Kern der Freiheit zum Erhalt von Informationen beeinträchtigt hatte. Um zu dieser Schlussfolgerung zu gelangen, untersuchte der Gerichtshof insbesondere den Zweck der angeforderten Informationen und deren Beitrag zu einer wichtigen öffentlichen Debatte, den Charakter der begehrten Informationen und ob diese von öffentlichem Interesse waren, sowie die gesellschaftliche Funktion der Beschwerdeführerin in dieser Rechtssache.

Der Gerichtshof stellte in seiner Argumentation fest, dass die seitens der NGO durchgeführte Studie die Arbeitsweise der Justiz und das Recht auf ein faires Verfahren betraf, welches innerhalb der EMRK von umfassender Bedeutung war. Da die angeforderten Informationen keine Daten außerhalb des öffentlichen Umfelds umfassten, wären die Rechte der betroffenen Personen durch den der Beschwerdeführerin seitens der Polizei erteilten Zugang auf die Informationen nicht gefährdet gewesen. Die seitens der Beschwerdeführerin angeforderten Informationen waren statistischer Natur und bezogen sich auf die Zahl der Bestellungen von Pflichtverteidigern zur Vertretung von Angeklagten im staatlich finanzierten Verfahrenshilfesystem.

In Anbetracht dessen, dass die Studie darauf abzielte, zu einer wichtigen Debatte über eine Angelegenheit von öffentlichem Interesse beizutragen, hätten Beschränkungen hinsichtlich der von der NGO vorgeschlagenen Publikation nach Ansicht des Gerichtshofs größtmögliche Vorsicht erfordert. Die betreffenden Informationen waren von öffentlichem Interesse, da das öffentliche Interesse „Angelegenheiten umfasst, die zu beträchtlichen Meinungsverschiedenheiten Anlass geben können, ein wichtiges gesellschaftliches Thema betreffen oder ein Problem beinhalten, in Bezug

auf das ein öffentliches Interesse besteht, darüber informiert zu werden“.¹¹² Folglich würden sie mit Sicherheit eine Diskussion über die Führung der Justiz und faire Verhandlungen umfassen, worin das Thema der Studie der Beschwerdeführerin bestand. Nach Abwägung der verschiedenen betroffenen Rechte und Anwendung des Grundsatzes der Verhältnismäßigkeit befand der EGMR, dass eine ungerechtfertigte Verletzung der der Beschwerdeführerin gemäß Artikel 10 EMRK zustehenden Rechte stattgefunden habe.

1.3.2. Berufsgeheimnis

Nach Maßgabe des nationalen Rechts können bestimmte Mitteilungen dem Berufsgeheimnis unterliegen. Das Berufsgeheimnis kann als besondere ethische Pflicht verstanden werden, aus der sich eine rechtliche Verpflichtung ergibt, die bestimmten auf Glauben und Vertrauen gründenden Berufen und Tätigkeiten innewohnt. Personen und Organe, die diese Tätigkeiten ausüben, sind dazu verpflichtet, von der Offenlegung der von ihnen im Laufe der Ausführung ihrer Pflichten erhaltenen vertraulichen Informationen abzusehen. Das Berufsgeheimnis findet insbesondere auf den Arztberuf und die Vertraulichkeit der anwaltlichen Korrespondenz Anwendung, wobei zahlreiche Rechtsprechungen auch der Finanzbranche ein Berufsgeheimnis einräumen. Das Berufsgeheimnis zählt zwar nicht zu den Grundrechten, ist jedoch als eine Form des Rechts auf die Achtung des Privatlebens geschützt. So hat der EuGH beispielsweise entschieden, dass es in bestimmten Fällen „zur Wahrung des Grundrechts eines Unternehmens auf Achtung des Privatlebens gemäß Artikel 8 EMRK und Artikel 7 der Grundrechtecharta in der Tat erforderlich sein kann, die Veröffentlichung bestimmter, als vertraulich eingestufter Informationen zu untersagen“.¹¹³ Wie in den hervorgerufenen Beispielen dargelegt, wurde auch der EGMR angerufen, um darüber zu entscheiden, ob Einschränkungen des Berufsgeheimnisses eine Verletzung von Artikel 8 EMRK darstellen.

¹¹² a.a.O., Randnr. 156.

¹¹³ EuGH, Rechtssache T-462/12 R, *Pilkington Group Ltd / Europäische Kommission*, Beschluss des Präsidenten des Gerichts, 11. März 2013, Randnr. 44.

Beispiel: In der Rechtssache *Pruteanu gegen Rumänien*¹¹⁴ war der Beschwerdeführer als Rechtsanwalt einer Handelsgesellschaft tätig, die im Anschluss an Betrugsvorwürfe von der Durchführung von Bankgeschäften ausgeschlossen worden war. Während der Untersuchung der Rechtssache erlaubten die rumänischen Gerichte den für die Strafverfolgung zuständigen Behörde über einen bestimmten Zeitraum das Abhören und Aufzeichnen von Telefongesprächen eines Teilhabers der Handelsgesellschaft. Die Aufzeichnungen und das Abhören umfassten dessen Gespräche mit seinem Rechtsanwalt.

Herr Pruteanu machte geltend, dass dies einen Eingriff in sein Recht auf Achtung seines Privatlebens und seiner Korrespondenz darstelle. Der EGMR hob in seinem Urteil den Status und die Bedeutung der Beziehung eines Rechtsanwalts zu seinem Mandanten hervor. Das Abhören der Gespräche eines Rechtsanwalts mit seinem Mandanten verletze zweifelsohne das Berufsgeheimnis, das das Fundament der Beziehung zwischen diesen beiden Personen darstelle. In einem solchen Fall könne sich der Rechtsanwalt auch über einen Eingriff in sein Recht auf Achtung seines Privatlebens und seiner Korrespondenz beschweren. Der EGMR befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Beispiel: In der Rechtssache *Brito Ferrinho Bexiga Villa-Nova gegen Portugal*¹¹⁵ verweigerte die Beschwerdeführerin, eine Rechtsanwältin, die Offenlegung ihrer persönlichen Kontoauszüge gegenüber den Steuerbehörden aufgrund des Berufsgeheimnisses und des Bankgeheimnisses. Die Staatsanwaltschaft leitete Ermittlungen im Hinblick auf einen Steuerbetrug ein und beantragte die Genehmigung für die Aussetzung des Berufsgeheimnisses. Die nationalen Gerichte ordneten die Aussetzung der Vorschriften in Bezug auf das Berufs- und das Bankgeheimnis mit der Begründung an, dass das öffentliche Interesse über die privaten Interessen der Beschwerdeführerin vorherrschen solle.

Nach Verweis der Rechtssache an den EGMR, befand der Gerichtshof, dass der Zugang zu den Kontoauszügen der Beschwerdeführerin einen Eingriff in ihr Recht auf Achtung des Berufsgeheimnisses darstelle, das unter den Schutz ihres Privatlebens fällt. Da der Eingriff auf die Strafprozessordnung gründete, hatte er eine Rechtsgrundlage und verfolgte ein berechtigtes Ziel. Bei der Untersuchung der Erforderlichkeit und Verhältnismäßigkeit des Eingriffs wies der EGMR auf die Tatsache hin, dass die Verfahren zur Aufhebung

114 EGMR, *Pruteanu / Rumänien*, Nr. 30181/05, 3. Februar 2015.

115 EGMR, *Brito Ferrinho Bexiga Villa-Nova / Portugal*, Nr. 69436/10, 1. Dezember 2015.

der Vertraulichkeit ohne Beteiligung oder Wissen der Beschwerdeführerin durchgeführt wurden. Folglich konnte die Beschwerdeführerin ihre Argumente nicht vorbringen. Obgleich das innerstaatliche Recht vorsah, dass bei solchen Verfahren die Stellungnahme der Rechtsanwaltsvereinigung einzuholen war, wurde die Vereinigung nicht hinzugezogen. Schließlich hatte die Beschwerdeführerin weder die Möglichkeit, die Aufhebung des Berufsgeheimnisses anzufechten, noch irgendein Rechtsmittel zur Anfechtung der Maßnahme einzulegen. Aufgrund der fehlenden Verfahrensgarantien und der fehlenden gerichtlichen Kontrolle über die Maßnahme zur Aussetzung der Vertraulichkeitspflicht befand der EGMR, dass eine Verletzung von Artikel 8 EMRK vorlag.

Die Interaktion zwischen Berufsgeheimnis und Datenschutz ist häufig ambivalent. Einerseits helfen die Datenschutzvorschriften und die Garantien bei der Gewährleistung des Berufsgeheimnisses. So zielen Vorschriften, die Verantwortliche und Auftragsverarbeiter zur Anwendung robuster Datenschutzmaßnahmen verpflichten, beispielsweise unter anderem darauf ab, den Verlust der Vertraulichkeit von durch das Berufsgeheimnis geschützten personenbezogenen Daten zu verhindern. Darüber hinaus ermöglicht die Datenschutz-Grundverordnung der EU die Verarbeitung von Gesundheitsdaten, die besondere Kategorien personenbezogener Daten darstellen, die besonderem Schutz bedürfen, unterstellt diese Verarbeitung jedoch dem Vorhandensein angemessener und spezifischer Maßnahmen zur Wahrung der Rechte der betroffenen Person, insbesondere des Berufsgeheimnisses.¹¹⁶

Andererseits kann das den Verantwortlichen und Auftragsverarbeitern in Bezug auf bestimmte personenbezogene Daten auferlegte Berufsgeheimnis die Rechte der betroffenen Personen einschränken, und hierbei insbesondere das Recht auf den Erhalt von Informationen. Obgleich die Datenschutz-Grundverordnung ein umfassendes Verzeichnis der Informationen enthält, die der betroffenen Person grundsätzlich mitzuteilen sind, wenn die personenbezogenen Daten nicht bei ihr erhoben wurden, findet diese Offenlegungsverpflichtung keine Anwendung, wenn die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen.¹¹⁷

¹¹⁶ Datenschutz-Grundverordnung, Artikel 9 Absatz 2 Buchstabe h und Artikel 9 Absatz 3.

¹¹⁷ a.a.O., Artikel 14 Absatz 5 Buchstabe d.

Die Datenschutz-Grundverordnung (DSGVO) sieht für die Mitgliedstaaten die Möglichkeit vor, den Schutz des Berufsgeheimnisses oder anderer gleichwertiger Geheimhaltungspflichten durch Rechtsvorschriften zu regeln und das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang zu bringen.¹¹⁸

Die DSGVO sieht vor, dass die Mitgliedstaaten die Befugnisse der Aufsichtsbehörden gegenüber den Verantwortlichen oder den Auftragsverarbeitern, die dem Berufsgeheimnis unterliegen, regeln können. Diese spezifischen Vorschriften beziehen sich auf die Befugnis zum Erhalt von Zugang zu den Geschäftsräumen des Verantwortlichen oder des Auftragsverarbeiters, zu dessen Datenverarbeitungsanlagen und den sich in seinem Besitz befindenden personenbezogenen Daten, sofern diese personenbezogenen Daten bei einer Tätigkeit erlangt wurden, die einer solchen Geheimhaltungspflicht unterliegt. Folglich müssen die mit dem Datenschutz betrauten Aufsichtsbehörden das Berufsgeheimnis einhalten, das die Verantwortlichen oder Auftragsverarbeiter bindet. Darüber hinaus sind auch die Mitglieder der Aufsichtsbehörden selbst sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung zur Wahrung von Verschwiegenheit verpflichtet. Die Mitglieder und Bediensteten der Aufsichtsbehörden können während der Ausübung ihrer Aufgaben in Kenntnis von vertraulichen Informationen gelangen. Artikel 54 Absatz 2 der Verordnung sieht eindeutig vor, dass sie in Bezug auf diese vertraulichen Informationen einer Verschwiegenheitspflicht unterliegen.

Die DSGVO erfordert, dass die Mitgliedstaaten die Kommission darüber unterrichten, welche Vorschriften sie annehmen, um den Datenschutz und die in der Verordnung festgesetzten Grundsätze mit dem Berufsgeheimnis in Einklang zu bringen.

1.3.3. Religions- und Weltanschauungsfreiheit

Die Religions- und Weltanschauungsfreiheit ist unter Artikel 9 EMRK (Gedanken-, Gewissens- und Religionsfreiheit) und Artikel 10 der Charta der Grundrechte der EU geschützt. Personenbezogene Daten, aus denen religiöse oder philosophische Überzeugungen hervorgehen, werden sowohl im EU-Recht als auch im Recht des Europarates als „sensible Daten“ betrachtet, deren Verarbeitung und Nutzung einem verstärkten Schutz unterliegen.

¹¹⁸ a.a.O., Erwägungsgrund 164 und Artikel 90.

Beispiel: Der Beschwerdeführer in der Rechtssache *Sinak Isik gegen die Türkei*¹¹⁹ war ein Mitglied der Religionsgemeinschaft der Aleviten, deren Glaube durch den Sufismus und andere vorislamische Überzeugungen beeinflusst ist und von einigen Gelehrten als gesonderte Religion, von anderen jedoch als Teil des Islam betrachtet wird. Der Beschwerdeführer beschwerte sich darüber, dass sein Personalausweis ein Kästchen aufwies, in dem seine Religion entgegen seinem Wunsch als „Islam“ statt als „Alevit“ angegeben wurde. Die innerstaatlichen Gerichte wiesen seinen Antrag auf Änderung seines Personalausweises in „Alevit“ zurück, da dieses Wort eine Untergruppierung des Islam und keine unabhängige Religion bezeichne. Im Anschluss daran beschwerte er sich beim EGMR darüber, dass er ohne seine Einwilligung zur Offenlegung seines Glaubens gezwungen worden sei, da die Angabe der Religion einer Person im Personalausweis vorgeschrieben war, was gegen sein Recht auf Religions- und Gewissensfreiheit verstoße, insbesondere in Anbetracht der Tatsache, dass die Bezeichnung „Islam“ auf seinem Personalausweis falsch sei.

Der EGMR wiederholte, dass die Religionsfreiheit die Freiheit zu der gemeinsam mit anderen, in der Öffentlichkeit und innerhalb des demselben Glauben angehörenden Personenkreises, aber auch allein und privat erfolgenden Bekundung der Religion einer Person mit sich bringt. Die innerstaatliche Gesetzgebung verpflichtete die Einzelnen zum damaligen Zeitpunkt zum Mitführen eines Personalausweises, der auf Anforderung aller staatlichen Behörden oder privaten Unternehmen vorgezeigt werden musste und aus dem die Religion hervorging. Eine solche Verpflichtung erkannte jedoch nicht an, dass das Recht auf Bekundung seiner Religion auch das gegenteilige Recht einräumte, das darin bestand, zur Offenlegung seines Glaubens nicht verpflichtet zu sein. Obgleich die Regierung argumentierte, dass die nationale Gesetzgebung geändert wurde und die Einzelnen nun beantragen könnten, dass das Kästchen mit der Angabe ihrer Religion in ihrem Personalausweis frei gelassen wird, kann nach Ansicht des Gerichtshofs bereits die bloße Tatsache, dass die Streichung der Religion beantragt werden muss, zu einer Verbreitung von Informationen führen, die Aspekte der Haltung einer Person zu ihrem Glauben betreffen. Mit der Möglichkeit, in Ausweisen die Rubrik „Religion“ freilassen zu können, ist unweigerlich eine bestimmte Konnotation verbunden. Die Inhaber von Identitätspapieren ohne Angabe der Religion unterscheiden sich nämlich von Personen, die

119 EGMR, *Sinan Isik / Türkei*, Nr. 21924/05, 2. Februar 2010.

einen Ausweis besitzen, in dem ihr Religionsbekenntnis eingetragen ist. Der EGMR befand, dass die innerstaatliche Gesetzgebung eine Verletzung von Artikel 9 EMRK darstellte.

Der Betrieb von Kirchen und religiösen Vereinigungen oder Gemeinschaften kann jedoch die Verarbeitung der personenbezogenen Daten ihrer Mitglieder erfordern, um die Kommunikation und die Organisation von Aktivitäten innerhalb der Kirchengemeinde zu ermöglichen. Folglich haben Kirchen und religiöse Vereinigungen oftmals Regeln in Bezug auf die Verarbeitung personenbezogener Daten eingeführt. Wenn diese Regeln umfassend sind, dürfen sie gemäß Artikel 91 der Datenschutz-Grundverordnung weiter angewandt werden, sofern sie mit den Vorschriften der Verordnung in Einklang gebracht werden. Kirchen und religiöse Vereinigungen, die solche Regeln anwenden, unterliegen der Aufsicht durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in der Datenschutz-Grundverordnung für diese Behörden niedergelegten Bedingungen erfüllt.¹²⁰

Religiöse Vereinigungen können die Verarbeitung personenbezogener Daten aus mehreren Gründen durchführen, wie beispielsweise um mit ihrer Kirchengemeinde in Kontakt zu bleiben oder Informationen über anstehende Events, religiöse Veranstaltungen oder Feste usw. mitzuteilen. In bestimmten Ländern müssen die Kirchen aus Steuergründen Verzeichnisse ihrer Mitglieder führen, da sich die Mitgliedschaft in religiösen Einrichtungen auf die seitens der Einzelnen zu entrichtenden Steuern auswirken kann. Nach europäischem Recht sind Daten, die religiöse Überzeugungen offenbaren, sensible Daten, und Kirchen sind für den Umgang mit solchen Daten und für deren Verarbeitung verantwortlich, insbesondere da die seitens religiöser Vereinigungen verarbeiteten Informationen häufig Kinder, ältere Menschen oder andere schutzbedürftige Mitglieder der Gesellschaft betreffen.

1.3.4. Freiheit der Kunst und der Wissenschaft

Ein weiteres Recht, das gegen das Recht auf Achtung des Privatlebens und auf Datenschutz abzuwägen ist, ist die Freiheit der Kunst und der Wissenschaft, die mit Artikel 13 der Charta der Grundrechte der EU ausdrücklich geschützt wird. Dieses Recht leitet sich in erster Linie aus der Gedankenfreiheit und der

¹²⁰ Datenschutz-Grundverordnung, Artikel 91 Absatz 2.

Freiheit der Meinungsäußerung ab und ist unter Wahrung von Artikel 1 der Charta (Würde des Menschen) auszuüben. Nach Auffassung des EGMR wird die Freiheit der Kunst durch Artikel 10 EMRK geschützt.¹²¹ Das in Artikel 13 der Charta garantierte Recht kann den durch Artikel 52 Absatz 1 der Charta gestatteten Einschränkungen unterworfen werden, die auch im Licht von Artikel 10 Absatz 2 EMRK ausgelegt werden können.¹²²

Beispiel: In der Rechtssache *Vereinigung bildender Künstler gegen Österreich*¹²³ untersagten die österreichischen Gerichte der beschwerdeführenden Vereinigung die Fortsetzung der Ausstellung eines Gemäldes, das Fotografien der Köpfe verschiedener Persönlichkeiten des öffentlichen Lebens in sexuellen Positionen enthielt. Ein österreichischer Parlamentarier, dessen Foto für das Gemälde verwendet worden war, ging gerichtlich gegen die beschwerdeführende Vereinigung vor und beantragte den Erlass einer einstweiligen Verfügung, mit der die Ausstellung des Gemäldes untersagt werden sollte. Das innerstaatliche Gericht erließ eine solche Verfügung. Der EGMR bekräftigte, dass sich Artikel 10 EMRK auf die Verbreitung von Ideen erstreckt, die den Staat oder einen Teil der Bevölkerung beleidigen, schockieren oder verstören. Personen, die Kunstwerke schaffen, aufführen, vertreiben oder ausstellen, tragen zum Austausch von Ideen und Meinungen bei, und der Staat hat die Pflicht, nicht ungebührlich in ihre Freiheit der Meinungsäußerung einzugreifen. Da es sich bei dem Gemälde um eine Collage handle und nur Fotos von den Köpfen von Personen verwendet worden seien, und da ihre Körper unrealistisch und übertrieben gemalt worden seien und offensichtlich nicht die Realität wiedergeben oder auch nur andeuten wollten, stellte der EGMR weiter fest, dass „das Gemälde kaum als Beschreibung von Einzelheiten des Privatlebens [des Abgebildeten] verstanden werden kann, sondern eher im Zusammenhang mit seiner Stellung in der Öffentlichkeit als Politiker zu sehen ist“, und dass „sich [der Abgebildete] in dieser Eigenschaft Kritik gegenüber toleranter zeigen muss“. Nach Abwägung der Interessen der Beteiligten kam der EGMR zu dem Schluss, ein uneingeschränktes Verbot einer weiteren Ausstellung des Gemäldes sei unverhältnismäßig. Der Gerichtshof befand, dass eine Verletzung von Artikel 10 EMRK vorlag.

121 EGMR, *Müller und andere / Schweiz*, Nr. 10737/84, 24. Mai 1988.

122 Erläuterungen zur Charta der Grundrechte, ABl. C 303 vom 14.12.2007.

123 EGMR, *Vereinigung bildender Künstler / Österreich*, Nr. 68345/01, 25. Januar 2007, Randnrn. 26 und 34.

Das europäische Datenschutzrecht erkennt auch den besonderen Wert der Wissenschaft für die Gesellschaft an. Sowohl die Datenschutz-Grundverordnung als auch das Modernisierte Übereinkommen Nr. 108 gestatten die Speicherung von Daten über längere Zeiträume, sofern die personenbezogenen Daten ausschließlich für wissenschaftliche oder historische Forschungszwecke verarbeitet werden. Auch und ungeachtet des ursprünglichen Zwecks einer bestimmten Verarbeitungstätigkeit gilt die spätere Weiterverwendung personenbezogener Daten für die wissenschaftliche Forschung nicht als unvereinbarer Zweck.¹²⁴ Gleichzeitig müssen geeignete Garantien für eine solche Verarbeitung eingerichtet werden, um die persönlichen Rechte und Freiheiten der betroffenen Personen zu schützen. Das EU-Recht oder das Recht der Mitgliedstaaten kann Ausnahmen von den Rechten der betroffenen Personen vorsehen, wie beispielsweise vom Recht auf Auskunft über ihre Daten, auf Berichtigung, auf Einschränkung der Verarbeitung sowie auf Widerspruch zur Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken (siehe auch [Abschnitt 6.1](#) und [Abschnitt 9.4](#)).

1.3.5. Schutz des geistigen Eigentums

Das Recht auf Schutz des Eigentums ist in Artikel 1 des Ersten Zusatzprotokolls zur EMRK sowie in Artikel 17 Absatz 1 der Charta verankert. Ein wichtiger Aspekt des Eigentumsrechts, der von besonderer Bedeutung für den Datenschutz ist, ist der Schutz des geistigen Eigentums, der in Artikel 17 Absatz 2 der Charta ausdrücklich erwähnt wird. Mehrere Richtlinien im EU-Recht befassen sich mit dem wirksamen Schutz des geistigen Eigentums und hierbei insbesondere des Urheberrechts. Geistiges Eigentum umfasst nicht nur das Eigentum an literarischen und künstlerischen Werken, sondern auch das Recht an Patenten, Marken und die damit verwandten Rechte.

Wie der EuGH in seiner Rechtsprechung klargemacht hat, muss der Schutz des Grundrechts auf Eigentum gegen den Schutz anderer Grundrechte, insbesondere des Rechts auf Datenschutz, abgewogen werden.¹²⁵ Es ist vorgekommen, dass für den Schutz des Urheberrechts zuständige Einrichtungen von Internetdiensteanbietern die Offenlegung der Identität von Nutzern von

¹²⁴ Datenschutz-Grundverordnung, Artikel 5 Absatz 1 Buchstabe b und Modernisiertes Übereinkommen 108, Artikel 5 Absatz 4 Buchstabe b.

¹²⁵ EuGH, C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU* [GK], 29. Januar 2008, Randnrn. 62–68.

Musiktauschbörsen im Internet gefordert haben. Häufig können Internetnutzer an solchen Börsen kostenlos Musiktitel herunterladen, selbst wenn diese Titel urheberrechtlich geschützt sind.

Beispiel: In der Rechtssache *Promusicae gegen Telefónica de España*¹²⁶ ging es um die Weigerung eines spanischen Internetanbieters, Telefónica, Promusicae, einer gemeinnützigen Organisation von Musikproduzenten und Herausgebern von Musikaufnahmen und audiovisuellen Aufnahmen, die personenbezogenen Daten bestimmter Personen offenzulegen, denen er Internetzugangsdienste anbot. Promusicae forderte die Offenlegung dieser Informationen, um zivilrechtlich gegen diese Personen vorgehen zu können, die nach seiner Aussage ein Filesharing-Programm für den Zugriff auf Tonträger nutzten, deren Verwertungsrechte bei Mitgliedern von Promusicae lagen.

Das spanische Gericht legte die Sache dem EuGH mit der Frage vor, ob nach dem Gemeinschaftsrecht solche personenbezogenen Daten im Rahmen zivilrechtlicher Verfahren zur Gewährleistung eines wirksamen Schutzes des Urheberrechts weitergegeben werden müssen. Es verwies auf die Richtlinien 2000/31, 2001/29 und 2004/48, auch vor dem Hintergrund von Artikel 17 und 47 der Charta. Der EuGH stellte fest, dass diese drei Richtlinien sowie die ePrivacy-Richtlinie (Richtlinie 2002/58) nicht die Möglichkeit der Mitgliedstaaten ausschließen, zum wirksamen Schutz des Urheberrechts eine Pflicht zur Offenlegung personenbezogener Daten im Rahmen eines Zivilverfahrens vorzusehen.

Nach Auffassung des EuGH warf die Sache somit die Frage auf, wie die Erfordernisse des Schutzes verschiedener Grundrechte, nämlich zum einen des Rechts auf Achtung des Privatlebens und zum anderen des Eigentumsrechts und des Rechts auf einen wirksamen Rechtsbehelf, miteinander in Einklang gebracht werden können.

Für den Gerichtshof ist es „Sache der Mitgliedstaaten, bei der Umsetzung der genannten Richtlinien darauf zu achten, dass sie sich auf eine Auslegung derselben stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Gemeinschaftsrechtsordnung

¹²⁶ a.a.O., Randnrn. 54 und 60.

geschützten Grundrechten sicherzustellen. Bei der Durchführung der Maßnahmen zur Umsetzung dieser Richtlinien haben die Behörden und Gerichte der Mitgliedstaaten nicht nur ihr nationales Recht im Einklang mit diesen Richtlinien auszulegen, sondern auch darauf zu achten, dass sie sich nicht auf eine Auslegung dieser Richtlinien stützen, die mit diesen Grundrechten oder den anderen allgemeinen Grundsätzen des Gemeinschaftsrechts, wie etwa dem Grundsatz der Verhältnismäßigkeit, kollidiert.“¹²⁷

Beispiel: In der Rechtssache *Bonnier Audio AB und andere gegen Perfect Communication Sweden AB*¹²⁸ ging es um das Gleichgewicht zwischen dem Recht des geistigen Eigentums und dem Schutz personenbezogener Daten. Die Beschwerdeführer – fünf Verlage, die die Urheberrechte an 27 Hörbüchern besitzen – leiteten vor dem schwedischen Gericht ein Verfahren mit der Behauptung ein, dass diese Urheberrechte mittels eines FTP-Servers (ein Datenübertragungsprotokoll, das File-Sharing und die Übertragung von Dateien über das Internet ermöglicht) verletzt worden seien. Die Beschwerdeführer forderten den Internetdienstleister zur Offenlegung des Namens und der Adresse derjenigen Person auf, die die IP-Adresse nutzte, von der aus die Daten übertragen wurden. Der Internetdienstleister, ePhone, trat diesem Antrag entgegen und machte geltend, dass dieser die Richtlinie 2006/24 (die 2014 außer Kraft gesetzte Richtlinie über die Vorratsspeicherung von Daten) verletze.

Das schwedische Gericht verwies die Rechtssache an den EuGH mit der Frage, ob die Richtlinie 2006/24 der Anwendung einer nationalen Vorschrift entgegensteht, die auf der Grundlage von Artikel 8 der Richtlinie 2004/48 (Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums) erlassen wurde, die den Erlass einer Verfügung erlaubt, durch die Internetdienstleister zu der an die Inhaber von Urheberrechten erfolgenden Übermittlung von Informationen über Teilnehmer aufgefordert werden können, von deren IP-Adressen aus dieses Recht angeblich verletzt worden sein soll. Dabei ist davon auszugehen, dass der Antragsteller deutliche Anhaltspunkte für eine Urheberrechtsverletzung geliefert hat und dass die Maßnahme verhältnismäßig ist.

127 a.a.O., Randnrn. 65 und 68; siehe auch EuGH, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) / Netlog NV*, 16. Februar 2012.

128 EuGH, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB / Perfect Communication Sweden AB*, 19. April 2012.

Der EuGH hob hervor, dass die Richtlinie 2006/24 ausschließlich die Verarbeitung und Vorratsspeicherung von Daten betreffe, die von Anbietern elektronischer Kommunikationsdienste zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten erzeugt werden, sowie ihre Offenlegung den zuständigen nationalen Behörden. Eine nationale Vorschrift zur Umsetzung der Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums liegt folglich außerhalb des Anwendungsbereichs der Richtlinie 2006/24 und steht dieser Richtlinie daher nicht entgegen.¹²⁹

In Bezug auf die seitens der Beschwerdeführer begehrte Auskunft über den betreffenden Namen und die betreffende Adresse, befand der EuGH, dass diese eine Verarbeitung personenbezogener Daten darstelle und in den Anwendungsbereich der Richtlinie 2002/58 (ePrivacy-Richtlinie) falle. Er stellte zudem fest, dass die Offenlegung der betreffenden Daten in einem Zivilverfahren zugunsten eines Urheberrechtsinhabers zum Zweck der Sicherstellung eines effektiven Urheberrechtsschutzes verlangt wurde und daher auch aufgrund ihres Gegenstands in den Anwendungsbereich der Richtlinie 2004/48 fällt.¹³⁰

Der EuGH befand, dass die Richtlinien 2002/58 und 2004/48 dahin auszulegen sind, dass sie nationalen Rechtsvorschriften wie den im Ausgangsverfahren in Rede stehenden nicht entgegenstehen, soweit es diese Rechtsvorschriften dem nationalen Gericht, bei dem beantragt wurde, die Offenlegung personenbezogener Daten anzuordnen, ermöglichen, anhand der Umstände des Einzelfalls und unter gebührender Berücksichtigung der sich aus dem Grundsatz der Verhältnismäßigkeit ergebenden Erfordernisse eine Abwägung der einander gegenüberstehenden Interessen vorzunehmen.

129 a.a.O., Randnr. 40 und 41.

130 a.a.O., Randnrn. 52–54. Siehe auch EuGH, C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU* [GK], 29. Januar 2008, Randnr. 58.

1.3.6. Datenschutz und wirtschaftliche Interessen

Im digitalen Zeitalter oder im Zeitalter der Big Data wurden Daten als „das neue Öl“ der Wirtschaft zur Ankurbelung von Innovation und Kreativität bezeichnet.¹³¹ Viele Unternehmen haben robuste Geschäftsmodelle rund um die Datenverarbeitung errichtet, und diese Verarbeitung betrifft häufig auch personenbezogene Daten. Bestimmte Unternehmen mögen glauben, dass besondere Vorschriften in Bezug auf den Schutz personenbezogener Daten in der Praxis zu übermäßig aufwändigen Verpflichtungen führen können, die ihre wirtschaftlichen Interessen beeinträchtigen könnten. Folglich ergibt sich die Frage, ob die wirtschaftlichen Interessen der Verantwortlichen und Auftragsverarbeiter oder der Allgemeinheit die Einschränkung des Rechts auf Datenschutz rechtfertigen könnten.

Beispiel: In der Rechtssache *Google Spain*¹³² befand der EuGH, dass Einzelne unter bestimmten Voraussetzungen dazu berechtigt sind, Suchmaschinen zur Entfernung von Suchergebnissen aus ihrem Suchindex aufzufordern. Der EuGH hob in seiner Argumentation hervor, dass die Nutzung von Suchmaschinen und die aufgelisteten Suchergebnisse ein detailliertes Profil einer Person erstellen können. Diese Informationen können zahlreiche Aspekte des Privatlebens einer Person betreffen und hätten ohne eine Suchmaschine nicht leicht gefunden oder miteinander verknüpft werden können. Folglich stelle dies einen potentiell schweren Eingriff in die Grundrechte der betroffenen Person auf Achtung des Privatlebens und Schutz personenbezogener Daten dar.

Im Anschluss daran untersuchte der EuGH, ob dieser Eingriff gerechtfertigt sein könnte. In Bezug auf das wirtschaftliche Interesse des Suchmaschinenbetreibers an der Durchführung der Verarbeitung erklärte der EuGH, dass „ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten gerechtfertigt werden kann“, und dass die Grundrechte aus den Artikeln 7 und 8 der Charta nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit daran, die Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche zu finden, überwiegen.¹³³

¹³¹ Siehe beispielsweise *Financial Times* (2016), „Data is the new oil... who's going to own it?“, 16. November 2016.

¹³² EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014.

¹³³ a.a.O., Randnrn. 81 und 97.

Eine der Hauptüberlegungen des europäischen Datenschutzrechts besteht darin, den Einzelnen mehr Kontrolle über ihre personenbezogenen Daten zu geben. Besonders im digitalen Zeitalter besteht ein Ungleichgewicht zwischen der Macht von Unternehmen, die große Mengen personenbezogener Daten verarbeiten und dazu Zugang haben, und der Macht der Einzelnen, denen diese personenbezogenen Daten gehören, ihre Informationen zu kontrollieren. Bei der Abwägung zwischen Datenschutz und wirtschaftlichen Interessen stellt der EuGH auf jeden Einzelfall ab, wie beispielsweise bei der Abwägung der Interessen Dritter gegenüber Aktiengesellschaften und Gesellschaften mit beschränkter Haftung, wie das nachstehende Urteil in der Rechtssache *Manni* veranschaulicht.

Beispiel: In der Rechtssache *Manni*¹³⁴ ging es um die Eintragung der personenbezogenen Daten einer Person in einem öffentlichen Handelsregister. Herr Manni hatte die Handelskammer von Lecce zur Entfernung seiner personenbezogenen Daten aus diesem Register aufgefordert, da er herausgefunden hatte, dass potenzielle Kunden auf das Register zurückgreifen und sehen würden, dass er der alleinige Geschäftsführer eines Unternehmens war, das über ein Jahrzehnt zuvor für insolvent erklärt worden war. Diese Information würde seine potenziellen Kunden beeinflussen und könne sich negativ auf seine Handelsinteressen auswirken.

Der EuGH wurde angerufen, um festzustellen, ob das EU-Recht in diesem Fall ein Recht auf das Löschen dieser Daten anerkenne. Im Zuge seiner Schlussfolgerung wägte der Gerichtshof die Datenschutzvorschriften der EU und das wirtschaftliche Interesse von Herrn Manni an der Entfernung der Informationen über die Insolvenz seines früheren Unternehmens gegen das öffentliche Interesse am Zugang zu diesen Informationen ab. Er nahm die Tatsache zur Kenntnis, dass die Offenlegung im öffentlichen Gesellschaftsregister gesetzlich und insbesondere von einer EU-Richtlinie vorgesehen war, die den Zugang Dritter zu Unternehmensinformationen erleichtern soll. Die Offenlegung war wichtig für den Schutz der Interessen Dritter, die möglicherweise mit einem bestimmten Unternehmen Geschäfte abwickeln möchten, da Aktiengesellschaften und Gesellschaften mit beschränkter Haftung zum Schutze Dritter lediglich das Gesellschaftsvermögen zur Verfügung stellen. „Die Offenlegung soll es Dritten

¹³⁴ EuGH, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni*, 9. März 2017.

[daher] erlauben, sich über die wesentlichen Urkunden der Gesellschaft sowie einige sie betreffende Angaben, insbesondere die Personalien derjenigen, die die Gesellschaft verpflichten können, zu unterrichten.“¹³⁵

In Anbetracht der Bedeutung des seitens des Registers verfolgten berechtigten Ziels, befand der EuGH, dass Herr Manni nicht zur Erwirkung der Löschung seiner personenbezogenen Daten berechtigt war, da die Notwendigkeit, die Interessen Dritter gegenüber Aktiengesellschaften und Gesellschaften mit beschränkter Haftung zu schützen und die Rechtssicherheit, die Lauterkeit von Handelsgeschäften und damit das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, Vorrang vor seinen Rechten im Rahmen der Datenschutzvorschriften haben. Dies gelte vor allem in Anbetracht der Tatsache, dass natürliche Personen, die sich dafür entscheiden, über eine Aktiengesellschaft oder eine Gesellschaft mit beschränkter Haftung am Wirtschaftsleben teilzunehmen, sich darüber bewusst sind, dass sie dazu verpflichtet sind, Informationen über ihre Personalien und Aufgaben offenzulegen.

Obgleich der EuGH befand, dass in diesem Fall keine Gründe für das Erwirken einer Löschung vorlagen, erkannte er das Vorliegen eines Widerspruchsrecht zu der Verarbeitung an und merkte diesbezüglich an, „dass [...] nicht auszuschließen ist, dass es besondere Situationen gibt, in denen es aus überwiegenden, schutzwürdigen, sich aus dem konkreten Fall der betroffenen Person ergebenden Gründen ausnahmsweise gerechtfertigt ist, den Zugang zu den im Register eingetragenen personenbezogenen Daten, die sie betreffen, nach Ablauf einer hinreichend langen Frist [...] auf Dritte zu beschränken, die ein besonderes Interesse an der Einsichtnahme in diese Daten nachweisen.“¹³⁶

Der EuGH erklärte, dass es Sache der vorlegenden Gerichte sei, unter Berücksichtigung aller maßgeblichen Umstände des Einzelnen in jedem Einzelfall zu beurteilen, ob überwiegende, schutzwürdige Gründe vorliegen oder nicht, die es gegebenenfalls ausnahmsweise rechtfertigen könnten, den Zugang Dritter zu personenbezogenen Daten in Gesellschaftsregistern zu beschränken. Er verdeutlichte jedoch, dass im Fall von Herrn Manni die bloße Tatsache, dass die Offenlegung seiner personenbezogenen Daten im Register seine Kundschaft angeblich beeinflusste, nicht als solch überwiegender und

135 a.a.O., Randnr. 49.

136 a.a.O., Randnr. 60.

schutzwürdiger Grund betrachtet werden könne. Die potenziellen Kunden von Herrn Manni haben ein berechtigtes Interesse an Informationen in Bezug auf die Insolvenz seines früheren Unternehmens.

Der Eingriff in die durch Artikel 7 und 8 der Charta gewährleisteten Grundrechte von Herrn Manni und anderen im Register enthaltenen Personen auf die Achtung des Privatlebens und den Schutz personenbezogener Daten diene einer Zielsetzung von allgemeinem Interesse und war notwendig und verhältnismäßig.

In der Rechtssache *Manni* entschied der EuGH daher, dass die Rechte auf Datenschutz und Privatsphäre nicht über dem Interesse Dritter auf Zugang zu den im Gesellschaftsregister enthaltenen Informationen in Bezug auf Aktiengesellschaften und Gesellschaften mit beschränkter Haftung stehen.

2

Datenschutzterminologie



EU	Behandelte Themen	Europarat
Personenbezogene Daten		
DSGVO, Artikel 4 Absatz 1 DSGVO, Artikel 4 Absatz 5 und Artikel 5 Absatz 1 Buchstabe e DSGVO, Artikel 9 EuGH, Verbundene Rechtssachen C-92/09 und C-93/09, <i>Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen</i> [GK], 2010 EuGH, C-275/06, <i>Productores de Música de España (Promusicae) / Telefónica de España SAU</i> [GK], 2008 EuGH, C-70/10, <i>Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)</i>, 2011 EuGH, C-582/14, <i>Patrick Breyer / Bundesrepublik Deutschland</i>, 2016 EuGH, Verbundene Rechtssachen C-141/12 und C-372/12, <i>YS gegen Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel / M und S</i>, 2014 EuGH, C-101/01, <i>Strafverfahren / Bodil Lindqvist</i>, 2003	Begriffsbestimmung des Datenschutzes	Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe a EGMR, <i>Bernh Larsen Holding AS und andere / Norwegen</i>, Nr. 24117/08, 2013 EGMR, <i>Uzun / Deutschland</i>, Nr. 35623/05, 2010 EGMR, <i>Amann / Schweiz</i> [GK], Nr. 27798/95, 2000
	Besondere Kategorien personenbezogener Daten (sensible Daten)	Modernisiertes Übereinkommen Nr. 108, Artikel 6 Absatz 1

EU	Behandelte Themen	Europarat
EuGH, C-434/16, <i>Peter Nowak / Data Protection Commissioner</i> , 2017	Anonymisierte und pseudonymisierte Daten	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe e Erläuternder Bericht zum Modernisierten Übereinkommen Nr. 108, Absatz 50
Datenverarbeitung		
DSGVO, Artikel 4 Absatz 2 EuGH, C-212/13, <i>František Ryneš / Úřad pro ochranu osobních údajů</i> , 2014 EuGH, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni</i> , 2017 EuGH, C-101/01, <i>Strafverfahren / Bodil Lindqvist</i> , 2003 EuGH, C-131/12, <i>Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GK]</i> , 2014	Begriffsbestimmungen	Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstaben b und c
Verwender von Daten		
DSGVO, Artikel 4 Absatz 7 EuGH, C-212/13, <i>František Ryneš / Úřad pro ochranu osobních údajů</i> , 2014 EuGH, C-131/12, <i>Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GK]</i> , 2014	Verantwortlicher	Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe d Profiling-Empfehlung, Artikel 1 Buchstabe g*
DSGVO, Artikel 4 Absatz 8	Auftragsverarbeiter	Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe f Profiling-Empfehlung, Artikel 1 Buchstabe h
DSGVO, Artikel 4 Absatz 9	Empfänger	Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe e
DSGVO, Artikel 4 Absatz 10	Dritter	

EU	Behandelte Themen	Europarat
Einwilligung		
DSGVO, Artikel 4 Absatz 11 und Artikel 7 EuGH, C-543/09, <i>Deutsche Telekom AG / Bundesrepublik Deutschland</i> , 2011 EuGH, C-536/15, <i>Tele2 (Netherlands) BV und andere / Autoriteit Consument en Markt (AMC)</i> , 2017	Begriffsbestimmung und Anforderungen an eine gültige Einwilligung	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 2 Empfehlung zum Schutz medizinischer Daten, Artikel 6, und mehrere spätere Empfehlungen EGMR, <i>Elberte / Lettland</i> , Nr. 61243/08, 2015

Anmerkung: *Europarat, Ministerkomitee (2010), Empfehlung CM/Rec(2010)13 des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling (Profiling-Empfehlung), 23. November 2010.

2.1. Personenbezogene Daten

Kernpunkte

- Daten sind personenbezogene Daten, wenn sie zu einer identifizierten oder identifizierbaren Person, der „betroffenen Person“, gehören.
- Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten ein Verantwortlicher oder eine andere Person alle Mittel berücksichtigen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.
- Authentifizierung bedeutet den Nachweis, dass eine bestimmte Person eine bestimmte Identität hat und/oder zur Ausführung bestimmter Tätigkeiten befugt ist.
- Es gibt besondere Datenkategorien, so genannte sensible Daten, die im Modernisierten Übereinkommen Nr. 108 und im europäischen Datenschutzrecht angeführt sind, und die besonders schutzbedürftig sind und daher besonderen rechtlichen Vorschriften unterliegen.
- Daten sind anonymisiert, wenn sie nicht länger identifizierten oder identifizierbaren Personen zugeordnet sind.
- Pseudonymisierung ist eine Maßnahme, durch die personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen, die gesondert aufbewahrt

werden, nicht mehr einer betroffenen Person zugeordnet werden können. Der „Schlüssel“, der die erneute Identifizierung der betroffenen Personen ermöglicht, ist gesondert und sicher aufzubewahren. Daten, die einem Pseudonymisierungsverfahren unterzogen wurden, bleiben personenbezogene Daten. Im EU-Recht gibt es den Begriff „pseudonymisierte Daten“ nicht.

- Die Grundsätze und Vorschriften des Datenschutzes finden auf anonymisierte Informationen keine Anwendung. Gleichwohl finden sie auf pseudonymisierte Daten Anwendung.

2.1.1. Hauptaspekte des Konzepts der personenbezogenen Daten

Sowohl **im EU-Recht** als auch **im Recht des Europarates**, werden „personenbezogene Daten“ als Informationen definiert, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.¹³⁷ Sie betreffen Informationen über eine Person, deren Identität eindeutig ist oder durch Einholen weiterer Informationen festgestellt werden kann. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten ein Verantwortlicher oder eine andere Person alle Mittel berücksichtigen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.¹³⁸

Werden Daten über eine solche Person verarbeitet, wird diese als „betroffene Person“ bezeichnet.

Die betroffene Person

Im EU-Recht sind natürliche Personen die einzigen Begünstigten der Datenschutzvorschriften¹³⁹ und nur lebende Personen sind durch das europäische Datenschutzrecht geschützt.¹⁴⁰ Die DSGVO definiert personenbezogene Daten als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

¹³⁷ Datenschutz-Grundverordnung, Artikel 4 Absatz 1, Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe a.

¹³⁸ Datenschutz-Grundverordnung, Erwägungsgrund 26.

¹³⁹ a.a.O., Artikel 1.

¹⁴⁰ a.a.O., Erwägungsgrund 27. Siehe auch Artikel-29-Datenschutzgruppe (2007), *Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“*, WP 136, 20. Juni 2007, S. 22.

Das Recht des Europarates und insbesondere das Modernisierte Übereinkommen Nr. 108 verweisen ebenfalls auf den Schutz des Menschen bei der Verarbeitung personenbezogener Daten. Auch dort sind personenbezogene Daten als alle Informationen definiert, die sich auf eine identifizierte oder identifizierbare Person beziehen. Diese natürliche Person oder Person im Sinne der DSGVO bzw. des Modernisierten Übereinkommens Nr. 108 wird im Datenschutzrecht als „betroffene Person“ bezeichnet.

Auch juristische Personen genießen einen gewissen Schutz. Es gibt Rechtsprechung des EGMR zu Beschwerden juristischer Personen wegen behaupteter Verletzung ihres Rechts nach Artikel 8 EMRK auf Schutz vor einer Verwendung ihrer Daten. Artikel 8 EMRK deckt sowohl das Recht auf Achtung des Privat- und Familienlebens als auch das Recht auf Achtung der Wohnung und der Korrespondenz ab. Der Gerichtshof kann Rechtssachen daher aus dem Blickwinkel des Rechts auf Achtung der Wohnung und der Korrespondenz und weniger aus der Perspektive des Privat- und Familienlebens prüfen.

Beispiel: In der Rechtssache *Bernh Larsen Holding AS und andere gegen Norwegen*¹⁴¹ ging es um eine Beschwerde dreier norwegischer Unternehmen gegen eine Entscheidung einer Finanzbehörde mit der Anordnung, den Steuerprüfern eine Kopie aller Daten auf einem Computerserver zur Verfügung zu stellen, den sie gemeinsam nutzten.

Der EGMR stellte fest, dass eine solche Verpflichtung für die beschwerdeführenden Unternehmen einen Eingriff in ihre Rechte auf Achtung der „Wohnung“ und der „Korrespondenz“ im Sinne von Artikel 8 EMRK bedeutete. Der Gerichtshof befand aber auch, dass die Steuerbehörden wirksame und angemessene Garantien gegen Missbrauch boten. Die beschwerdeführenden Unternehmen waren rechtzeitig über die Steuerprüfung informiert worden; sie waren anwesend und konnten sich während der Prüfung vor Ort äußern, und das Material sollte nach Abschluss der Steuerprüfung vernichtet werden. Angesichts dessen war ein angemessenes Gleichgewicht zwischen dem Recht der beschwerdeführenden Unternehmen auf Achtung ihrer „Wohnung“ und ihrer „Korrespondenz“ sowie ihrem Interesse am Schutz der Privatsphäre

¹⁴¹ EGMR, *Bernh Larsen Holding AS und andere / Norwegen*, Nr. 24117/08, 14. März 2013. Siehe jedoch auch EGMR, *Liberty und andere / Vereinigtes Königreich*, Nr. 58243/00, 1. Juli 2008.

ihrer Mitarbeiter auf der einen Seite und dem öffentlichen Interesse an einer wirksamen Kontrolle für steuerliche Zwecke auf der anderen Seite gegeben. Der Gerichtshof befand, dass daher keine Verletzung von Artikel 8 vorlag.

Gemäß dem Modernisierten Übereinkommen Nr. 108 geht es beim Datenschutz vorrangig um den Schutz natürlicher Personen, doch können die Vertragsparteien in ihrem innerstaatlichen Recht den Datenschutz auch auf juristische Personen wie Unternehmen und Verbände ausdehnen. Im erläuternden Bericht zum Modernisierten Übereinkommen heißt es, dass das nationale Recht die berechtigten Interessen juristischer Personen durch die Ausdehnung des Anwendungsbereichs des Übereinkommens auf diese Akteure schützen kann.¹⁴² Das **EU-Datenschutzrecht** gilt nicht für die Verarbeitung von Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.¹⁴³ Die ePrivacy-Richtlinie schützt jedoch die Vertraulichkeit der Kommunikation und die berechtigten Interessen juristischer Personen im Hinblick auf die zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung personenbezogener Daten über Teilnehmer und Nutzer.¹⁴⁴ Gleichmaßen dehnt der Entwurf der ePrivacy-Verordnung den Schutz auf juristische Personen aus.

Beispiel: In der Rechtssache *Volker und Markus Schecke und Hartmut Eifert gegen Land Hessen*¹⁴⁵ stellte der EuGH bezüglich der Veröffentlichung personenbezogener Daten von Empfängern von Agrarbeihilfen fest, dass „sich juristische Personen gegenüber einer solchen Bestimmung auf den durch Artikel 7 und 8 der Charta verliehenen Schutz nur berufen können, soweit der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt. [...]e in den Artikeln 7 und 8 der Charta anerkannte Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten erstreckt sich auf jede Information, die eine bestimmte oder bestimmbare Person betrifft [...]“.¹⁴⁶

142 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 30.

143 Datenschutz-Grundverordnung, Erwägungsgrund 14.

144 ePrivacy-Richtlinie, Erwägungsgrund 7 und Artikel 1 Absatz 2.

145 EuGH, Verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen* [GK], 9. November 2010, Randnr. 53.

146 a.a.O., Randnrn. 52 und 53.

Bei der Abwägung zwischen dem Interesse der EU an der Gewährleistung von Transparenz bei der Zuweisung von Beihilfen einerseits und den Grundrechten der Empfänger der Beihilfen auf Privatsphäre und Datenschutz andererseits, befand der EuGH, dass der Eingriff in diese Grundrechte unverhältnismäßig war. Er war der Ansicht, dass das Ziel der Transparenz ebenso wirksam durch Maßnahmen hätte erreicht werden können, die einen weniger einschneidenden Eingriff in die Rechte der betroffenen Personen dargestellt hätten. Bei der Untersuchung der Verhältnismäßigkeit der Veröffentlichung von Informationen über juristische Personen, die Beihilfen erhielten, gelangte der EuGH jedoch zu einer anderen Schlussfolgerung und entschied, dass eine solche Veröffentlichung nicht über die Grenzen des Grundsatzes der Verhältnismäßigkeit hinausging. Er stellte fest: „Die Verletzung des Rechts auf Schutz der personenbezogenen Daten hat nämlich bei juristischen Personen ein anderes Gewicht als bei natürlichen Personen“.¹⁴⁷ Juristische Personen unterlägen einer erweiterten Verpflichtung zur Veröffentlichung von sie betreffenden Informationen. Der EuGH vertrat die Ansicht, dass die Verpflichtung der nationalen Behörden zu der vor der Veröffentlichung der Daten erfolgenden Überprüfung, ob die Daten jeder juristischen Person, die Beihilfen empfängt, damit verbundene natürliche Personen bestimmen, diesen Behörden eine unverhältnismäßige Verwaltungslast aufbürden würde. Daher habe die Gesetzgebung, die eine allgemeine Veröffentlichung von Daten über juristische Personen verlangt, einen gerechten Ausgleich zwischen den konkurrierenden Interessen geschaffen.

Art der Daten

Alle Informationen können als personenbezogene Daten gelten, vorausgesetzt sie beziehen sich auf eine identifizierte oder identifizierbare Person.

Beispiel: Bei der Beurteilung der beruflichen Leistungen eines Arbeitnehmers durch seinen Vorgesetzten, die in der Personalakte des Beschäftigten aufbewahrt wird, handelt es sich um personenbezogene Daten über den Beschäftigten. Dies ist auch dann der Fall, wenn sie ganz oder teilweise nur die persönliche Meinung des Vorgesetzten wiedergibt, wie z. B.: „Der Arbeitnehmer zeigt bei der Arbeit keinen Einsatz“, und keine harten Fakten wie „Der Arbeitnehmer war in den letzten sechs Monaten fünf Wochen von seinem Arbeitsplatz abwesend“.

¹⁴⁷ a.a.O., Randnr. 87.

Personenbezogene Daten sind alle Informationen über das Privatleben einer Person, das auch berufliche Tätigkeiten umfasst, sowie Informationen über ihr Leben in der Öffentlichkeit.

In der Rechtssache *Amann*¹⁴⁸ legte der EGMR den Begriff „personenbezogene Daten“ als nicht auf zur Privatsphäre einer Person gehörende Angelegenheiten begrenzt aus. Diese Bedeutung des Begriffs „personenbezogene Daten“ ist auch für die DSGVO von Belang.

Beispiel: In der Rechtssache *Volker und Markus Schecke und Hartmut Eifert gegen Land Hessen*¹⁴⁹ stellte der EuGH fest: „Der Umstand, dass sich die veröffentlichten Daten auf berufliche Tätigkeiten beziehen, ist insoweit ohne Belang [...]. Der Europäische Gerichtshof für Menschenrechte hat in Bezug auf die Auslegung von Artikel 8 EMRK entschieden, dass der Begriff „Privatleben“ nicht eng ausgelegt werden darf und dass es grundsätzlich nicht in Betracht kommt, berufliche Tätigkeiten [...] vom Begriff des Privatlebens auszunehmen“.

Beispiel: In den verbundenen Rechtssachen *YS gegen Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel gegen M und S*¹⁵⁰ stellte der EuGH fest, dass die in einem Entscheidungsentwurf der Einwanderungs- und Einbürgerungsbehörde enthaltene rechtliche Analyse in Bezug auf Anträge auf eine Aufenthaltserlaubnis als solche keine personenbezogenen Daten darstellt, wenngleich sie einige personenbezogene Daten enthalten kann.

Die Rechtsprechung des EGMR zu Artikel 8 EMRK bestätigt, dass es mitunter schwierig ist, Fragen von Privatleben und Beruf vollkommen voneinander zu trennen.¹⁵¹

148 Siehe EGMR, *Amann / Schweiz*, Nr. 27798/95, 16. Februar 2000, Randnr. 65.

149 EuGH, Verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen* [GK], 9. November 2010, Randnr. 59.

150 EuGH, Verbundene Rechtssachen C-141/12 und C-372/12, *YS / Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie und Integratie en Asiel / M und S*, 17. Juli 2014, Randnr. 39.

151 Siehe z. B. EGMR, *Rotaru / Rumänien* [GK], Nr. 28341/95, 4. Mai 2000, Randnr. 43; EGMR, *Niemietz / Deutschland*, Nr. 13710/88, 16. Dezember 1992, Randnr. 29.

Beispiel: In der Rechtssache *Bărbulescu gegen Rumänien*¹⁵² wurde der Beschwerdeführer entlassen, weil er während der Arbeitszeit unter Verletzung der internen Regeln das Internet seines Arbeitgebers verwendet hatte. Sein Arbeitgeber hatte seine Kommunikation überwacht und die Aufzeichnungen, die Nachrichten rein privater Natur zeigten, wurden im Zuge des Verfahrens vor dem innerstaatlichen Gericht vorgelegt. Der EuGH befand, dass Artikel 8 Anwendung findet und ließ die Frage offen, ob die restriktiven Regelungen des Arbeitgebers beim Beschwerdeführer eine angemessene Erwartungshaltung von Privatsphäre hinterließen, war jedoch in jedem Fall der Ansicht, dass die Anweisungen eines Arbeitgebers das private soziale Leben am Arbeitsplatz nicht auf Null reduzieren könnten. In Bezug auf die Begründetheit müsse den Vertragsstaaten ein großer Ermessensspielraum eingeräumt werden für die Beurteilung der Notwendigkeit zur Festsetzung rechtlicher Rahmenbedingungen für die Voraussetzungen, unter denen ein Arbeitgeber die in elektronischer oder sonstiger Form erfolgende private Kommunikation seiner Arbeitnehmer am Arbeitsplatz regeln könne. Gleichwohl müssten die innerstaatlichen Behörden gewährleisten, dass die seitens eines Arbeitgebers erfolgende Einführung von Maßnahmen zur Überwachung der Korrespondenz und sonstigen Kommunikation unabhängig vom Umfang und von der Dauer dieser Maßnahmen von angemessenen und hinreichenden Garantien gegen Missbrauch begleitet sind. Verhältnismäßigkeit und Verfahrensgarantien gegen Willkür seien von entscheidender Bedeutung und der EGMR ermittelte eine Reihe von diesbezüglich maßgeblichen Gesichtspunkten. Zu diesen Gesichtspunkten zählten beispielsweise der Umfang der Überwachung der Arbeitnehmer seitens des Arbeitgebers und das Ausmaß des Eindringens in die Privatsphäre des Arbeitnehmers, die Folgen für den Arbeitnehmer und ob angemessene Garantien bereitgestellt wurden. Darüber hinaus müssten die innerstaatlichen Behörden sicherstellen, dass ein Arbeitnehmer, dessen Kommunikation überwacht wurde, Zugang zu einem Rechtsmittel vor einem zuständigen Gericht hat, um zumindest der Sache nach zu ermitteln, inwiefern die dargelegten Kriterien eingehalten wurden und ob die angefochtenen Maßnahmen rechtmäßig waren. In der vorliegenden Rechtssache stellte der EGMR eine Verletzung von Artikel 8 fest, da die innerstaatlichen Behörden keinen angemessenen Schutz des Rechts des Beschwerdeführers auf Achtung seines Privatlebens und seiner Korrespondenz gewährt hatten und folglich kein angemessenes Gleichgewicht zwischen den betreffenden Interessen sichergestellt haben.

¹⁵² EGMR, *Bărbulescu / Rumänien* [GK], Nr. 61496/08, 5. September 2017, Randnr. 121.

Sowohl **gemäß EU-Recht** als auch **gemäß dem Recht des Europarates** enthalten Informationen Daten über eine Person, wenn

- in diesen Informationen eine Person identifiziert wird oder identifizierbar ist, oder
- eine Person zwar nicht identifiziert, aber durch diese Informationen so ausgesondert werden kann, dass es möglich ist, durch weitere Nachforschungen herauszufinden, wer die betroffene Person ist.

Im europäischen Datenschutzrecht sind beide Arten von Informationen gleichermaßen geschützt. Die direkte oder indirekte Identifizierbarkeit von Personen erfordert eine kontinuierliche Beurteilung, „wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“.¹⁵³ Der EGMR hat wiederholt festgestellt, dass der Begriff „personenbezogene Daten“ im Sinne der EMRK dem im Übereinkommen Nr. 108 entspricht, insbesondere im Hinblick auf die Bedingung des Zusammenhangs mit einer bestimmten oder bestimmbarer Person.¹⁵⁴

Die DSGVO sieht vor, dass eine natürliche Person identifizierbar ist, wenn sie „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.¹⁵⁵ Die Identifizierung erfordert folglich Angaben, die eine Person so beschreiben, dass sie sich von allen anderen Personen unterscheidet und als Individuum erkennbar ist. Ein herausragendes Beispiel für eine solche beschreibende Angabe ist der Name einer Person, der diese direkt identifizieren kann. In einigen Fällen können andere Kennzeichen ähnliche Wirkung wie ein Name haben und eine Person indirekt identifizierbar machen. Eine Telefonnummer, Sozialversicherungsnummer und ein amtliches Kennzeichen sind allesamt Beispiele für Informationen, die eine Person identifizierbar machen können. Auch Kennzeichen wie Computerdateien, Cookies und Instrumente zur Überwachung des Internetverkehrs können verwendet werden, um Personen

¹⁵³ Datenschutz-Grundverordnung, Erwägungsgrund 26.

¹⁵⁴ Siehe EGMR, *Amann / Schweiz* [GK], Nr. 27798/95, 16. Februar 2000, Randnr. 65.

¹⁵⁵ Datenschutz-Grundverordnung, Artikel 4 Absatz 1.

anhand der Ermittlung ihres Verhaltens und ihrer Gewohnheiten auszusondern. Wie in einer Stellungnahme der Artikel-29-Datenschutzgruppe erläutert: „Die Person kann also ohne Kenntnis ihres Namens und ihrer Adresse anhand sozio-ökonomischer, psychologischer, philosophischer oder sonstiger Kriterien kategorisiert und mit bestimmten Entscheidungen in Zusammenhang gebracht werden, da der Kontaktpunkt der Person (Computer) die Offenlegung ihrer Identität im engeren Sinn nicht mehr zwingend erfordert“.¹⁵⁶ Die Definition personenbezogener Daten ist sowohl im Recht des Europarates als auch im EU-Recht hinreichend weit gefasst, um sämtliche Möglichkeiten der Identifizierung (und demnach auch sämtliche Grade der Identifizierbarkeit) zu umfassen.

Beispiel: In der Rechtssache *Promusicae gegen Telefónica de España*¹⁵⁷ befand der EuGH: „Es steht fest, dass für die von Promusicae verlangte Mitteilung der Namen und der Adressen bestimmter Nutzer von [einer bestimmten Musiktatschbörse] die Offenlegung von personenbezogenen Daten, also gemäß der Definition des Artikel 2 Buchstabe a der Richtlinie 95/46 [gegenwärtig Artikel 4 Absatz 1 DSGVO] von Informationen über eine bestimmte oder bestimmbare natürliche Person, erforderlich ist. Diese Offenlegung von Informationen, die Telefónica Promusicae zufolge speichert – was Telefónica auch nicht bestreitet –, stellt eine Verarbeitung personenbezogener Daten dar“.¹⁵⁸

Beispiel: In der Rechtssache *Scarlet Extended SA gegen Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*¹⁵⁹ ging es um die Weigerung von Scarlet, einem Anbieter von Internetzugangsdiensten, ein System der Filterung elektronischer Kommunikationen durch Programme zum Austausch von Dateien einzurichten, um den das Urheberrecht von SABAM, einer Verwertungsgesellschaft, die Autoren, Komponisten und Herausgeber von Werken der Musik vertritt, verletzenden Austausch von Dateien zu verhindern. Der EuGH befand, dass es sich bei den IP-Adressen der Nutzer „um geschützte personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen“.

156 Artikel-29-Datenschutzgruppe, *Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“*, WP 136, 20. Juni 2007, S. 15.

157 EuGH, C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU* [GK], 29. Januar 2008, Randnr. 45.

158 Frühere Richtlinie 95/46/EG, Artikel 2 Buchstabe b, nun Datenschutz-Grundverordnung, Artikel 4 Absatz 2.

159 EuGH, C-70/10, *Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. November 2011, Randnr. 51.

Da viele Namen nicht einzigartig sind, bedarf es zur Bestimmung einer Person möglicherweise weiterer Kennzeichen, um zu gewährleisten, dass eine Person nicht mit einer anderen verwechselt wird. Zur Identifizierung der Person, auf die sich die Informationen beziehen, müssen direkte und indirekte Kennzeichen zuweilen kombiniert werden. Häufig werden Geburtsdatum und Geburtsort verwendet. In einigen Ländern wurden darüber hinaus Personenkenntzahlen eingeführt, um die Bürger besser unterscheiden zu können. Bei übermittelten Steuerdaten,¹⁶⁰ in einem Verwaltungsdokument enthaltenen Daten in Bezug auf einen Antragsteller auf eine Aufenthaltserlaubnis¹⁶¹ und Dokumenten in Bezug auf Banken- und Treuhandbeziehungen¹⁶² kann es sich um personenbezogene Daten handeln. Im Zeitalter moderner Technologien gewinnen biometrische Daten wie Fingerabdrücke, digitale Fotos oder Iris-Erkennung, Standortdaten und Online-Kennzeichen für die Bestimmung von Personen zunehmend an Bedeutung.

Für die Anwendbarkeit des europäischen Datenschutzrechts ist jedoch keine aufwändige Bestimmung der betroffenen Person erforderlich; es reicht aus, dass die betroffene Person bestimmbar ist. Als bestimmbar wird eine Person angesehen, wenn genügend Elemente zur Verfügung stehen, mit denen die Person direkt oder indirekt identifiziert werden kann.¹⁶³ Gemäß Erwägungsgrund 26 der DSGVO ist entscheidend, ob wahrscheinlich ist, dass angemessene Mittel für die Bestimmung verfügbar sind und von den mutmaßlichen Verwendern der Information eingesetzt werden. Dies umfasst auch Informationen, die sich im Besitz von Drittempfängern befinden (siehe [Abschnitt 2.3.2](#)).

Beispiel: Eine lokale Behörde beschließt, Daten über Fahrzeuge zu erheben, die mit zu hoher Geschwindigkeit durch die örtlichen Straßen fahren. Sie macht Aufnahmen von den Fahrzeugen und erfasst automatisch Zeit und Ort, um die Daten dann an die zuständige Behörde weiterzugeben, damit diese Geldstrafen gegen die Geschwindigkeitssünder verhängen kann. Eine betroffene Person legt Beschwerde mit dem Argument ein, die lokale Behörde verfüge nach dem Datenschutzrecht über keine Rechtsgrundlage für diese Datenerhebung. Die lokale Behörde beharrt darauf, sie erhebe keine

160 EuGH, C-201/14, *Smaranda Bara und andere / Casa Națională de Asigurări de Sănătate und andere*, 1. Oktober 2015.

161 EuGH, YS / *Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel / M und S*, 17. Juli 2014.

162 EGMR, *M.N. und andere / San Marino*, Nr. 28005/12, 7. Juli 2015.

163 Datenschutz-Grundverordnung, Artikel 4 Absatz 1.

personenbezogenen Daten. Kennzeichenschilder sind ihrer Auffassung nach anonym. Die lokale Behörde sei rechtlich nicht befugt, zwecks Feststellung der Identität des Fahrers oder Halters des Fahrzeugs Einsicht in das allgemeine Kraftfahrzeugregister zu nehmen.

Diese Argumentation steht nicht im Einklang mit Erwägungsgrund 26 der DSGVO. Da der Zweck der Datenerhebung eindeutig darin besteht, Raser zu identifizieren und mit einer Geldstrafe zu belegen, ist absehbar, dass eine Identifizierung versucht wird. Auch wenn die lokalen Behörden selber nicht unmittelbar über Identifizierungsmittel verfügen, übermitteln sie die Daten doch an die zuständige Behörde, also die Polizei, die über solche Mittel sehr wohl verfügt. Erwägungsgrund 26 behandelt ausdrücklich auch das Szenario, bei dem es absehbar ist, dass weitere Datenempfänger, also andere als die sofortigen Verwender der Daten, versuchen könnten, die natürliche Person zu bestimmen. Unter Berücksichtigung von Erwägungsgrund 26 kommt das Vorgehen der lokalen Behörde der Erhebung von Daten über bestimmbare Personen gleich und erfordert daher eine Rechtsgrundlage im Datenschutzrecht.

„Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Umstände, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“.¹⁶⁴

Beispiel: In der Rechtssache *Breyer gegen Bundesrepublik Deutschland*¹⁶⁵ berücksichtigte der EuGH den Begriff der indirekten Identifizierbarkeit von betroffenen Personen. In dieser Rechtssache ging es um dynamische IP-Adressen, die sich bei jeder neuen Internetverbindung ändern. Die seitens Einrichtungen des Bundes betriebenen deutschen Websites zeichneten dynamische IP-Adressen auf und speicherten diese, um Cyberattacken zu verhindern und bei Bedarf eine Strafverfolgung einzuleiten. Lediglich der von Herrn Breyer verwendete Internetzugangsanbieter verfügte über die zu dessen Identifizierung benötigten Zusatzdaten.

¹⁶⁴ a.a.O., Erwägungsgrund 26.

¹⁶⁵ EuGH, C-582/14, *Patrick Breyer / Bundesrepublik Deutschland*, 19. Oktober 2016, Randnr. 43.

Der EuGH war der Ansicht, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich gemacht hat, gespeichert wird, für den Anbieter ein personenbezogenes Datum darstellt, wenn nur ein Dritter – hier der Internetzugangsanbieter dieser Person – über die zu ihrer Identifizierung erforderlichen Zusatzinformationen verfügt.¹⁶⁶ Er befand, dass es für die Einstufung eines Datums als personenbezogenes Datum „nicht erforderlich ist, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden“. Nutzer einer seitens eines Internetzugangsanbieters registrierten dynamischen IP-Adresse können in bestimmten Situationen, wie beispielsweise im Rahmen der Strafverfolgung im Zuge von Cyberattacken, mit Hilfe Dritter identifiziert werden.¹⁶⁷ Wenn der Anbieter „über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen“, stellt dies nach Auffassung des EuGH „ein Mittel dar, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann“. Daher werden solche Daten als personenbezogene Daten betrachtet.

Im Recht des Europarates wird die Identifizierbarkeit ähnlich gesehen. Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 enthält eine ähnliche Beschreibung: der Begriff „identifizierbar“ bezieht sich nicht nur auf die bürgerliche oder rechtliche Identität der Person als solche, sondern auch darauf, wodurch eine Person in Bezug auf andere „individualisiert“ oder ausgesondert werden und infolge dessen potenziell anders behandelt werden kann. Diese „Individualisierung“ könnte beispielsweise durch die namentliche Bezugnahme auf diese Person oder auf ein mit einer Identifizierungsnummer verbundenes Gerät oder eine Kombination von Geräten (Computer, Mobiltelefon, Kamera, Spielekonsole, usw.), ein Pseudonym, biometrische oder genetische Informationen, Standortdaten, eine IP-Adresse oder ein anderes Kennzeichen erfolgen.¹⁶⁸ Eine Person gilt als nicht „identifizierbar“, wenn ihre Identifizierung ein unzumutbar hohes Maß an Zeit, Anstrengungen oder

166 Frühere Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Artikel 2 Buchstabe a.

167 EuGH, C-582/14, *Patrick Breyer / Bundesrepublik Deutschland*, 19. Oktober 2016, Randnrn. 47 und 48.

168 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 18.

Hilfsmitteln erfordert. Dies trifft beispielsweise dann zu, wenn die Identifizierung einer betroffenen Person komplexe, lange und kostenintensive Tätigkeiten erfordern würde. Die Beurteilung, ob die Identifizierung ein unzumutbar hohes Maß an Zeit, Anstrengungen oder Hilfsmitteln erfordert, ist für jeden Einzelfall gesondert vorzunehmen, wobei Faktoren wie der Zweck der Verarbeitung, die Kosten und Nutzen der Identifizierung, die Art des Verantwortlichen und die eingesetzte Technologie zu berücksichtigen sind.¹⁶⁹

Was die Form betrifft, in der personenbezogene Daten gespeichert oder verwendet werden, so ist darauf hinzuweisen, dass diese für die Anwendbarkeit des Datenschutzrechts unerheblich ist. Schriftliche oder gesprochene Kommunikation kann personenbezogene Daten genauso wie Bilder¹⁷⁰ einschließlich Bilder von Videoüberwachungsanlagen (CCTV)¹⁷¹ oder Ton enthalten.¹⁷² Elektronisch gespeicherte Informationen sowie Informationen auf Papier können ebenfalls personenbezogene Daten sein. Selbst Zellproben menschlichen Gewebes, die Auskunft über die DNS einer Person geben, können Quellen für die Entnahme biometrischer Daten darstellen,¹⁷³ solange sich die Daten auf die ererbten oder erworbenen genetischen Eigenschaften einer Person beziehen, eindeutige Informationen über ihre Gesundheit oder Physiologie liefern und aus der Analyse einer biologischen Probe der betreffenden Person gewonnen wurden.¹⁷⁴

Anonymisierung

Im Einklang mit dem Grundsatz der Speicherbegrenzung, der sowohl in der DSGVO als auch im Modernisierten Übereinkommen Nr. 108 verankert ist (auf den näher in [Kapitel 3](#) eingegangen wird), müssen Daten „so aufbewahrt

169 a.a.O., Randnr. 17.

170 EGMR, *Von Hannover / Deutschland*, Nr. 59320/00, 24. Juni 2004; EGMR, *Sciacca / Italien*, Nr. 50774/99, 11. Januar 2005; EuGH, C-212/13, *František Ryneš / Úřad pro ochranu osobních údajů*, 11. Dezember 2014.

171 EGMR, *Peck / Vereinigtes Königreich*, Nr. 44647/98, 28. Januar 2003; EGMR, *Köpke / Deutschland* (Entscheidung), Nr. 420/07, 5. Oktober 2010; EDSB (2010), *Leitlinien des Europäischen Datenschutzbeauftragten zur Videoüberwachung*, 17. März 2010.

172 EGMR, *P.G. und J.H. / Vereinigtes Königreich*, Nr. 44787/98, 25. September 2001, Randnrn. 59 und 60; EGMR, *Wisse / Frankreich*, Nr. 71611/01, 20. Dezember 2005 (französischsprachige Fassung).

173 Siehe Artikel-29-Datenschutzgruppe (2007), *Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“*, WP136, 20. Juni 2007, S. 9; Europarat, Empfehlung Nr. Rec (2006) 4 des Ministerkomitees an die Mitgliedstaaten über Forschung mit humanbiologischem Material, 15. März 2006.

174 Datenschutz-Grundverordnung, Artikel 4 Absatz 13.

werden, dass der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die die personenbezogenen Daten verarbeitet worden sind, erfordern.“¹⁷⁵ Daraus ergibt sich, dass Daten gelöscht oder anonymisiert werden müssen, wenn ein Verantwortlicher sie weiter speichern möchte, auch wenn sie nicht mehr benötigt werden und nicht mehr ihrem ursprünglichen Zweck dienen.

Das Verfahren zur Anonymisierung von Daten besteht in der Entfernung aller identifizierenden Elemente aus einem Satz personenbezogener Daten, sodass die betroffene Person nicht mehr identifiziert werden kann.¹⁷⁶ Die Artikel-29-Datenschutzgruppe analysiert in ihrer Stellungnahme 5/2014 die Wirksamkeit und die Grenzen der verschiedenen Anonymisierungstechniken.¹⁷⁷ Sie ist sich des potenziellen Werts solcher Techniken bewusst, betont jedoch, dass bestimmte Techniken nicht unbedingt in jedem Fall funktionieren. Um die in einer gegebenen Situation am besten geeignete Lösung zu finden, sollte das geeignete Anonymisierungsverfahren auf der Grundlage einer Einzelfallbewertung gewählt werden. Unabhängig von der verwendeten Technik, muss die Identifizierung unumkehrbar verhindert werden. Die Anonymisierung von Daten erfordert folglich, dass in den Informationen kein Element verbleiben darf, das dazu dienen könnte, unter zumutbaren Anstrengungen die betreffende(n) Person(en) erneut zu identifizieren.¹⁷⁸ Die Gefahr der erneuten Identifizierung kann unter Berücksichtigung „der in Anbetracht der Art der Daten erforderlichen Zeit, des erforderlichen Aufwands oder der erforderlichen Hilfsmittel, des Kontexts ihrer Nutzung, der verfügbaren Technologien für die erneute Identifizierung und der damit verbundenen Kosten“ beurteilt werden.¹⁷⁹

Wurden Daten erfolgreich anonymisiert, gelten sie nicht mehr als personenbezogene Daten und die Datenschutzvorschriften finden nicht länger Anwendung.

175 a.a.O., Artikel 5 Absatz 1 Buchstabe e; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe e.

176 Datenschutz-Grundverordnung, Erwägungsgrund 26.

177 Artikel-29-Datenschutzgruppe (2014), *Stellungnahme 5/2014 zu Anonymisierungstechniken*, WP216, 10. April 2014.

178 Datenschutz-Grundverordnung, Erwägungsgrund 26.

179 Europarat, Komitee zum Übereinkommen 108 (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. Januar 2017, Absatz 6.2.

Die DSGVO sieht vor, dass die Person oder Organisation, die die Verarbeitung personenbezogener Daten kontrolliert, nicht dazu verpflichtet werden kann, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren. Für diese Regel gibt es jedoch eine wichtige Ausnahme: Wann immer die betroffene Person zum Zwecke der Ausübung der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit dem Verantwortlichen zusätzliche Informationen bereitstellt, die ihre Identifizierung ermöglichen, werden die zuvor anonymisierten Daten erneut zu personenbezogenen Daten.¹⁸⁰

Pseudonymisierung

Personenbezogene Informationen enthalten Kennzeichen wie Name, Geburtsdatum, Geschlecht, Adresse oder sonstige Elemente, die eine Identifizierung ermöglichen könnten. Das Verfahren zur Pseudonymisierung personenbezogener Daten besteht im Ersatz dieser Kennzeichen durch ein Pseudonym.

Das EU-Recht definiert die „Pseudonymisierung“ als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“¹⁸¹ Im Gegensatz zu anonymisierten Daten sind pseudonymisierte Daten nach wie vor personenbezogene Daten und unterliegen demnach den Datenschutzvorschriften. Obgleich die Pseudonymisierung die Sicherheitsrisiken für die betroffenen Personen verringern kann, ist sie nicht vom Anwendungsbereich der DSGVO ausgeschlossen.

Die DSGVO erkennt verschiedene Einsatzmöglichkeiten der Pseudonymisierung als geeignete technische Maßnahme zur Erhöhung des Datenschutzes und besonders für die Technik und Sicherheit ihrer Datenverarbeitung an.¹⁸²

¹⁸⁰ Datenschutz-Grundverordnung, Artikel 11.

¹⁸¹ a.a.O., Artikel 4 Absatz 5.

¹⁸² a.a.O., Artikel 25 Absatz 1.

Sie stellt auch eine geeignete Garantie dar, die zur Verarbeitung personenbezogener Daten zu anderen Zwecken als denjenigen, zu denen sie ursprünglich erhoben wurden, herangezogen werden kann.¹⁸³

In der Begriffsbestimmung des Modernisierten Übereinkommens Nr. 108 des **Europarates** ist die Pseudonymisierung nicht ausdrücklich erwähnt. Aus dem erläuternden Bericht zum Modernisierten Übereinkommen Nr. 108 geht jedoch eindeutig hervor, dass „die Verwendung eines Pseudonyms oder einer beliebigen digitalen Kennung/digitalen Identität nicht zur Anonymisierung der Daten führt, da die betroffene Person nach wie vor identifizierbar sein oder individualisiert werden kann.“¹⁸⁴ Eine Möglichkeit der Pseudonymisierung von Daten ist die Datenverschlüsselung. Sobald die Daten pseudonymisiert wurden, besteht die Verbindung zur Identität in Form des Pseudonyms mit einem Entschlüsselungscode. Ohne diesen Code ist es schwierig, pseudonymisierte Daten zu identifizieren. Wer den Entschlüsselungscode anwenden darf, kann jedoch leicht eine erneute Identifizierung vornehmen. Entschlüsselungscodes müssen besonders gegen die Verwendung durch Unbefugte geschützt werden. Folglich „sind [p]seudonymisierte Daten [...] als personenbezogene Daten zu betrachten [...]“, die unter das Modernisierte Übereinkommen Nr. 108 fallen.¹⁸⁵

Authentifizierung

Hierbei handelt es sich um ein Verfahren, mit dem eine Person beweisen kann, dass sie eine bestimmte Identität besitzt und/oder zu bestimmten Handlungen befugt ist, wie zum Betreten eines Sicherheitsbereichs oder zum Abheben von Geld von einem Bankkonto. Eine Authentifizierung kann durch den Vergleich biometrischer Daten wie Fotos oder Fingerabdrücke in einem Pass mit den Daten erfolgen, die die Person selber beispielsweise bei der Einreisekontrolle vorlegt,¹⁸⁶ oder durch Erfragen von Informationen, die nur der Person mit einer bestimmten Identität oder Genehmigung bekannt sind, wie einer persönlichen Identifizierungsnummer (PIN) oder eines Passwortes; oder durch Vorlage eines bestimmten Gegenstands, der sich ausschließlich im Besitz der Person mit

183 a.a.O., Artikel 6 Absatz 4.

184 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 18.

185 a.a.O.

186 a.a.O., Absätze 56 und 57.

einer bestimmten Identität oder Genehmigung befindet, wie einer besonderen Chipkarte oder eines Schlüssels zu einem Bankschließfach. Abgesehen von Passwörtern und Chipkarten, mitunter in Kombination mit PINs, sind vor allem elektronische Signaturen geeignet, in der elektronischen Kommunikation eine Person zu identifizieren und zu authentifizieren.

2.1.2. Besondere Kategorien personenbezogener Daten

Sowohl im **EU-Recht** als auch im **Recht des Europarates** gibt es besondere Kategorien personenbezogener Daten, die aufgrund ihrer Art bei ihrer Verarbeitung ein Risiko für die betroffenen Personen bedeuten können und daher eines verstärkten Schutzes bedürfen. Die Erhebung solcher Daten ist Gegenstand eines allgemeinen Verbots und ihre Verarbeitung ist nur unter einer begrenzten Anzahl an Voraussetzungen rechtmäßig.

Im Rahmen des Modernisierten Übereinkommens Nr. 108 (Artikel 6) und der DSGVO (Artikel 9) gelten die nachstehenden Kategorien als sensible Daten:

- personenbezogene Daten, aus denen die rassische oder ethnische Herkunft hervorgehen;
- personenbezogene Daten, aus denen politische Meinungen, religiöse oder sonstige Überzeugungen einschließlich philosophischer Überzeugungen hervorgehen;
- personenbezogene Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht;
- zur Identifizierung einer Person verarbeitete genetische Daten und biometrische Daten;
- personenbezogene Daten über Gesundheit, Sexualleben oder sexuelle Orientierung.

Beispiel: In der Rechtssache *Bodil Lindqvist*¹⁸⁷ ging es um den auf einer Internetseite erfolgten Hinweis auf verschiedene Personen durch ihren Namen oder auf andere Weise, wie durch ihre Telefonnummer oder Informationen über ihre Freizeitbeschäftigungen. Der EuGH befand, dass „die Angabe, dass sich eine Person den Fuß verletzt hat und partiell krankgeschrieben ist, zu den personenbezogenen Daten über Gesundheit gehört“.¹⁸⁸

Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten

Das Modernisierte Übereinkommen Nr. 108 schließt personenbezogene Daten über Straftaten, Strafverfahren und Strafurteile und damit verbundene Sicherungsmaßnahmen in die Liste der besonderen Kategorien personenbezogener Daten ein.¹⁸⁹ Im Rahmen der DSGVO werden personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen als solche nicht in der Liste der besonderen Kategorien von personenbezogenen Daten genannt, werden jedoch in einem gesonderten Artikel behandelt. Artikel 10 DSGVO sieht vor, dass die Verarbeitung solcher Daten nur „unter behördlicher Aufsicht vorgenommen werden [darf] oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die persönlichen Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist“. Andererseits können umfassende Register mit Informationen über strafrechtliche Verurteilungen nur unter spezieller behördlicher Aufsicht geführt werden.¹⁹⁰ In der EU ist die Verarbeitung personenbezogener Daten im Kontext der Strafverfolgung durch ein spezielles Rechtsinstrument, die Richtlinie (EU) 2016/680, geregelt.¹⁹¹ Die Richtlinie sieht spezifische Vorschriften für den Datenschutz vor, die für die zuständigen Behörden bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten verbindlich sind (siehe [Abschnitt 8.2.1](#)).

187 EuGH, C-101/01, *Strafverfahren / Bodil Lindqvist*, 6. November 2003, Randnr. 51.

188 Frühere Richtlinie 95/46/EG, Artikel 8 Absatz 1, nun Datenschutz-Grundverordnung, Artikel 9 Absatz 1.

189 Modernisiertes Übereinkommen Nr. 108, Artikel 6 Absatz 1.

190 Datenschutz-Grundverordnung, Artikel 10.

191 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 4.5.2016.

2.2. Datenverarbeitung

Kernpunkte

- „Datenverarbeitung“ betrifft jeden Vorgang im Zusammenhang mit personenbezogenen Daten.
- Der Begriff „Verarbeitung“ umfasst die automatisierte und die nicht automatisierte Verarbeitung.
- Im EU-Recht umfasst „Verarbeitung“ auch die manuelle Verarbeitung in strukturierten Dateien.
- Im Recht des Europarates kann die Bedeutung von „Verarbeitung“ durch innerstaatliches Recht auch auf manuelle Verarbeitung ausgedehnt werden.

2.2.1. Der Begriff „Datenverarbeitung“

Sowohl im EU-Recht als auch im Recht des Europarates ist der Begriff „Verarbeitung“ sehr weit definiert: „Verarbeitung personenbezogener Daten“ [...] bezeichnet jeden Vorgang [...] im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“¹⁹² Das Modernisierte Übereinkommen Nr. 108 fügt dieser Definition noch die Aufbewahrung personenbezogener Daten hinzu.¹⁹³

Beispiel: In der Rechtssache *František Ryneš*¹⁹⁴ erfasste Herr Ryneš über das von ihm zum Schutz seines Eigentums eingerichtete heimische Videoüberwachungssystem das Bild von zwei Personen, die die Fenster seines Hauses einschlugen. Der EuGH befand, dass eine Videoüberwachung, die die Aufzeichnung und Speicherung personenbezogener Daten umfasst, eine automatisierte Datenverarbeitung darstelle, die in den Anwendungsbereich des EU-Datenschutzrechts fällt.

¹⁹² Datenschutz-Grundverordnung, Artikel 4 Absatz 2. Siehe auch Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe b.

¹⁹³ Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe b.

¹⁹⁴ EuGH, C-212/13, *František Ryneš / Úřad pro ochranu osobních údajů*, 11. Dezember 2014, Randnr. 25.

Beispiel: In der Rechtssache *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce gegen Salvatore Manni*¹⁹⁵ ersuchte Herr Manni um die Löschung seiner personenbezogenen Daten aus dem Register einer Ratingagentur, das ihn mit der Liquidation einer Immobiliengesellschaft in Verbindung brachte und sich dadurch schlecht auf seinen Ruf auswirkte. Der EuGH befand, dass „indem die mit der Führung des Registers betraute Stelle diese Informationen in das Register einträgt und darin aufbewahrt und sie gegebenenfalls auf Antrag an Dritte übermittelt, nimmt sie eine „Verarbeitung personenbezogener Daten“ vor, für die sie „Verantwortlicher“ ist“.

Beispiel: Arbeitgeber erheben und verarbeiten Daten über ihre Beschäftigten, einschließlich Informationen über deren Löhne und Gehälter. Die Arbeitsverträge liefern die Rechtsgrundlage für ein diesbezügliches rechtmäßiges Vorgehen.

Die Arbeitgeber haben die Lohn- und Gehaltsdaten ihrer Beschäftigten den Steuerbehörden zu melden. Diese Übermittlung von Daten ist auch eine „Verarbeitung“ im Sinne dieses Begriffs im Modernisierten Übereinkommen Nr. 108 und in der DSGVO. Die Rechtsgrundlage für diese Offenlegung sind jedoch nicht die Arbeitsverträge. Es muss eine weitere Rechtsgrundlage für die Verarbeitungen geben, an deren Ende die Übermittlung von Lohn- und Gehaltsdaten durch den Arbeitgeber an die Steuerbehörden steht. Diese Rechtsgrundlage findet sich normalerweise in den Bestimmungen der innerstaatlichen Steuergesetze. Ohne derartige Bestimmungen und in Ermangelung jedwedes sonstigen berechtigten Grunds für die Verarbeitung wäre die Übermittlung der Daten eine unrechtmäßige Verarbeitung.

2.2.2. Automatisierte Datenverarbeitung

Der Datenschutz nach dem Modernisierten Übereinkommen Nr. 108 und der DSGVO findet auf die automatisierte Datenverarbeitung vollständig Anwendung.

¹⁹⁵ EuGH, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni*, 9. März 2017, Randnr. 35.

Im **EU-Recht** betrifft die automatisierte Datenverarbeitung die „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten“.¹⁹⁶ Das Modernisierte Übereinkommen Nr. 108 enthält eine ähnliche Definition.¹⁹⁷ In der Praxis bedeutet dies, dass jede automatisierte Verarbeitung personenbezogener Daten, die beispielsweise mithilfe eines Computers, eines Mobilgeräts oder eines Routers erfolgt, sowohl unter die Datenschutzvorschriften der EU als auch unter die des Europarates fällt.

Beispiel: In der Rechtssache *Bodil Lindqvist*¹⁹⁸ ging es um den auf einer Internetseite erfolgten Hinweis auf verschiedene Personen durch ihren Namen oder auf andere Weise, wie durch ihre Telefonnummer oder Informationen über ihre Freizeitbeschäftigungen. Der EuGH befand, dass „die Handlung, die darin besteht, auf einer Internetseite auf verschiedene Personen hinzuweisen und diese entweder durch ihren Namen oder auf andere Weise, etwa durch Angabe ihrer Telefonnummer oder durch Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen, erkennbar zu machen, eine ‚ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten‘“ im Sinne von Artikel 3 Absatz 1 der Richtlinie 95/46/EG darstellt.¹⁹⁹

Beispiel: In der Rechtssache *Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos (AEPD), Mario Costeja González*²⁰⁰ ersuchte Herr González um die Löschung oder Veränderung einer Verbindung zwischen seinem Namen in der Google-Suchmaschine und zwei Seiten einer Tageszeitung, auf denen die Versteigerung eines Grundstücks wegen Forderungen der Sozialversicherung angekündigt wurde. Der EuGH stellte Folgendes fest: „Indem er das Internet automatisch, kontinuierlich und systematisch auf die dort veröffentlichten Informationen durchforstet, ‚erhebt‘ der Suchmaschinenbetreiber mithin personenbezogene Daten, die er dann mit seinen Indexierprogrammen ‚ausliest‘, ‚speichert‘ und ‚organisiert‘, auf seinen Servern ‚aufbewahrt‘ und gegebenenfalls in Form von Ergebnislisten

¹⁹⁶ Datenschutz-Grundverordnung, Artikel 2 Absatz 1 und Artikel 4 Absatz 2.

¹⁹⁷ Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstaben b und c; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 21.

¹⁹⁸ EuGH, C-101/01, *Strafverfahren / Bodil Lindqvist*, 6. November 2003, Randnr. 27.

¹⁹⁹ Datenschutz-Grundverordnung, Artikel 2 Absatz 1.

²⁰⁰ EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014.

an seine Nutzer ‚weitergibt‘ und diesen, bereitstellt“.²⁰¹ Der EuGH befand, dass solche Handlungen als „Verarbeitung“ einzustufen sind, „ohne dass es darauf ankommt, ob der Suchmaschinenbetreiber dieselben Vorgänge auch bei anderen Arten von Informationen ausführt und ob er zwischen diesen Informationen und personenbezogenen Daten unterscheidet“.

2.2.3. Nicht automatisierte Datenverarbeitung

Auch die manuelle Datenverarbeitung erfordert Datenschutz.

Im EU-Recht ist der Datenschutz keineswegs auf automatisierte Datenverarbeitung beschränkt. Entsprechend findet der Datenschutz im EU-Recht auf die Verarbeitung personenbezogener Daten in einem manuellen Dateisystem Anwendung, d. h. in einer speziell strukturierten Papierakte.²⁰² Ein strukturiertes Dateisystem ist ein Dateisystem, das einen Satz personenbezogener Daten kategorisiert und nach Maßgabe bestimmter Kriterien zugänglich macht. Wenn ein Arbeitgeber beispielsweise eine Papierakte mit dem Titel „Urlaub der Beschäftigten“ führt, die sämtliche Einzelheiten über die Urlaube enthält, die die Beschäftigten im vergangenen Jahr in Anspruch genommen haben, und in alphabetischer Reihenfolge geordnet ist, stellt diese Akte ein manuelles Dateisystem dar, das den Datenschutzvorschriften der EU unterliegt. Der Grund für diese Ausdehnung des Datenschutzes liegt darin, dass:

- Papierakten derart strukturiert sein können, dass sie ein schnelles und leichtes Auffinden der Informationen ermöglichen;
- durch die Speicherung personenbezogener Daten in einer strukturierten Papierakte die gesetzlich festgesetzten Beschränkungen für die automatisierte Datenverarbeitung leicht umgangen werden können.²⁰³

Im Recht des Europarates erkennt die Definition der automatisierten Verarbeitung an, dass zwischen automatisierten Vorgängen einige Phasen der manuellen Verwendung personenbezogener Daten erforderlich sein können.²⁰⁴ Artikel 2 Buchstabe c des Modernisierten Übereinkommens Nr. 108 besagt:

²⁰¹ a.a.O., Randnr. 28.

²⁰² Datenschutz-Grundverordnung, Artikel 2 Absatz 1.

²⁰³ Datenschutz-Grundverordnung, Erwägungsgrund 15.

²⁰⁴ Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe b und c.

„Sofern nicht auf die automatisierte Verarbeitung zurückgegriffen wird, ist unter ‚Datenverarbeitung‘ ein Vorgang oder eine Reihe von Vorgängen im Zusammenhang mit personenbezogenen Daten innerhalb einer strukturierten Sammlung dieser Daten zu verstehen, die nach Maßgabe bestimmter Kriterien zugänglich oder abrufbar ist“.

2.3. Verwender personenbezogener Daten

Kernpunkte

- Wer auch immer über die Mittel und Zwecke der Verarbeitung von personenbezogenen Daten anderer entscheidet, ist nach dem Datenschutzrecht ein „Verantwortlicher“; wird diese Entscheidung von mehreren Personen getroffen, spricht man von „gemeinsam für die Verarbeitung Verantwortlichen“.
- Ein „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.
- Ein Auftragsverarbeiter wird zu einem Verantwortlichen, wenn er über die Mittel und Zwecke der Verarbeitung von personenbezogenen Daten selbst entscheidet.
- Jede Person, der personenbezogene Daten offengelegt werden, ist ein „Empfänger“.
- Ein „Dritter“ ist eine natürliche oder juristische Person außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.
- Die Einwilligung als Rechtsgrundlage der Verarbeitung personenbezogener Daten ist eine ohne Zwang, in Kenntnis der Sachlage, für den konkreten Fall und unmissverständlich abgegebene Willensbekundung in Form einer eindeutigen bestätigenden Handlung, die das Einverständnis mit der Verarbeitung bedeutet.
- Die auf Grundlage einer Einwilligung erfolgende Verarbeitung besonderer Kategorien personenbezogener Daten erfordert eine ausdrückliche Einwilligung.

2.3.1. Verantwortliche und Auftragsverarbeiter

Die wohl wichtigste Konsequenz der Tatsache, dass jemand Verantwortlicher oder Auftragsverarbeiter ist, liegt darin, dass er nach dem Gesetz für die Einhaltung der jeweiligen im Datenschutzrecht festgelegten Verpflichtungen verantwortlich ist. Im privaten Sektor ist dies üblicherweise eine natürliche oder juristische Person, im öffentlichen Sektor normalerweise eine Behörde. Es gibt

einen wesentlichen Unterschied zwischen einem Verantwortlichen und einem Auftragsverarbeiter: bei Ersterem handelt es sich um die natürliche oder juristische Person, die über die Mittel und Zwecke der Verarbeitung entscheidet, während es sich bei Letzterem um die natürliche oder juristische Person handelt, die die Daten unter Befolgung strenger Anweisungen im Auftrag des Verantwortlichen verarbeitet. Grundsätzlich ist es der Verantwortliche, der die Kontrolle über die Verarbeitung ausüben muss und die diesbezügliche Verantwortung einschließlich der rechtlichen Haftung trägt. Durch die Reform der Datenschutzvorschriften sind Auftragsverarbeiter nun jedoch zur Erfüllung vieler Auflagen verpflichtet, die für die Verantwortlichen gelten. Nach Maßgabe der DSGVO müssen Auftragsverarbeiter zum Nachweis der Einhaltung ihrer Verpflichtungen aus der Verordnung beispielsweise ein Verzeichnis zu allen Kategorien von Tätigkeiten der Verarbeitung führen.²⁰⁵ Auftragsverarbeiter müssen auch geeignete technische und organisatorische Maßnahmen treffen, um den Schutz der Verarbeitung zu gewährleisten,²⁰⁶ in bestimmten Situationen einen Datenschutzbeauftragten benennen²⁰⁷ und Verletzungen des Datenschutzes dem Verantwortlichen melden.²⁰⁸

Ob eine Person über die Fähigkeit verfügt, über die Zwecke und Mittel der Verarbeitung zu entscheiden und diese festzusetzen, hängt von den Sachverhalten und Umständen des Falles ab. Nach der Definition des Begriffs „Verantwortlicher“ in der DSGVO können natürliche Personen, juristische Personen oder jedwede anderen Stellen ein Verantwortlicher sein. Um den Einzelnen ein stabileres Gebilde für die Ausübung ihrer Rechte zu bieten, hob die Artikel-29-Datenschutzgruppe jedoch hervor, dass „bevorzugt das Unternehmen oder die Stelle an sich als für die Verarbeitung Verantwortlicher betrachtet werden [sollte] und nicht eine bestimmte Person innerhalb des Unternehmens oder der Stelle“.²⁰⁹ So ist beispielsweise ein Unternehmen, das Gesundheitsprodukte an Ärzte verkauft, der Verantwortliche für die Erstellung und Führung der Verteilerliste sämtlicher Ärzte in einem bestimmten Gebiet, und nicht der Vertriebsleiter, der diese Liste verwendet und führt.

205 Datenschutz-Grundverordnung, Artikel 30 Absatz 2.

206 a.a.O., Artikel 32.

207 a.a.O., Artikel 37.

208 a.a.O., Artikel 33 Absatz 2.

209 Artikel-29-Datenschutzgruppe (2010), *Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“*, WP 169, Brüssel, 16. Februar 2010.

Beispiel: Wenn die Marketingabteilung des Unternehmens Sunshine die Verarbeitung personenbezogener Daten für eine Marktstudie plant, ist das Unternehmen Sunshine und nicht die Mitarbeiter der Marketingabteilung der Verantwortliche. Die Marketingabteilung verfügt über keine eigene Rechtspersönlichkeit und kann daher nicht der Verantwortliche sein.

Sowohl im EU-Recht als auch im Recht des Europarates kann es sich bei den Verantwortlichen um natürliche Personen handeln. Individuen, die Daten anderer Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten verarbeiten, fallen jedoch nicht unter die Vorschriften der DSGVO und des Modernisierten Übereinkommens Nr. 108 und gelten nicht als Verantwortliche.²¹⁰ Eine Privatperson, die ihren Schriftverkehr in Form eines persönlichen Tagebuchs führt und darin Begebenheiten mit Freunden und Kollegen und Gesundheitsdaten von Familienmitgliedern beschreibt, kann von den Datenschutzvorschriften freigestellt werden, da es sich bei diesen Tätigkeiten um rein persönliche oder familiäre Tätigkeiten handeln könnte. Ferner präzisiert die DSGVO, dass als persönliche oder familiäre Tätigkeiten auch die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten könnten.²¹¹ Die Datenschutzvorschriften gelten hingegen in vollem Umfang für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für persönliche oder familiäre Tätigkeiten bereitstellen (beispielsweise Plattformen für soziale Netzwerke).²¹²

Durch den Zugang der Bürger zum Internet und die Möglichkeit der Nutzung von E-Commerce-Plattformen, sozialen Netzwerken und Blog-Seiten zum Teilen personenbezogener Informationen über sich selbst und andere Personen, wird es zunehmend schwerer, die persönliche Verarbeitung von der nicht persönlichen Verarbeitung zu unterscheiden.²¹³ Ob Tätigkeiten rein persönlich oder familiär sind, hängt von den Umständen ab.²¹⁴ Tätigkeiten, die berufliche oder wirtschaftliche Aspekte aufweisen, können nicht

210 Datenschutz-Grundverordnung, Erwägungsgrund 18 und Artikel 2 Absatz 2 Buchstabe c; Modernisiertes Übereinkommen Nr. 108, Artikel 3 Buchstabe 2.

211 Datenschutz-Grundverordnung, Erwägungsgrund 18.

212 *a.a.O.*, Erwägungsgrund 18; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 29.

213 Siehe die Erklärung der Artikel-29-Datenschutzgruppe zu den Diskussionen in Bezug auf das Reformpaket zum Datenschutz (2013), *Annex 2: Proposals and Amendments regarding exemption for personal or household activities*, 27. Februar 2013.

214 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 28.

unter die Ausnahmeregelung für familiäre Tätigkeiten fallen.²¹⁵ Wenn das Ausmaß und die Häufigkeit der Datenverarbeitung auf eine berufliche oder Vollzeittätigkeit hindeuten, könnte eine Privatperson folglich als Verantwortlicher betrachtet werden. Neben dem beruflichen oder wirtschaftlichen Charakter der Verarbeitungstätigkeit ist noch ein weiterer Umstand zu berücksichtigen, der darin besteht, ob die personenbezogenen Daten einer großen Anzahl von sich selbstverständlich außerhalb der Privatsphäre der Person befindenden Personen zur Verfügung gestellt werden. Die Rechtsprechung zur Datenschutzrichtlinie befand, dass das Datenschutzrecht Anwendung findet, wenn eine Privatperson im Zuge der Internetnutzung Daten über andere Personen auf einer öffentlichen Webseite veröffentlicht. Bislang hat der EuGH noch nicht über vergleichbare Sachverhalte nach Maßgabe der DSGVO entschieden, die eine größere Orientierungshilfe zu Themen liefert, die im Rahmen der Ausnahmeregelung für familiäre Tätigkeiten als außerhalb des Geltungsbereichs der Datenschutzvorschriften betrachtet werden könnten, wie beispielsweise die Nutzung sozialer Medien zu persönlichen Zwecken.

Beispiel: In der Rechtssache *Bodil Lindqvist*²¹⁶ ging es um den auf einer Internetseite erfolgten Hinweis auf verschiedene Personen durch ihren Namen oder auf andere Weise, wie durch ihre Telefonnummer oder Informationen über ihre Freizeitbeschäftigungen. Der EuGH befand, dass „die Handlung, die darin besteht, auf einer Internetseite auf verschiedene Personen hinzuweisen und diese entweder durch ihren Namen oder auf andere Weise [...] erkennbar zu machen, eine ‚ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten‘“ im Sinne von Artikel 3 Absatz 1 der Datenschutzrichtlinie darstellt.²¹⁷

Eine derartige Verarbeitung personenbezogener Daten gehört nicht zu ausschließlich persönlichen oder familiären Tätigkeiten, die nicht in den Anwendungsbereich der Datenschutzvorschriften der EU fallen, da diese Ausnahme „somit dahin auszulegen ist, dass mit ihr nur Tätigkeiten gemeint sind, die zum Privat- oder Familienleben von Einzelpersonen gehören, was

215 Siehe Datenschutz-Grundverordnung, Erwägungsgrund 18 und Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 27.

216 EuGH, C-101/01, *Strafverfahren / Bodil Lindqvist*, 6. November 2003.

217 a.a.O., Randnr. 27; Frühere Richtlinie 95/46/EG, Artikel 3 Absatz 1, nun Datenschutz-Grundverordnung, Artikel 2 Absatz 1.

offensichtlich nicht der Fall ist bei der Verarbeitung personenbezogener Daten, die in deren Veröffentlichung im Internet besteht, so dass diese Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden.“²¹⁸

Dem EuGH zufolge können die Videoaufzeichnungen einer privat installierten Überwachungskamera unter bestimmten Umständen ebenfalls unter die Datenschutzvorschriften der EU fallen.

Beispiel: In der Rechtssache *František Ryneš*²¹⁹ erfasste Herr Ryneš über das von ihm zum Schutz seines Eigentums eingerichtete heimische Videoüberwachungssystem das Bild von zwei Personen, die die Fenster seines Hauses einschlugen. Die Aufzeichnungen wurden der Polizei übergeben und anschließend im Rahmen des eingeleiteten Strafverfahrens verwertet.

Der EuGH befand, dass „[s]oweit sich eine Videoüberwachung [...] auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten auf diese Weise verarbeitet, kann sie nicht als eine ausschließlich „persönliche oder familiäre“ Tätigkeit [...] angesehen werden.“²²⁰

Verantwortlicher

Im EU-Recht wird der Verantwortliche definiert als derjenige, der „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.²²¹ Der Verantwortliche setzt fest, warum und wie Daten verarbeitet werden.

Im Recht des Europarates definiert das Modernisierte Übereinkommen Nr. 108 einen „Verantwortlichen“ als „die natürliche oder juristische Person, die Behörde, den Dienst, die Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Entscheidungsbefugnis in Bezug auf die

218 EuGH, C-101/01, *Strafverfahren / Bodil Lindqvist*, 6. November 2003, Randnr. 47.

219 EuGH, C-212/13, *František Ryneš / Úřad pro ochranu osobních údajů*, 11. Dezember 2014, Randnr. 33.

220 Frühere Richtlinie 95/46/EG, Artikel 3 Absatz 2, nun Datenschutz-Grundverordnung, Artikel 2 Absatz 2.

221 Datenschutz-Grundverordnung, Artikel 4 Absatz 7.

Datenverarbeitung verfügt".²²² Diese Entscheidungsbefugnis betrifft sowohl die Zwecke und Mittel der Verarbeitung als auch die zu verarbeitenden Datenkategorien und den Zugang zu den Daten.²²³ Ob sich diese Befugnis aus einer rechtlichen Bestellung oder aus den tatsächlichen Umständen ergibt, ist für jeden Einzelfall zu entscheiden.²²⁴

Beispiel: Die Rechtssache *Google Spain*²²⁵ wurde von einem Spanier eingeleitet, der wollte, dass ein alter Zeitungsbericht über seine finanzielle Vorgeschichte aus Google gelöscht wird.

Der EuGH wurde gefragt, ob Google als Betreiber einer Suchmaschine der „Verantwortliche“ der Daten im Sinne von Artikel 2 Buchstabe d der Datenschutzrichtlinie sei.²²⁶ Der EuGH zog eine weite Bestimmung des Begriffs des „Verantwortlichen“ in Betracht, um „einen wirksamen und umfassenden Schutz der betroffenen Personen“ zu gewährleisten.²²⁷ Der EuGH befand, dass der Suchmaschinenbetreiber über die Zwecke und Mittel dieser Tätigkeit entscheide und seitens Herausgebern von Websites auf Internetseiten gestellte Daten jedem Internetnutzer zugänglich mache, der eine Suche anhand des Namens der betreffenden Person durchführt.²²⁸ Daher entschied der EuGH, dass Google als der „Verantwortliche“ angesehen werden kann.²²⁹

Wenn ein Verantwortlicher oder Auftragsverarbeiter nicht in der EU niedergelassen ist, benennt dieses Unternehmen schriftlich einen Vertreter in der EU.²³⁰ Die DSGVO betont, dass der Vertreter „in einem der Mitgliedstaaten [niedergelassen sein muss], in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder

222 Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe d.

223 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 22.

224 a.a.O.

225 EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014.

226 Datenschutz-Grundverordnung, Artikel 4 Absatz 7; EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014, Randnr. 21.

227 EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014, Randnr. 34.

228 a.a.O., Randnrn. 35–40.

229 a.a.O., Randnr. 41.

230 Datenschutz-Grundverordnung, Artikel 27 Absatz 1.

Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, sich befinden".²³¹ Sofern kein Vertreter benannt ist, können gleichwohl rechtliche Schritte gegen den Verantwortlichen oder den Auftragsverarbeiter selbst eingeleitet werden.²³²

Gemeinsame Verantwortung für die Verarbeitung

Die DSGVO sieht vor, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, sie gemeinsam Verantwortliche sind. Das bedeutet, dass sie gemeinsam beschließen, Daten für einen gemeinsamen Zweck zu verarbeiten.²³³ Im erläuternden Bericht zum Modernisierten Übereinkommen Nr. 108 heißt es, dass im **Rechtsrahmen des Europarates** auch mehrere Verantwortliche oder eine Mitverantwortung möglich sind.²³⁴

Die Artikel-29-Datenschutzgruppe weist darauf hin, dass die gemeinsame Verantwortung verschiedene Formen aufweisen kann und die Beteiligung der verschiedenen Verantwortlichen an den Kontrolltätigkeiten ungleichmäßig verteilt sein kann.²³⁵ Eine solche Flexibilität ermöglicht es, den zunehmend komplexen Gegebenheiten im Bereich der Datenverarbeitung Rechnung zu tragen.²³⁶ Zur Erfüllung der durch die Verordnung auferlegten Pflichten müssen die gemeinsam für die Verarbeitung Verantwortlichen ihre jeweiligen Verantwortlichkeiten demnach in einer spezifischen Vereinbarung festsetzen.²³⁷

Die gemeinsame Verantwortung für die Verarbeitung führt zu einer gemeinsamen Verantwortlichkeit für eine Verarbeitungstätigkeit.²³⁸ Im Rahmen des **EU-Rechts** bedeutet dies, dass jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten durch die unter gemeinsamer Verantwortung

²³¹ a.a.O., Artikel 27 Absatz 3.

²³² a.a.O., Artikel 27 Absatz 5.

²³³ a.a.O., Artikel 4 Absatz 7 und Artikel 26.

²³⁴ Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe d; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 22.

²³⁵ Artikel-29-Datenschutzgruppe (2010), *Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“*, WP 169, Brüssel, 16. Februar 2010, S. 19.

²³⁶ a.a.O.

²³⁷ Datenschutz-Grundverordnung, Erwägungsgrund 79.

²³⁸ a.a.O., Randnr. 21.

erfolgte Verarbeitung verursachten Schaden haftbar gemacht werden kann, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.²³⁹

Beispiel: Ein Beispiel für eine gemeinsame Verantwortung für die Verarbeitung ist eine von mehreren Kreditinstituten geführte Datenbank über säumige Kunden. Beantragt nun jemand eine Kreditlinie bei einer Bank, die zu den gemeinsam Verantwortlichen gehört, führt die Bank eine Abfrage der Datenbank durch, um in Kenntnis der Sachlage über die Kreditwürdigkeit des Antragstellers entscheiden zu können.

In den gesetzlichen Bestimmungen ist nicht ausdrücklich geregelt, ob bei gemeinsamer Verantwortung alle Verantwortlichen den gleichen Zweck verfolgen müssen, oder ob es ausreicht, wenn sich ihre Zwecke teilweise überschneiden. Bislang liegt allerdings auf europäischer Ebene noch keine Rechtsprechung zu dieser Frage vor. In ihrer Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ aus dem Jahr 2010 legt die Artikel-29-Datenschutzgruppe dar, dass bei gemeinsam für die Verarbeitung Verantwortlichen entweder alle Zwecke und Mittel der Verarbeitung vollständig übereinstimmen können oder aber nur einige Zwecke oder Mittel oder nur Teile davon.²⁴⁰ Während Ersteres eine sehr enge Bindung zwischen den verschiedenen Akteuren bedeuten würde, würde Letzteres auf eine lockerere Bindung hinweisen.

Die Artikel-29-Datenschutzgruppe plädiert für eine breitere Auslegung des Begriffs der gemeinsamen Verantwortung, damit eine gewisse Flexibilität möglich ist, um der zunehmenden Komplexität der heutigen Gegebenheiten im Bereich der Datenverarbeitung Rechnung zu tragen.²⁴¹ Ein Fall, an dem die Society for Worldwide Interbank Financial Telecommunication (SWIFT) beteiligt war, verdeutlicht die Haltung der Datenschutzgruppe.

Beispiel: Im so genannten SWIFT-Fall nutzten europäische Banken SWIFT, anfänglich als Auftragsverarbeiter, um Daten im Zuge von Bankgeschäften zu übertragen. SWIFT gab diese Daten über Banktransaktionen, die in einem

239 a.a.O., Artikel 82 Absatz 4.

240 Artikel-29-Datenschutzgruppe (2010), *Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“*, WP 169, Brüssel, 16. Februar 2010, S. 19.

241 a.a.O.

Rechendienstleistungszentrum in den Vereinigten Staaten gespeichert waren, an das US-Finanzministerium weiter, ohne hierzu ausdrücklich von den europäischen Banken, die es nutzten, beauftragt worden zu sein. Bei der Prüfung der Rechtmäßigkeit dieses Vorgangs kam die Artikel-29-Datenschutzgruppe zu dem Schluss, dass die europäischen Banken, die SWIFT verwendeten, aber auch SWIFT selber gegenüber den europäischen Kunden als gemeinsam für die Verarbeitung Verantwortliche anzusehen seien, die die Daten an die US-Behörden weitergegeben hatten.²⁴²

Auftragsverarbeiter

Als Auftragsverarbeiter ist **im EU-Recht** eine Person definiert, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.²⁴³ Die einem Auftragsverarbeiter übertragenen Tätigkeiten können auf eine ganz konkrete Aufgabe oder einen ganz bestimmten Kontext beschränkt oder auch recht allgemeiner Art und umfassend sein.

Im Recht des Europarates hat der Begriff des Auftragsverarbeiters die gleiche Bedeutung wie im EU-Recht.²⁴⁴

Auftragsverarbeiter verarbeiten nicht nur Daten für andere, sondern sind selber auch Verantwortliche bei Verarbeitungen, die sie für eigene Zwecke vornehmen, wie beispielsweise bei der Verwaltung ihrer Beschäftigten, Verkäufe und Konten.

Beispiel: Das Unternehmen Everready hat sich auf die Datenverarbeitung für andere Unternehmen im Bereich Verwaltung der Humanressourcen spezialisiert. In dieser Rolle ist Everready ein Auftragsverarbeiter. Sobald Everready jedoch die Daten der eigenen Beschäftigten verarbeitet, ist es Verantwortlicher bezüglich von Verarbeitungen, mit denen es seinen Pflichten als Arbeitgeber nachkommt.

242 Artikel- 29-Datenschutzgruppe (2006), *Stellungnahme 10/2006 zur Verarbeitung personenbezogener Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Brüssel, 22. November 2006.

243 Datenschutz-Grundverordnung, Artikel 4 Absatz 8.

244 Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe f.

Beziehung zwischen Verantwortlichem und Auftragsverarbeiter

Wie wir bereits gesehen haben, ist der Verantwortliche als derjenige definiert, der die Zwecke und die Mittel der Verarbeitung bestimmt. Die DSGVO legt eindeutig dar, dass der Auftragsverarbeiter personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten darf, es sei denn, der Auftragsverarbeiter ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet.²⁴⁵ Der Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter stellt einen wesentlichen Bestandteil ihrer Beziehung und eine rechtliche Voraussetzung dar.²⁴⁶

Beispiel: Der Geschäftsführer des Unternehmens Sunshine beschließt, dass das Unternehmen Cloudy, Spezialist für Cloud-basierte Datenspeicherung, die Kundendaten von Sunshine verwalten soll. Das Unternehmen Sunshine bleibt der Verantwortliche, und Cloudy ist lediglich Auftragsverarbeiter, da gemäß Vertrag Cloudy die Kundendaten des Unternehmens Sunshine nur für die von Sunshine festgelegten Zwecke verwenden darf.

Wird die Befugnis zur Bestimmung der Mittel der Verarbeitung an einen Auftragsverarbeiter delegiert, muss der Verantwortliche dessen ungeachtet weiter in der Lage sein, ein angemessenes Maß an Kontrolle über die Entscheidungen des Auftragsverarbeiters über die Mittel der Verarbeitung auszuüben. Die Gesamtverantwortung liegt nach wie vor beim Verantwortlichen, der die Auftragsverarbeiter überwachen muss, um zu gewährleisten, dass deren Entscheidungen im Einklang mit dem Datenschutzrecht und mit seinen eigenen Weisungen stehen.

Sollte sich ein Auftragsverarbeiter ferner nicht an die vom Verantwortlichen vorgegebenen Bedingungen für die Datenverarbeitung halten, ist der Auftragsverarbeiter zumindest insoweit zu einem Verantwortlichen geworden, wie er gegen die Weisungen des Verantwortlichen verstoßen hat. Damit dürfte der Auftragsverarbeiter höchstwahrscheinlich zu einem Verantwortlichen werden, der rechtswidrig handelt. Der ursprüngliche Verantwortliche dürfte wiederum erklären müssen, wie es so weit kommen konnte, dass der Auftragsverarbeiter

²⁴⁵ Datenschutz-Grundverordnung, Artikel 29.

²⁴⁶ a.a.O., Artikel 28 Absatz 3.

gegen seinen Auftrag verstoßen konnte.²⁴⁷ Die Artikel-29-Datenschutzgruppe neigt dazu, in derartigen Fällen von gemeinsamer Verantwortung auszugehen, da sich so der bestmögliche Schutz der Interessen der betroffenen Personen erreichen lässt.²⁴⁸

Probleme bei der Aufteilung der Verantwortung können auch auftreten, wenn der Verantwortliche ein kleines Unternehmen und der Auftragsverarbeiter ein großes Unternehmen ist, das die Bedingungen für die Erbringung seiner Dienstleistungen diktieren kann. Auch unter diesen Umständen sollte allerdings nach Auffassung der Artikel-29-Datenschutzgruppe das Verantwortungsniveau nicht wegen wirtschaftlichen Ungleichgewichts gesenkt werden und sollte sich an der Auslegung des Begriffs des Verantwortlichen nichts ändern.²⁴⁹

Der Klarheit und Transparenz halber sind die Einzelheiten der Beziehung zwischen einem Verantwortlichen und einem Auftragsverarbeiter in einem schriftlichen Vertrag festzuhalten.²⁵⁰ Der Vertrag muss insbesondere den Gegenstand, die Art, den Zweck und die Dauer der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen enthalten. Darüber hinaus sollte er auch die Pflichten und Rechte des Verantwortlichen festlegen, wie die Anforderungen in Bezug auf Vertraulichkeit und Sicherheit. Das Fehlen eines solchen Vertrags stellt einen Verstoß gegen die Pflicht des Verantwortlichen zur Bereitstellung einer schriftlichen Dokumentation der gegenseitigen Zuständigkeiten dar und könnte Sanktionen nach sich ziehen. Wenn durch Nichtbeachtung oder Nichteinhaltung der rechtmäßigen Weisungen des Verantwortlichen Schaden verursacht wird, kann nicht nur der Verantwortliche sondern auch der Auftragsverarbeiter haftbar gemacht werden.²⁵¹ Der Auftragsverarbeiter führt Verzeichnisse zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.²⁵² Diese Verzeichnisse sind der Aufsichtsbehörde auf Anfrage zur

247 a.a.O., Artikel 82 Absatz 2.

248 Artikel-29-Datenschutzgruppe (2010), *Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“*, WP 169, Brüssel, 16. Februar 2010, S. 25; Artikel-29-Datenschutzgruppe (2006), *Stellungnahme 10/2006 zur Verarbeitung personenbezogener Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Brüssel, 22. November 2006.

249 Artikel-29-Datenschutzgruppe (2010), *Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“*, WP 169, Brüssel, 16. Februar 2010, S. 26.

250 Datenschutz-Grundverordnung, Artikel 28 Absatz 3 und 9.

251 a.a.O., Artikel 82 Absatz 2.

252 a.a.O., Artikel 30 Absatz 2.

Verfügung zu stellen, da der Verantwortliche und der Auftragsverarbeiter mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten müssen.²⁵³ Verantwortliche und Auftragsverarbeiter haben auch die Möglichkeit der Einhaltung genehmigter Verhaltensregeln oder eines Zertifizierungsverfahrens, um ihre Übereinstimmung mit den Anforderungen der DSGVO nachzuweisen.²⁵⁴

Es kann vorkommen, dass Auftragsverarbeiter bestimmte Aufgaben an Unterauftragsverarbeiter delegieren möchten. Dies ist rechtlich zulässig, sofern entsprechende Vertragsbestimmungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgesetzt wurden, in denen auch geregelt sein sollte, ob die Zustimmung des für die Verarbeitung Verantwortlichen in jedem Einzelfall erforderlich ist oder ob allein seine Unterrichtung ausreicht. Die DSGVO setzt fest, dass der erste Auftragsverarbeiter gegenüber dem Verantwortlichen haftet, sofern ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nachkommt.²⁵⁵

Im Recht des Europarates gelten in vollem Umfang die oben bereits erläuterten Definitionen der Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“.²⁵⁶

2.3.2. Empfänger und Dritte

Der Unterschied zwischen diesen beiden mit der Datenschutzrichtlinie eingeführten Kategorien von Personen oder Stellen liegt hauptsächlich in ihrer Beziehung zum Verantwortlichen und folglich in ihrer Befugnis, auf im Besitz des Verantwortlichen befindliche Daten zuzugreifen.

Ein „Dritter“ unterscheidet sich vom Verantwortlichen und vom Auftragsverarbeiter. Gemäß Artikel 4 Absatz 10 DSGVO ist ein Dritter „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu

253 a.a.O., Artikel 30 Absatz 4 und Artikel 31.

254 a.a.O., Artikel 28 Absatz 5 und Artikel 42 Absatz 4.

255 a.a.O., Artikel 28 Absatz 4.

256 Siehe beispielsweise Modernisiertes Übereinkommen Nr. 108, Artikel 2 Buchstabe b und f; Profiling-Empfehlung, Artikel 1.

verarbeiten“. Das bedeutet, dass Personen, die in einem anderen Unternehmen arbeiten, auch wenn dieses demselben Konzern oder derselben Holding angehört, als „Dritte“ (oder zu einem Dritten gehörend) angesehen werden. Auf der anderen Seite dürfen Bankfilialen, die Verarbeitungen im Bereich der Kundenverwaltung unter der unmittelbaren Verantwortung des Hauptsitzes durchführen, nicht als „Dritte“ angesehen werden.²⁵⁷

Der Begriff „Empfänger“ ist breiter gefasst als der des „Dritten“. Nach Artikel 4 Absatz 9 DSGVO ist ein Empfänger „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht“. Dieser Empfänger kann entweder eine Person sein, die nicht zum Verantwortlichen oder dem Auftragsverarbeiter gehört und dann ein „Dritter“ wäre, oder eine Person, die zum Verantwortlichen oder Auftragsverarbeiter gehört, also ein Beschäftigter oder eine andere Abteilung innerhalb desselben Unternehmens oder derselben Behörde.

Im Hinblick auf die Voraussetzungen für eine rechtmäßige Offenlegung von Daten ist die Unterscheidung zwischen Empfängern und Dritten sehr wichtig. Die Beschäftigten eines Verantwortlichen oder Auftragsverarbeiters können ohne weitere rechtliche Anforderungen Empfänger personenbezogener Daten sein, wenn sie in die Verarbeitungsvorgänge des Verantwortlichen oder Auftragsverarbeiters eingebunden sind. Ein Dritter hingegen, der nichts mit dem Verantwortlichen oder Auftragsverarbeiter zu tun hat, ist nicht befugt, die vom Verantwortlichen verarbeiteten personenbezogenen Daten zu verwenden, sofern es für den konkreten Fall keine besondere Rechtsgrundlage gibt.

Beispiel: Ein Beschäftigter eines Verantwortlichen, der personenbezogene Daten bei der Wahrnehmung der ihm vom Arbeitgeber übertragenen Aufgaben verwendet, ist Datenempfänger, nicht jedoch Dritter, da er die Daten im Namen und auf Weisung des Verantwortlichen verwendet. Sofern ein Arbeitgeber beispielsweise seiner Personalabteilung im Hinblick auf bevorstehende Leistungsbewertungen personenbezogene Daten über seine Beschäftigten offenlegt, ist das Team der Personalabteilung der Empfänger der personenbezogenen Daten, da ihm die Daten im Zuge der Verarbeitung für den Verantwortlichen offengelegt wurden.

²⁵⁷ Artikel-29-Datenschutzgruppe (2010), *Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“*, WP 169, Brüssel, 16. Februar 2010, S. 31.

Stellt das Unternehmen die Daten über seine Beschäftigten hingegen einem Schulungsunternehmen bereit, das diese zur Ausarbeitung eines Schulungsprogramms für die Beschäftigten verwendet, so ist das Schulungsunternehmen ein Dritter. Dies liegt daran, dass das Schulungsunternehmen nicht über die spezielle Rechtmäßigkeit oder Befugnis (die sich im Falle der „Personalabteilung“ aus dem Beschäftigungsverhältnis mit dem Verantwortlichen ergibt) zur Verarbeitung dieser personenbezogenen Daten verfügt. Anders ausgedrückt, hat das Schulungsunternehmen die Informationen nicht im Zuge seiner Beschäftigung beim Verantwortlichen erhalten.

2.4. Einwilligung

Kernpunkte

- Die Einwilligung als Rechtsgrundlage der Verarbeitung personenbezogener Daten ist eine ohne Zwang, in Kenntnis der Sachlage, für den konkreten Fall und unmissverständlich abgegebene Willensbekundung in Form einer eindeutigen bestätigenden Handlung, die das Einverständnis mit der Verarbeitung bedeutet.
- Die Verarbeitung besonderer Kategorien personenbezogener Daten erfordert eine ausdrückliche Einwilligung.

Wie in [Kapitel 4](#) detailliert behandelt wird, stellt die Einwilligung einen der sechs berechtigten Gründe für die Verarbeitung personenbezogener Daten dar. Einwilligung bezeichnet „jede ohne Zwang für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Willensbekundung der betroffenen Person.“²⁵⁸

Nach dem **EU-Recht** müssen mehrere Elemente gegeben sein, damit eine Einwilligung gültig ist, mit denen gewährleistet werden soll, dass betroffene Personen einer bestimmten Verwendung ihrer Daten auch wirklich zugestimmt haben:²⁵⁹

²⁵⁸ Datenschutz-Grundverordnung; Artikel 4 Absatz 11. Siehe auch Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 2.

²⁵⁹ Datenschutz-Grundverordnung, Artikel 7.

- Die Erteilung der Einwilligung erfolgt durch eine eindeutige bestätigende Handlung, mit der ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist. Bei diesem Akt kann es sich um eine Handlung oder um eine Erklärung handeln.
- Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.
- Im Rahmen einer schriftlichen Erklärung, die noch andere Sachverhalte wie beispielsweise die „Arbeitsbedingungen“ betrifft, muss das Ersuchen um Einwilligung in einer klaren und einfachen Sprache und in verständlicher und leicht zugänglicher Form erfolgen, die die Einwilligung von den anderen Sachverhalten klar unterscheidet; Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen die DSGVO darstellen.

Sind alle diese Anforderungen erfüllt, ist die Einwilligung im Rahmen des Datenschutzrechts gültig. Dem Verantwortlichen obliegt der Nachweis, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.²⁶⁰ Auf die Bestandteile einer gültigen Einwilligung wird in [Abschnitt 4.1.1](#) über die rechtmäßigen Gründe für die Verarbeitung personenbezogener Daten näher eingegangen.

Das Übereinkommen Nr. 108 enthält keine Definition der Einwilligung; diese bleibt dem innerstaatlichen Recht überlassen. Im **Recht des Europarates** entsprechen jedoch die Bestandteile einer gültigen Einwilligung den bereits dargestellten.²⁶¹

Weitere im Zivilrecht geregelte Anforderungen wie die Rechtsfähigkeit gelten natürlich auch im Zusammenhang mit dem Datenschutz, da es sich bei derartigen Anforderungen um grundlegende gesetzliche Voraussetzungen handelt. Ungültige Einwilligungen nicht geschäftsfähiger Personen haben zur Folge, dass es bei der Verarbeitung von Daten über solche Personen an einer Rechtsgrundlage mangelt. Was die Geschäftsfähigkeit Minderjähriger zum Abschluss von Verträgen betrifft, so sieht die DSGVO vor, dass ihre Vorschriften in Bezug auf das für den Erhalt einer gültigen Einwilligung erforderliche Mindestalter das allgemeine Vertragsrecht der Mitgliedstaaten unberührt lassen.²⁶²

²⁶⁰ a.a.O., Artikel 7 Absatz 1.

²⁶¹ Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 2; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absätze 42–45.

²⁶² Datenschutz-Grundverordnung, Artikel 8 Absatz 3.

Die Einwilligung muss auf eindeutige Weise erteilt werden, so dass kein Zweifel an den Absichten der betroffenen Person besteht.²⁶³ Die Verarbeitung sensibler Daten bedarf einer ausdrücklichen Einwilligung, die mündlich oder schriftlich erfolgen kann.²⁶⁴ Letztere kann auch elektronisch erfolgen.²⁶⁵ Sowohl **im EU-Recht** als auch **im Recht des Europarates** ist die Zustimmung zur Verarbeitung seiner personenbezogenen Daten in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung zu erteilen.²⁶⁶ Folglich kann die Einwilligung nicht aus Stillschweigen, bereits angekreuzten Kästchen, vorausgefüllten Formularen oder Untätigkeit abgeleitet werden.²⁶⁷

263 a.a.O., Artikel 6 Absatz 1 und Artikel 9 Absatz 2 Buchstabe a.

264 a.a.O., Erwägungsgrund 32.

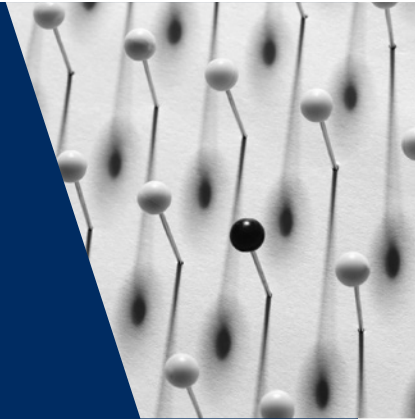
265 a.a.O.

266 a.a.O., Artikel 4 Absatz 11; Ad-hoc-Ausschuss Datenschutz (CAHDATA), Erläuternder Bericht zum Modernisierten Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108), Absatz 40.

267 Datenschutz-Grundverordnung, Erwägungsgrund 32; Ad-hoc-Ausschuss Datenschutz (CAHDATA), Erläuternder Bericht zum Modernisierten Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Absatz 40.

3

Kerngrundsätze des europäischen Datenschutzrechts



EU	Behandelte Themen	Europarat
DSGVO, Artikel 5 Absatz Buchstabe a	Grundsatz der Rechtmäßigkeit	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 3
DSGVO, Artikel 5 Absatz 1 Buchstabe a	Grundsatz der Verarbeitung nach Treu und Glauben	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe a EGMR, <i>K.H. und andere / Slowakei</i> , Nr. 32881/04, 2009
DSGVO, Artikel 5 Absatz 1 Buchstabe a EuGH, C-201/14, <i>Smaranda Bara und andere / Casa Națională de Asigurări de Sănătate und andere</i> , 2015	Grundsatz der Transparenz	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe a und Artikel 8 EGMR, <i>Haralambie / Rumänien</i> , Nr. 21737/03, 2009
DSGVO, Artikel 5 Absatz 1 Buchstabe b	Grundsatz der Zweckbindung	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe b
DSGVO, Artikel 5 Absatz 1 Buchstabe c EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, <i>Digital Rights Ireland und Kärntner Landesregierung und andere</i> [GK], 2014	Grundsatz der Datenminimierung	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe c

EU	Behandelte Themen	Europarat
DSGVO, Artikel 5 Absatz 1 Buchstabe d EuGH, C-553/07, <i>College van burgemeester en wethouders van Rotterdam / M. E. E. Rijkeboer</i> , 2009	Grundsatz der sachlichen Richtigkeit der Daten	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe d
DSGVO, Artikel 5 Absatz 1 Buchstabe e EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, <i>Digital Rights Ireland und Kärntner Landesregierung und andere</i> [GK], 2014	Grundsatz der Speicherbegrenzung	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe e EGMR, <i>S. und Marper / Vereinigtes Königreich</i> [GK], Nrn. 30562/04 und 30566/04, 2008
DSGVO, Artikel 5 Absatz 1 Buchstabe f und Artikel 32	Grundsatz der Datensicherheit (Integrität und Vertraulichkeit)	Modernisiertes Übereinkommen Nr. 108, Artikel 7
DSGVO, Artikel 5 Absatz 2	Grundsatz der Rechenschaftspflicht (Grundsatz der Verantwortlichkeit)	Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 1

Artikel 5 der DSGVO legt die Grundsätze für die Verarbeitung personenbezogener Daten dar. Diese Grundsätze umfassen:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz;
- Zweckbindung;
- Datenminimierung;
- Richtigkeit der Daten;
- Speicherbegrenzung;
- Integrität und Vertraulichkeit.

Die Grundsätze dienen als Ausgangspunkt für detailliertere Bestimmungen in den weiteren Artikeln der Verordnung. Sie erscheinen auch in den Artikeln 5, 7, 8 und 10 des Modernisierten Übereinkommens Nr. 108. Alle späteren Datenschutzvorschriften des Europarates oder der EU müssen mit diesen

Grundsätzen in Einklang stehen und sie müssen bei der Auslegung dieser Rechtsvorschriften berücksichtigt werden. Im EU-Recht sind Einschränkungen der Verarbeitungsgrundsätze lediglich erlaubt, sofern sie den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen und den Wesensgehalt der Grundrechte und Grundfreiheiten achten. Ausnahmen von diesen Kerngrundsätzen und Einschränkungen dieser Kerngrundsätze können auf nationaler Ebene vorgesehen werden;²⁶⁸ sie müssen gesetzlich vorgesehen sein, ein rechtmäßiges Ziel verfolgen und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen.²⁶⁹ Es müssen alle drei Bedingungen erfüllt sein.

3.1. Die Grundsätze der Rechtmäßigkeit der Verarbeitung, der Verarbeitung nach Treu und Glauben und der Transparenz der Verarbeitung

Kernpunkte

- Die Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben und der Transparenz finden auf jede Verarbeitung personenbezogener Daten Anwendung.
- Nach Maßgabe der DSGVO erfordert die Rechtmäßigkeit die Erfüllung einer der nachstehenden Bedingungen:
 - Einwilligung der betroffenen Person;
 - Notwendigkeit für die Erfüllung eines Vertrags;
 - eine rechtliche Verpflichtung;
 - Notwendigkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person;
 - Notwendigkeit für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt;

²⁶⁸ Modernisiertes Übereinkommen Nr. 108, Artikel 11 Absatz 1; DSGVO, Artikel 23 Absatz 1.

²⁶⁹ DSGVO, Artikel 23 Absatz 1.

- Notwendigkeit zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Rechte der betroffenen Person überwiegen.
- Die Verarbeitung personenbezogener Daten sollte nach Treu und Glauben erfolgen.
 - Die betroffene Person muss über das Risiko informiert sein, um sicherzustellen, dass die Verarbeitung keine unvorhersehbaren negativen Auswirkungen hat.
- Die Verarbeitung personenbezogener Daten sollte transparent erfolgen.
 - Die Verantwortlichen setzen die betroffenen Personen vor der Verarbeitung ihrer Daten unter anderem über den Zweck der Verarbeitung und den Namen und die Anschrift des Verantwortlichen in Kenntnis.
 - Die Informationen über die Verarbeitungsvorgänge sind in klarer und einfacher Sprache bereitzustellen, um den betroffenen Personen das leichte Verständnis der damit verbundenen Vorschriften, Risiken, Garantien und Rechte zu ermöglichen.
 - Die betroffenen Personen verfügen unabhängig vom Ort der Verarbeitung über ein Auskunftsrecht über ihre Daten.

3.1.1. Rechtmäßigkeit der Verarbeitung

Die Datenschutzgesetze der EU und des Europarates erfordern die rechtmäßige Verarbeitung personenbezogener Daten.²⁷⁰ Die rechtmäßige Verarbeitung erfordert die Einwilligung der betroffenen Person oder einen anderen in den Datenschutzvorschriften vorgesehenen berechtigten Grund.²⁷¹ Artikel 6 Absatz 1 DSGVO enthält neben der Einwilligung fünf weitere rechtmäßige Gründe für die Verarbeitung: wenn die Verarbeitung für die Erfüllung eines Vertrags, für die Wahrnehmung einer Aufgabe, die in Ausübung öffentlicher Gewalt erfolgt, zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten oder zum Schutz der lebenswichtigen Interessen der betroffenen Person erforderlich ist. Diese Thematik wird in [Abschnitt 4.1](#) näher erläutert.

270 Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 3; Datenschutz-Grundverordnung, Artikel 8 Absatz 1 Buchstabe a.

271 Charta der Grundrechte der Europäischen Union, Artikel 8 Absatz 2; Datenschutz-Grundverordnung, Erwägungsgrund 40 und Artikel 6–9; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 2; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 41.

3.1.2. Verarbeitung nach Treu und Glauben

Zusätzlich zur rechtmäßigen Verarbeitung erfordert das Datenschutzrecht der EU und des Europarates die Verarbeitung personenbezogener Daten nach Treu und Glauben.²⁷² Der Grundsatz der Verarbeitung nach Treu und Glauben regelt in erster Linie die Beziehung zwischen dem Verantwortlichen und der betroffenen Person.

Die Verantwortlichen sollten die betroffenen Personen und die breite Öffentlichkeit darüber in Kenntnis setzen, dass sie die Daten rechtmäßig und transparent verarbeiten, und müssen die Übereinstimmung der Verarbeitungsvorgänge mit der DSGVO nachweisen können. Verarbeitungsvorgänge dürfen nicht im Geheimen vorgenommen werden und die betroffenen Personen sollten sich der potenziellen Risiken bewusst sein. Soweit möglich sollten die Verantwortlichen ferner den Wünschen der betroffenen Person unverzüglich nachkommen, und dies insbesondere dann, wenn deren Einwilligung die Rechtsgrundlage der Datenverarbeitung bildet.

Beispiel: In der *Rechtssache K.H. und andere gegen Slowakei*²⁷³ waren die Beschwerdeführerinnen, acht Roma-Frauen, während ihrer Schwangerschaft und bei der Niederkunft in zwei Krankenhäusern im Osten der Slowakei behandelt worden. Danach konnte trotz wiederholter Versuche keine von ihnen mehr ein Kind empfangen. Die innerstaatlichen Gerichte wiesen die Krankenhäuser an, den Beschwerdeführerinnen und ihren Vertretern die Möglichkeit zur Einsicht in die Patientenakten und zur Anfertigung handschriftlicher Exzerpte zu geben, lehnten jedoch deren Antrag auf Anfertigung von Fotokopien mit dem Argument ab, es müsse ein Missbrauch der Unterlagen vermieden werden. Zu den positiven Verpflichtungen des Staates gemäß Artikel 8 EMRK gehört mit Sicherheit die Verpflichtung, der betroffenen Person Kopien ihrer Daten zur Verfügung zu stellen. Es war Sache des Staates, die Regelungen für das Kopieren personenbezogener Daten festzulegen oder gegebenenfalls darzulegen, aus welchen zwingenden Gründen er dies ablehnt. In der die Beschwerdeführerinnen betreffenden Sache begründeten die innerstaatlichen Gerichte das Verbot der Anfertigung von Fotokopien der Patientenakten grundsätzlich mit der Notwendigkeit,

²⁷² Datenschutz-Grundverordnung, Artikel 5 Absatz 1 Buchstabe a; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe a.

²⁷³ EGMR, *K.H. und andere / Slowakei*, Nr. 32881/04, 28. April 2009.

die einschlägigen Daten vor Missbrauch zu schützen. Der EGMR konnte jedoch nicht recht erkennen, wie die Beschwerdeführerinnen, denen ja auf jeden Fall Einsicht in ihre gesamten Patientenakten gewährt worden war, sie betreffende Informationen hätten missbrauchen können. Außerdem hätte das Risiko eines solchen Missbrauchs durch andere Mittel als die Verweigerung von Kopien der Akten der Beschwerdeführerinnen ausgeräumt werden können, beispielsweise durch eine Einschränkung des Personenkreises, der Zugang zu den Akten hat. Der Staat konnte keine zwingenden Gründe dafür anführen, dass den Beschwerdeführerinnen die effektive Einsicht in ihre Gesundheit betreffende Daten verweigert wurde. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 vorlag.

Im Zusammenhang mit Internetdiensten müssen Datenverarbeitungssysteme so gestaltet sein, dass betroffene Personen wirklich verstehen, was mit ihren Daten geschieht. In jedem Fall geht der Grundsatz der Verarbeitung nach Treu und Glauben über die Verpflichtungen zur Transparenz hinaus und könnte auch mit einer auf ethische Weise erfolgenden Verarbeitung personenbezogener Daten im Zusammenhang stehen.

Beispiel: Eine Forschungsabteilung einer Universität führt ein Experiment durch, in dessen Rahmen an 50 Probanden Stimmungsschwankungen untersucht werden. Hierfür müssen die Probanden ihre Gedanken stündlich zu einer festgesetzten Zeit in einer elektronischen Datei aufzeichnen. Die 50 Personen erteilten ihre Einwilligung zu diesem bestimmten Projekt und zu dieser spezifischen Verwendung der Daten seitens der Universität. Die Forschungsabteilung stellte bald fest, dass die elektronische Aufzeichnung von Gedanken für ein anderes Projekt sehr hilfreich wäre, das sich auf die psychische Gesundheit konzentrierte und unter Koordination eines anderen Teams durchgeführt wurde. Obgleich die Universität als Verantwortlicher angesichts der miteinander zu vereinbarenden Zwecke dieselben Daten ohne weitere Schritte zur Sicherstellung der Rechtmäßigkeit der Verarbeitung dieser Daten für die Arbeit eines anderen Teams verwenden hätte können, setzte sie die Probanden unter Einhaltung ihres Ethikkodex für die Forschung und des Grundsatzes der Verarbeitung nach Treu und Glauben darüber in Kenntnis und bat sie um deren erneute Einwilligung.

3.1.3. Transparenz der Verarbeitung

Das Datenschutzrecht der EU und des Europarates erfordern, dass die Verarbeitung personenbezogener Daten „in einer für die betroffene Person nachvollziehbaren Weise“ erfolgt.²⁷⁴

Dieser Grundsatz birgt die Verpflichtung für den Verantwortlichen, alle geeigneten Maßnahmen zu ergreifen, um die betroffenen Personen, bei denen es sich um Nutzer, Kunden oder Klienten handeln kann, über die Verwendung ihrer Daten auf dem Laufenden zu halten.²⁷⁵ Transparenz kann sich auf die Informationen beziehen, die der Person vor Beginn der Verarbeitung mitgeteilt werden,²⁷⁶ die Informationen, die den betroffenen Personen während der Verarbeitung einfach zugänglich sein sollten,²⁷⁷ aber auch auf die Informationen, die den betroffenen Personen im Anschluss an einen Antrag auf Auskunft über ihre Daten mitgeteilt werden.²⁷⁸

Beispiel: In der Rechtssache *Haralambie gegen Rumänien*²⁷⁹ wurde dem Beschwerdeführer erst fünf Jahre nach seinem Ersuchen Einsicht in die Informationen gewährt, die der Geheimdienst über ihn besaß. Der EGMR bekräftigte erneut, dass Personen, über die bei Behörden Akten geführt werden, ein lebenswichtiges Interesse daran haben, in diese Akten Einsicht nehmen zu können. Es sei Pflicht der Behörden, mit einem wirksamen Verfahren Auskunft über diese Daten zu ermöglichen. Der EGMR befand, dass weder die Menge übermittelter Akten noch Mängel im Archivierungssystem es rechtfertigten, dass dem Antrag des Beschwerdeführers auf Akteneinsicht erst nach fünf Jahren stattgegeben wurde. Die Behörden hätten dem Beschwerdeführer kein wirksames und leicht zugängliches Verfahren zur Verfügung gestellt, damit er innerhalb einer angemessenen Frist Einsicht in seine Akte nehmen konnte. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

²⁷⁴ Datenschutz-Grundverordnung, Artikel 5 Absatz 1 Buchstabe a; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe a und Artikel 8.

²⁷⁵ Datenschutz-Grundverordnung, Artikel 12.

²⁷⁶ a.a.O., Artikel 13 und 14.

²⁷⁷ Artikel-29-Datenschutzgruppe, *Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz*, S. 23.

²⁷⁸ Datenschutz-Grundverordnung, Artikel 15.

²⁷⁹ EGMR, *Haralambie / Rumänien*, Nr. 21737/03, 27. Oktober 2009.

Verarbeitungsvorgänge sind den betroffenen Personen auf leicht verständliche Weise zu erläutern, damit sie auch begreifen, was mit ihren Daten geschieht. Dies bedeutet, dass der bestimmte Zweck, zu dem die personenbezogenen Daten verarbeitet werden, der betroffenen Person zum Zeitpunkt der Erhebung der personenbezogenen Daten bekannt sein muss.²⁸⁰ Die Transparenz der Verarbeitung erfordert die Verwendung einer klaren und einfachen Sprache.²⁸¹ Die betroffenen Personen müssen sich über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten im Klaren sein.²⁸²

Auch **im Recht des Europarates** ist präzisiert, dass die seitens des Verantwortlichen proaktiv erfolgende Bereitstellung bestimmter grundlegender Informationen an die betroffenen Personen zwingend erforderlich ist. Informationen in Bezug auf den Namen und die Anschrift des Verantwortlichen (oder Mitverantwortlichen), die Rechtsgrundlage und die Zwecke der Datenverarbeitung, die Kategorien der verarbeiteten Daten und die Empfänger, sowie die Mittel zur Ausübung der Rechte können in jedem angemessenen Format (über eine Webseite, über technische Tools auf Privatgeräten, usw.) bereitgestellt werden, vorausgesetzt, die Informationen werden den betroffenen Personen nach Treu und Glauben und auf wirksame Weise erteilt. Die erteilten Informationen sollten leicht zugänglich, nachvollziehbar, verständlich und an die entsprechenden betroffenen Personen angepasst sein (beispielsweise bei Bedarf in kindgerechter Sprache). Auch alle zusätzlichen Informationen, die zur Gewährleistung einer Datenverarbeitung nach Treu und Glauben erforderlich oder zweckdienlich sind, wie die Aufbewahrungszeit, die Kenntnis der der Datenverarbeitung zugrunde liegenden Argumentation oder Informationen über Datenübermittlungen an Empfänger in einer anderen Vertragspartei oder Nicht-Vertragspartei (einschließlich darüber, ob die betreffende Nicht-Vertragspartei über ein angemessenes Schutzniveau verfügt oder über die vom Verantwortlichen zur Gewährleistung eines angemessenen Schutzniveaus der Daten ergriffenen Maßnahmen), sind bereitzustellen.²⁸³

280 Datenschutz-Grundverordnung, Erwägungsgrund 39.

281 a.a.O.

282 a.a.O.

283 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 68.

Nach Maßgabe des Auskunftsrechts²⁸⁴ hat eine betroffene Person das Recht, auf Anfrage von einem Verantwortlichen zu erfahren, ob ihre Daten verarbeitet werden und wenn ja, welche Daten einer solchen Verarbeitung unterliegen.²⁸⁵ Nach Maßgabe des Rechts auf Information²⁸⁶ sind die Personen, deren Daten verarbeitet werden, von den Verantwortlichen oder Auftragsverarbeitern grundsätzlich vor Beginn der Verarbeitungstätigkeit proaktiv unter anderem über die Zwecke, die Dauer und die Mittel der Verarbeitung zu informieren.

Beispiel: In der Rechtssache *Smaranda Bara und andere gegen Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Administrare Fiscală (ANAF)*²⁸⁷ ging es um die Übermittlung der Steuerdaten über die Einkünfte Selbstständiger von der Nationalen Agentur der Steuerverwaltung an den Nationalen Einheitsfonds der sozialen Krankenversicherungen in Rumänien, auf deren Grundlage die Zahlung rückständiger Krankenversicherungsbeiträge verlangt wurde. Der EuGH wurde gefragt, ob die Verarbeitung der Daten durch den Nationalen Einheitsfonds der sozialen Krankenversicherungen eine vorherige Unterrichtung der betroffenen Personen über die Identität des Verantwortlichen und den Zweck der Übermittlung dieser Daten erfordert hätte. Der EuGH befand, dass die Übermittlung personenbezogener Daten durch eine Verwaltungsbehörde eines Mitgliedstaats an eine andere Verwaltungsbehörde, die diese Daten weiterverarbeitet, die Unterrichtung der betroffenen Personen von der Übermittlung und der Verarbeitung erfordert.

In bestimmten Situationen sind Ausnahmen von der Pflicht zur Information der betroffenen Personen über die Datenverarbeitung erlaubt, auf die in [Abschnitt 6.1](#) über die Rechte der betroffenen Person genauer eingegangen wird.

²⁸⁴ Datenschutz-Grundverordnung, Artikel 15.

²⁸⁵ Modernisiertes Übereinkommen Nr. 108, Artikel 8 und Artikel 9 Absatz 1 Buchstabe b.

²⁸⁶ Datenschutz-Grundverordnung, Artikel 13 und 14.

²⁸⁷ EuGH, C-201/14, *Smaranda Bara und andere / Casa Națională de Asigurări de Sănătate und andere*, 1. Oktober 2015, Randnrn. 28–46.

3.2. Grundsatz der Zweckbindung

Kernpunkte

- Der Zweck der Datenverarbeitung muss vor dem Beginn der Verarbeitung festgelegt werden.
- Die Daten dürfen nicht in einer mit dem ursprünglichen Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden, obgleich die Datenschutz-Grundverordnung für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken Ausnahmen von dieser Bestimmung vorsieht.
- Im Wesentlichen bedeutet der Grundsatz der Zweckbindung, dass jede Verarbeitung personenbezogener Daten für einen bestimmten, genau festgelegten Zweck erfolgen muss und nur für zusätzliche, festgelegte Zwecke erfolgen darf, die mit dem ursprünglichen Zweck zu vereinbaren sind.

Der Grundsatz der Zweckbindung zählt zu den wesentlichen Grundsätzen des europäischen Datenschutzrechts. Er steht in engem Zusammenhang mit Transparenz, Vorhersagbarkeit und Nutzerkontrolle: wenn der Zweck der Verarbeitung hinreichend konkret und klar ist, wissen die Personen, was sie erwartet, was zu einer besseren Transparenz und Rechtssicherheit führt. Gleichzeitig ist die klare Abgrenzung des Zwecks wichtig, damit die betroffenen Personen ihre Rechte wie das Widerspruchsrecht gegen die Verarbeitung wirksam ausüben können.²⁸⁸

Der Grundsatz erfordert, dass jede Verarbeitung personenbezogener Daten für einen bestimmten, genau festgelegten Zweck erfolgen muss und nur für zusätzliche, festgelegte Zwecke erfolgen darf, die mit dem ursprünglichen Zweck zu vereinbaren sind.²⁸⁹ Die Verarbeitung personenbezogener Daten zu unbestimmten und/oder unbegrenzten Zwecken ist demnach rechtswidrig. Die Verarbeitung personenbezogener Daten ohne bestimmten Zweck und auf alleiniger Grundlage der Überlegung, dass diese Daten irgendwann in Zukunft nützlich sein könnten, ist ebenfalls rechtswidrig. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten hängt vom Zweck der Verarbeitung ab, der eindeutig, festgelegt und rechtmäßig sein muss.

²⁸⁸ Artikel-29-Datenschutzgruppe (2013), *Stellungnahme 3/2013 zur Zweckbindung*, WP 203, 2. April 2013.

²⁸⁹ DSGVO, Artikel 5 Absatz 1 Buchstabe b.

Für jeden neuen Zweck, zu dem Daten verarbeitet werden, der nicht mit dem ursprünglichen Zweck vereinbar ist, muss eine eigene Rechtsgrundlage vorliegen; er darf sich nicht darauf stützen, dass die Daten ursprünglich für einen anderen rechtmäßigen Zweck erhoben oder verarbeitet wurden. Eine rechtmäßige Verarbeitung wiederum ist auf den ursprünglich festgelegten Zweck beschränkt; ein neuer Verarbeitungszweck bedarf einer eigenen neuen Rechtsgrundlage. Die für einen neuen Zweck erfolgende Offenlegung personenbezogener Daten ist beispielsweise sorgfältig zu prüfen, da eine solche Offenlegung wahrscheinlich einer zusätzlichen Rechtsgrundlage bedarf, die eine andere als die für die Erhebung der Daten ist.

Beispiel: Eine Fluggesellschaft erhebt für eine reibungslose Abwicklung des Fluges bei der Buchung Daten ihrer Fluggäste. Sie benötigt Daten zu den Sitznummern der Fluggäste, zu besonderen körperlichen Einschränkungen wie Rollstuhlbedarf, und zu besonderen Wünschen an die Verpflegung wie koschere oder Halal-Speisen. Werden Fluggesellschaften nun aufgefordert, diese in den Fluggastdatensätzen enthaltenen Daten an die Einwanderungsbehörden am Bestimmungsflughafen zu übermitteln, werden diese Daten dort für Zwecke der Grenzkontrolle verwendet, also nicht für den Zweck, für den sie ursprünglich erhoben wurden. Für die Übermittlung dieser Daten an die Einwanderungsbehörde ist daher eine neue eigene Rechtsgrundlage erforderlich.

Bei der Prüfung des Geltungsbereichs und der Grenzen eines bestimmten Zwecks stützen sich das Modernisierte Übereinkommen Nr. 108 und die DSGVO auf das Konzept der Vereinbarkeit: Die Verwendung von Daten zu kompatiblen Zwecken darf auf der ursprünglichen Rechtsgrundlage geschehen. Die Weiterverarbeitung der Daten darf daher nicht in einer Weise erfolgen, die für die betreffende Person unerwartet, unangemessen oder unerwünscht ist.²⁹⁰ Zur Beurteilung, ob die Weiterverarbeitung als vereinbar zu betrachten ist, sollte der Verantwortliche (unter anderem) die nachstehenden Punkte berücksichtigen:

- „jede Verbindung zwischen diesen Zwecken und den Zwecken der beabsichtigten Weiterverarbeitung;

²⁹⁰ Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 49.

- den Zusammenhang, in dem die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten;
- die Art der personenbezogenen Daten;
- die Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen; und
- das Vorhandensein geeigneter Garantien sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang.²⁹¹ Dies könnte beispielsweise durch Verschlüsselung oder Pseudonymisierung erfolgen.

Beispiel: Das Unternehmen Sunshine erhebt im Rahmen des Kundenbeziehungsmanagements (CRM) Kundendaten. Danach übermittelt es diese Daten an das Direktmarketingunternehmen Moonlight, das diese Daten für Marketingkampagnen dritter Unternehmen verwenden möchte. Die seitens Sunshine für das Marketing anderer Unternehmen erfolgte Übermittlung der Daten stellt eine nachfolgende Verwendung der Daten für einen neuen Zweck dar, der mit Kundenbeziehungsmanagement, also dem Zweck, für den das Unternehmen Sunshine ursprünglich die Daten erhoben hat, nicht vereinbar ist. Für die Übermittlung der Daten an das Unternehmen Moonlight ist daher eine eigene Rechtsgrundlage erforderlich.

Verwendet hingegen das Unternehmen Sunshine die Kundenbeziehungsmanagementdaten für seine eigenen Marketingzwecke, also den Versand von Werbenachrichten für ihre eigenen Produkte an ihre eigenen Kunden, gilt dies im Allgemeinen als vereinbar Zweck.

In der Datenschutz-Grundverordnung und im Modernisierten Übereinkommen Nr. 108 heißt es, dass „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ *a priori* als mit dem

²⁹¹ Datenschutz-Grundverordnung, Erwägungsgrund 50 und Artikel 6 Absatz 4; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 49.

ursprünglichen Zweck vereinbar betrachtet wird.²⁹² Im Falle der Weiterverarbeitung personenbezogener Daten sind jedoch geeignete Garantien wie Anonymisierung, Verschlüsselung oder Pseudonymisierung der Daten oder eine Beschränkung des Zugangs zu den Daten einzurichten.²⁹³ Die DSGVO fügt hinzu: „Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten dürfen“.²⁹⁴ Im Falle einer Weiterverarbeitung sollte die betroffene Person daher über die Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet werden.²⁹⁵

Beispiel: Das Unternehmen Sunshine hat Kundenbeziehungsmanagementdaten (CRM-Daten) über seine Kunden erhoben und gespeichert. Eine Weiterverwendung dieser Daten durch das Unternehmen Sunshine für eine statistische Analyse des Kaufverhaltens seiner Kunden ist zulässig, da Statistiken zu den zu vereinbarenden Zwecken gehören. Es ist hierfür keine weitere Rechtsgrundlage wie z. B. die Einwilligung der betroffenen Personen erforderlich. Für die Weiterverarbeitung der personenbezogenen Daten für statistische Zwecke muss das Unternehmen Sunshine jedoch angemessene Garantien für die persönlichen Rechte und Freiheiten der betroffenen Personen ergreifen. Die von Sunshine zu treffenden technischen und organisatorischen Maßnahmen können die Pseudonymisierung umfassen.

292 DSGVO, Artikel 5 Absatz 1 Buchstabe b; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe b. Ein Beispiel für solche innerstaatlichen Bestimmungen ist das österreichische Datenschutzgesetz; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe b. Ein Beispiel für solche innerstaatlichen Bestimmungen ist das österreichische Datenschutzgesetz, Bundesgesetzblatt I Nr. 165/1999, Paragraph 46.

293 DSGVO, Artikel 6 Absatz 4; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe b; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 50.

294 DSGVO, Erwägungsgrund 50.

295 a.a.O.

3.3. Grundsatz der Datenminimierung

Kernpunkte

- Die Datenverarbeitung muss auf das für die Erfüllung eines rechtmäßigen Zwecks notwendige Maß beschränkt sein.
- Die Verarbeitung personenbezogener Daten sollte nur erfolgen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.
- Die Datenverarbeitung darf keinen unverhältnismäßigen Eingriff in die betreffenden Interessen, Rechte und Freiheiten darstellen.

Es dürfen nur Daten verarbeitet werden, die „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen“.²⁹⁶ Die für die Verarbeitung ausgewählten Datenkategorien müssen für das angegebene übergeordnete Ziel der Verarbeitung erforderlich sein, und ein Verantwortlicher sollte die Erhebung von Daten streng auf die Informationen beschränken, die für den mit der Verarbeitung verfolgten konkreten Zweck erheblich sind.

Beispiel: In der Rechtssache *Digital Rights Ireland*²⁹⁷ prüfte der EuGH die Gültigkeit der Richtlinie über die Vorratsspeicherung von Daten, die auf die Harmonisierung der nationalen Bestimmungen in Bezug auf die Vorratsspeicherung personenbezogener Daten abzielte, die mittels öffentlich zugänglicher elektronischer Kommunikationsdienste oder Netze für deren mögliche Übermittlung an die zuständigen Behörden zur Bekämpfung von schweren Straftaten wie organisierter Kriminalität und Terrorismus erzeugt oder verarbeitet wurden. Obwohl dies als Zweck betrachtet wurde, der eine Zielsetzung von allgemeinem Interesse erfüllte, wurde die Verallgemeinerung, mit der sich die Richtlinie auf „alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten [erstreckt], ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen“, als problematisch eingestuft.²⁹⁸

296 Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe c; Datenschutz-Grundverordnung, Artikel 5 Absatz 1 Buchstabe c.

297 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014.

298 a.a.O., Randnm. 44 und 57.

Durch den Einsatz von Technologien zur Verbesserung des Schutzes der Privatsphäre ist es darüber hinaus mitunter möglich, die Verwendung personenbezogener Daten ganz zu vermeiden oder Maßnahmen zur Verringerung der Fähigkeit der Zuordnung von Daten zu einer betroffenen Person einzusetzen (beispielsweise mittels Pseudonymisierung), eine Lösung, die dem Schutz der Privatsphäre entgegenkommt. Dies ist vor allem in umfassenden Verarbeitungssystemen angebracht.

Beispiel: Eine Gemeinde bietet regelmäßigen Benutzern der kommunalen Verkehrsbetriebe gegen eine gewisse Gebühr eine Chipkarte an. Der Name des Nutzers ist auf die Oberfläche der Karte aufgedruckt und außerdem elektronisch in dem Chip gespeichert. Beim Einsteigen in einen Bus oder eine Straßenbahn muss die Chipkarte vor das dort installierte Lesegerät gehalten werden. Die von dem Gerät gelesenen Daten werden elektronisch mit einer Datenbank abgeglichen, in der die Namen der Personen gespeichert sind, die die Fahrkarte gekauft haben.

Dieses System befolgt den Grundsatz der Datenminimierung nicht auf optimale Weise: Es ließe sich auch ohne Abgleich der auf dem Chip gespeicherten personenbezogenen Daten mit einer Datenbank überprüfen, ob eine Person befugt ist, das Verkehrsmittel zu benutzen. Es würde beispielsweise ausreichen, in dem Chip auf der Karte ein besonderes elektronisches Bild wie beispielsweise einen Strichcode zu speichern, der bei dem Vorbeiführen vor dem Lesegerät bestätigen könnte, ob die Karte gültig ist oder nicht. Ein solches System würde nicht erfassen, wer wann welches Verkehrsmittel benutzt hat. Dies wäre mit Blick auf den Grundsatz der Datenminimierung die optimale Lösung, denn dieser Grundsatz hebt darauf ab, möglichst wenige Daten zu erheben.

Artikel 5 Absatz 1 des Modernisierten Übereinkommens Nr. 108 enthält eine Verhältnismäßigkeitsanforderung für die Verarbeitung personenbezogener Daten in Bezug auf den verfolgten rechtmäßigen Zweck. In allen Phasen der Verarbeitung muss ein angemessenes Gleichgewicht zwischen allen betroffenen Interessen bestehen. Das bedeutet, dass „[p]ersonenbezogene Daten, die dem Zweck angemessen und erheblich sind, aber einen unverhältnismäßigen Eingriff in die betreffenden Grundrechte und Freiheiten zur Folge hätten, als übermäßig betrachtet werden sollten“.²⁹⁹

²⁹⁹ Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 52; Datenschutz-Grundverordnung, Artikel 5 Absatz 1 Buchstabe c.

3.4. Grundsatz der sachlichen Richtigkeit der Daten

Kernpunkte

- Der Verantwortliche wendet den Grundsatz der sachlichen Richtigkeit der Daten bei allen Verarbeitungstätigkeiten an.
- Unrichtige Daten müssen unverzüglich gelöscht oder berichtigt werden.
- Zur Sicherstellung der Richtigkeit müssen die Daten möglicherweise regelmäßig überprüft und auf dem neuesten Stand gehalten werden.

Ein Verantwortlicher, in dessen Besitz sich personenbezogene Daten befinden, darf diese Daten nicht verwenden, ohne mit hinreichender Gewissheit gewährleisten zu können, dass die Daten sachlich richtig und auf dem neuesten Stand sind.³⁰⁰

Die Verpflichtung zur Gewährleistung der sachlichen Richtigkeit von Daten ist im Zusammenhang mit dem Zweck der Datenverarbeitung zu sehen.

Beispiel: In der Rechtssache *Rijkeboer*³⁰¹ prüfte der EuGH den Antrag eines niederländischen Staatsbürgers auf den Erhalt von Informationen von der Gemeinde der Stadt Amsterdam über die Identität der Personen, denen die ihn betreffenden und von der Gemeinde aufbewahrten Daten in den beiden vorausgegangenen Jahren mitgeteilt wurden sowie über den Inhalt der weitergegebenen Daten. Der EuGH führte aus: Das „Recht auf Schutz der Privatsphäre setzt voraus, dass sich die betroffene Person vergewissern kann, dass ihre personenbezogenen Daten fehlerfrei verarbeitet werden und die Verarbeitung zulässig ist, d. h. insbesondere, dass die sie betreffenden Basisdaten richtig sind und dass sie an Empfänger gerichtet sind, die zu ihrer Verarbeitung befugt sind.“ Im Anschluss daran verwies der EuGH auf

300 Datenschutz-Grundverordnung, Artikel 5 Absatz 1 Buchstabe d; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe d.

301 EuGH, C-553/07, *College van burgemeester en wethouders van Rotterdam / M. E. E. Rijkeboer*, 7. Mai 2009.

die Präambel der Datenschutzrichtlinie, die besagt, dass die betroffenen Personen ein Auskunftsrecht hinsichtlich ihrer personenbezogenen Daten haben müssen, um nachprüfen zu können, ob die Daten richtig sind.³⁰²

Es kann vorkommen, dass die Aktualisierung gespeicherter Daten gesetzlich untersagt ist, weil der Zweck der Datenspeicherung im Wesentlichen in der Dokumentierung von Ereignissen als historische „Momentaufnahme“ besteht.

Beispiel: Ein Bericht über einen medizinischen Eingriff darf nicht abgeändert oder, in anderen Worten, auf den neuesten Stand gebracht werden, auch wenn sich in dem Bericht erwähnte Befunde im Nachhinein als falsch erweisen. In einem solchen Fall dürfen dem Bericht nur Bemerkungen hinzugefügt werden, die allerdings eindeutig als im Nachhinein gemachte Eintragungen gekennzeichnet werden müssen.

Andererseits gibt es aber auch Situationen, in denen eine regelmäßige Kontrolle der Richtigkeit von Daten einschließlich deren Aktualisierung unbedingt erforderlich ist, weil der betroffenen Person möglicherweise Schaden entstehen könnte, blieben die Daten unrichtig.

Beispiel: Vor dem Abschluss eines Vertrags zwischen einem Kunden und einem Geldinstitut überprüft die Bank üblicherweise die Kreditwürdigkeit des künftigen Kunden. Für diesen Zweck stehen spezielle Datenbanken mit Daten zur Kreditgeschichte von Privatpersonen zur Verfügung. Enthält eine solche Datenbank unrichtige oder überholte Daten zu einer natürlichen Person, kann dies für diese Person negative Auswirkungen haben. Die Verantwortlichen solcher Datenbanken müssen daher besondere Anstrengungen zur Wahrung des Grundsatzes der sachlichen Richtigkeit unternehmen.

302 Früherer Erwägungsgrund 41, Präambel der Richtlinie 95/46/EG.

3.5. Grundsatz der Speicherbegrenzung

Kernpunkt

- Der Grundsatz der Speicherbegrenzung besagt, dass personenbezogene Daten gelöscht oder anonymisiert werden müssen, sobald sie für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind.

Artikel 5 Absatz 1 Buchstabe e DSGVO sowie Artikel 5 Absatz 4 Buchstabe e des Modernisierten Übereinkommens Nr. 108 verlangen, dass personenbezogene Daten „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“. Sobald diese Zwecke erreicht sind, müssen die Daten daher gelöscht oder anonymisiert werden. Zu diesem Zweck „sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen“, um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden.³⁰³

In der Rechtssache *S. und Marper* befand der EGMR, dass die Kernprinzipien der einschlägigen Instrumente des Europarates sowie das Recht und die Praxis der anderen Vertragsparteien verlangen, dass die Datenspeicherung in einem angemessenen Verhältnis zum Zweck der Erhebung stehen und befristet sein muss, insbesondere im Polizeisektor.³⁰⁴

Beispiel: In der Rechtssache *S. und Marper*³⁰⁵ urteilte der EGMR, dass die unbegrenzte Speicherung der Fingerabdrücke, Zellproben und DNA-Profile in einer demokratischen Gesellschaft unverhältnismäßig und unnötig sei, in Anbetracht der Tatsache, dass die Strafverfolgung gegen beide Beschwerdeführer durch einen Freispruch bzw. einen Einstellungsbeschluss beendet worden war.

³⁰³ Datenschutz-Grundverordnung, Erwägungsgrund 39.

³⁰⁴ EGMR, *S. und Marper / Vereinigtes Königreich* [GK], Nrn. 30562/04 und 30566/04, 4. Dezember 2008; siehe ferner beispielsweise: EGMR, *M.M. / Vereinigtes Königreich*, Nr. 24029/07, 13. November 2012.

³⁰⁵ EGMR, *S. und Marper / Vereinigtes Königreich* [GK], Nrn. 30562/04 und 30566/04, 4. Dezember 2008.

Die Befristung der Speicherung personenbezogener Daten gilt nur für Daten, die in einer Form aufbewahrt werden, die eine Bestimmung betroffener Personen zulässt. Eine rechtmäßige Aufbewahrung nicht länger benötigter Daten könnte daher durch Anonymisierung der Daten erreicht werden.

Daten, die für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Zwecke oder für die statistische Verwendung gespeichert wurden, dürfen länger gespeichert werden, soweit diese Daten ausschließlich für die oben genannten Zwecke verwendet werden.³⁰⁶ Zum Schutz der Rechte und Freiheiten der betroffenen Person sind für die weitere Speicherung und Verwendung personenbezogener Daten geeignete technische und organisatorische Maßnahmen zu treffen.

Das Modernisierte Übereinkommen Nr. 108 erlaubt auch Ausnahmen vom Grundsatz der Speicherbegrenzung, vorausgesetzt, diese sind gesetzlich vorgesehen, achten den Wesensgehalt der Grundrechte und Grundfreiheiten und sind für das Erreichen einer begrenzten Anzahl an rechtmäßigen Zielen notwendig und verhältnismäßig.³⁰⁷ Diese beinhalten unter anderem den Schutz der nationalen Sicherheit, die Ermittlung und Verfolgung von Straftaten, die Strafvollstreckung, den Schutz der betroffenen Person und den Schutz der Rechte und Grundfreiheiten anderer Personen.

Beispiel: In der Rechtssache *Digital Rights Ireland*³⁰⁸ prüfte der EuGH die Gültigkeit der Richtlinie über die Vorratsspeicherung von Daten, die auf die Harmonisierung der nationalen Bestimmungen in Bezug auf die Vorratsspeicherung personenbezogener Daten abzielte, die mittels öffentlich zugänglicher elektronischer Kommunikationsdienste oder Netze für deren mögliche Übermittlung an die zuständigen Behörden zur Bekämpfung von schweren Straftaten wie organisierter Kriminalität und Terrorismus erzeugt oder verarbeitet wurden. Die Richtlinie über die Vorratsspeicherung von Daten setzte die Dauer der Vorratsspeicherung von Daten auf einen Zeitraum von „mindestens sechs Monaten [...] [fest], ohne dass eine Unterscheidung

306 Datenschutz-Grundverordnung, Artikel 5 Absatz 1 Buchstabe e; Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe b und Artikel 11 Absatz 2.

307 Modernisiertes Übereinkommen Nr. 108, Artikel 11.1; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absätze 91–98.

308 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014.

zwischen den in Artikel 5 der Richtlinie genannten Datenkategorien nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen getroffen wird".³⁰⁹ Der EuGH brachte auch das Problem zur Sprache, dass in der Richtlinie über die Vorratsspeicherung von Daten objektive Kriterien fehlen, auf deren Grundlage der genaue Zeitraum der Vorratsdatenspeicherung, der zwischen mindestens sechs Monaten und höchstens 24 Monaten variiert, zu bestimmen ist, um zu gewährleisten, dass dieser Zeitraum auf das absolut Notwendige beschränkt wird.³¹⁰

3.6. Grundsatz der Datensicherheit

Kernpunkte

- Die Sicherheit und Vertraulichkeit personenbezogener Daten sind zur Verhinderung nachteiliger Auswirkungen für die betroffene Person von entscheidender Bedeutung.
- Die Sicherheitsmaßnahmen können technischer und/oder organisatorischer Art sein.
- Pseudonymisierung ist ein Verfahren, durch das personenbezogene Daten geschützt werden können.
- Die Angemessenheit der Sicherheitsmaßnahmen ist für jeden Einzelfall festzusetzen und regelmäßig zu überprüfen.

Der Grundsatz der Datensicherheit erfordert das Treffen geeigneter technischer und organisatorischer Maßnahmen bei der Verarbeitung personenbezogener Daten, um die Daten vor unbeabsichtigtem, unbefugtem oder unrechtmäßigem Zugang oder Verlust und vor unbeabsichtigter, unbefugter oder unrechtmäßiger Verwendung, Änderung, Offenlegung, Zerstörung oder Schädigung zu schützen.³¹¹ Die DSGVO besagt, dass die Umsetzung dieser Maßnahmen seitens des Verantwortlichen und des Auftragsverarbeiters unter Berücksichtigung „des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit des Eintritts und Schwere des Risikos für die persönlichen Rechte

³⁰⁹ a.a.O., Randnr. 63.

³¹⁰ a.a.O., Randnr. 64.

³¹¹ Datenschutz-Grundverordnung, Erwägungsgrund 39 und Artikel 5 Absatz 1 Buchstabe f; Modernisiertes Übereinkommen Nr. 108, Artikel 7.

und Freiheiten natürlicher Personen“ erfolgen sollte.³¹² In Abhängigkeit von den spezifischen Umständen jedes Falls, könnten die angemessenen technischen und organisatorischen Maßnahmen beispielsweise die Pseudonymisierung und Verschlüsselung personenbezogener Daten und/oder die regelmäßige Überprüfung und Evaluierung der Wirksamkeit der Maßnahmen umfassen, um die Sicherheit der Datenverarbeitung zu gewährleisten.³¹³

Wie in [Abschnitt 2.1.1](#) beschrieben, werden bei der Pseudonymisierung von Daten die in personenbezogenen Daten enthaltenen Kennzeichen, die die Identifizierung der betroffenen Person ermöglichen, durch ein Pseudonym ersetzt und die Kennzeichen im Rahmen technischer oder organisatorischer Maßnahmen gesondert aufbewahrt. Das Verfahren zur Pseudonymisierung ist nicht mit dem Verfahren zur Anonymisierung zu verwechseln, bei dem sämtliche Verbindungen zur Identifizierung der Person entfernt werden.

Beispiel: Der Satz „Charles Spencer, geboren am 3. April 1967, ist Vater von vier Kindern, zwei Jungen und zwei Mädchen“ lässt sich beispielsweise folgendermaßen pseudonymisieren:

„C.S. 1967 ist Vater von vier Kindern, zwei Jungen und zwei Mädchen“; oder

„324 ist Vater von vier Kindern, zwei Jungen und zwei Mädchen“; oder

„YESz3201 ist Vater von vier Kindern, zwei Jungen und zwei Mädchen“.

Nutzer, die Zugriff auf diese pseudonymisierten Daten haben, dürften normalerweise nicht in der Lage sein, „Charles Spencer, geboren am 3. April 1967“ anhand von „324“ oder „YESz3201“ zu identifizieren. Solche Daten dürften daher eher vor Missbrauch geschützt sein.

Das erste Beispiel bietet allerdings weniger Sicherheit. Wird der Satz „C.S. 1967 ist Vater von vier Kindern, zwei Jungen und zwei Mädchen“ in dem kleinen Dorf verwendet, in dem Charles Spencer lebt, dürfte Herr Spencer leicht wiederzuerkennen sein. Die Methode der Pseudonymisierung kann die Wirksamkeit des Datenschutzes berühren.

³¹² Datenschutz-Grundverordnung, Artikel 32 Absatz 1.

³¹³ a.a.O.

Personenbezogene Daten mit verschlüsselten oder gesondert aufbewahrten Kennzeichen werden in vielen Situationen eingesetzt, um die Identität von Personen geheim zu halten. Dies ist vor allem sinnvoll, wenn Verantwortliche sichergehen müssen, dass sie es mit denselben betroffenen Personen zu tun haben, aber dazu nicht die echte Identität der betroffenen Personen kennen müssen oder sollten. Dies ist z. B. der Fall, wenn ein Forscher den Verlauf einer Krankheit mit Patienten untersucht, deren Identität nur dem behandelnden Krankenhaus bekannt ist, von dem er die pseudonymisierten Krankengeschichten erhält. Die Pseudonymisierung ist daher eine starke Waffe im Arsenal der Technologien zur Verbesserung des Schutzes der Privatsphäre. Sie kann auch bei der Umsetzung des Datenschutzes durch Technikgestaltung eine wichtige Rolle spielen. Darunter versteht man den Einbau des Datenschutzes in das Gewebe fortschrittlicher Datenverarbeitungssysteme.

Artikel 25 DSGVO, der sich mit dem Datenschutz durch Technikgestaltung befasst, verweist ausdrücklich auf die Pseudonymisierung als Beispiel für eine geeignete technische und organisatorische Maßnahme, die die Verantwortlichen treffen sollten, um den Grundsätzen des Datenschutzes Rechnung zu tragen und notwendige Garantien aufzunehmen. Dadurch erfüllen die Verantwortlichen die Anforderungen der Verordnung und schützen die Rechte der betroffenen Personen bei der Verarbeitung ihrer personenbezogenen Daten.

Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann sich beim Nachweis der Erfüllung der Anforderung der Verarbeitungssicherheit als hilfreich erweisen.³¹⁴ In seiner Stellungnahme zu den datenschutzrechtlichen Auswirkungen der Verarbeitung von Fluggastdatensätzen liefert der Europarat weitere Beispiele geeigneter Sicherheitsmaßnahmen für den Schutz personenbezogener Daten in Fluggastdatensystemen. Dies beinhaltet etwa die Aufbewahrung der Daten in einem physisch sicheren Umfeld, die Beschränkung der Zugangskontrolle über mehrschichtige Logins und den Schutz der Datenübertragung durch eine starke Verschlüsselung.³¹⁵

Beispiel: Social-Networking-Seiten und E-Mail-Provider bieten den Nutzern durch die Einführung der zweistufigen Authentifizierung zusätzlichen Datenschutz bei den von ihnen bereitgestellten Dienstleistungen. Zusätzlich

314 a.a.O., Artikel 32 Absatz 3.

315 Europarat, Ausschuss für das Übereinkommen Nr. 108, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19. August 2016, S. 9.

zur Eingabe eines persönlichen Passwortes müssen sich die Nutzer zum Aufrufen ihres persönlichen Kontos ein zweites Mal einloggen. Dieses zweite Einloggen könnte beispielsweise in der Eingabe eines Sicherheitscodes bestehen, der an die mit dem persönlichen Konto verbundene Mobilfunknummer gesendet wurde. Auf diese Weise bietet die zweistufige Überprüfung einen besseren Schutz der personenbezogenen Daten vor dem unbefugten Zugang zu persönlichen Konten mittels Hacking.

Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 liefert weitere Beispiele für geeignete Garantien, wie die Einführung einer Verpflichtung zur Wahrung des Berufsgeheimnisses oder die Annahme qualifizierter technischer Sicherheitsmaßnahmen wie der Datenverschlüsselung.³¹⁶ Bei der Einrichtung spezifischer Sicherheitsmaßnahmen sollte der Verantwortliche oder gegebenenfalls der Auftragsverarbeiter mehrere Faktoren wie die Art und Menge der verarbeiteten personenbezogenen Daten, potenzielle nachteilige Folgen für die betroffenen Personen und das Erfordernis eines eingeschränkten Datenzugangs berücksichtigen.³¹⁷ Bei der Einführung geeigneter Sicherheitsmaßnahmen ist der gegenwärtige Stand der Technik in Bezug auf Datensicherheitsmethoden und Datenverarbeitungstechniken zu berücksichtigen. Die Kosten für diese Maßnahmen müssen zur Ernsthaftigkeit und Wahrscheinlichkeit potenzieller Risiken im Verhältnis stehen. Die Sicherheitsmaßnahmen sind regelmäßig zu überprüfen, damit sie bei Bedarf aktualisiert werden können.³¹⁸

Im Falle einer Verletzung des Schutzes personenbezogener Daten verlangen sowohl das Modernisierte Übereinkommen Nr. 108 als auch die DSGVO vom Verantwortlichen, die Verletzung, die Risiken für die persönlichen Rechte und Freiheiten natürlicher Personen birgt, unverzüglich der zuständigen Aufsichtsbehörde zu melden.³¹⁹ Eine vergleichbare Verpflichtung zur Benachrichtigung der betroffenen Person liegt vor, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für ihre persönlichen Rechte und Freiheiten zur Folge hat.³²⁰ Die Benachrichtigung der betroffenen Personen über

316 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 56.

317 *a.a.O.*, Randnr. 62.

318 *a.a.O.*, Absatz 63.

319 Modernisiertes Übereinkommen Nr. 108, Artikel 7 Absatz 2; Datenschutz-Grundverordnung, Artikel 33 Absatz 1.

320 Modernisiertes Übereinkommen Nr. 108, Artikel 7 Absatz 2; Datenschutz-Grundverordnung, Artikel 34 Absatz 1.

derartige Verletzungen muss in klarer und einfacher Sprache erfolgen.³²¹ Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, ist der Verantwortliche unverzüglich darüber zu unterrichten.³²² In bestimmten Situationen können Ausnahmen von der Meldepflicht Anwendung finden. So ist der Verantwortliche beispielsweise nicht zur Benachrichtigung der Aufsichtsbehörde verpflichtet, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt“.³²³ Ebenso ist es nicht erforderlich, die betroffene Person zu benachrichtigen, wenn die getroffenen Sicherheitsvorkehrungen die Daten für unbefugte Personen unzugänglich machen oder wenn nachfolgende Maßnahmen sicherstellen, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht.³²⁴ Sofern die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen mit einem unverhältnismäßigen Aufwand verbunden wäre, kann eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme gewährleisten, dass „die betroffenen Personen vergleichbar wirksam informiert werden“.³²⁵

3.7. Grundsatz der Verantwortlichkeit (Rechenschaftspflicht)

Kernpunkte

- Der Grundsatz der Verantwortlichkeit verlangt von Verantwortlichen und Auftragsverarbeitern, die aktive und kontinuierliche Durchführung von Maßnahmen zur Förderung und Gewährleistung des Datenschutzes bei ihrer Verarbeitungstätigkeit.
- Verantwortliche und Auftragsverarbeiter tragen dafür Verantwortung, dass ihre Verarbeitungsvorgänge im Einklang mit dem Datenschutzrecht und ihren jeweiligen Verpflichtungen stehen.

³²¹ Datenschutz-Grundverordnung, Artikel 34 Absatz 2.

³²² a.a.O., Artikel 33 Absatz 2.

³²³ a.a.O., Artikel 33 Absatz 1.

³²⁴ a.a.O., Artikel 34 Absatz 3 Buchstaben a und b.

³²⁵ a.a.O., Artikel 34 Absatz 3 Buchstabe c.

- Verantwortliche müssen jederzeit gegenüber betroffenen Personen, der breiten Öffentlichkeit und den Datenschutzbehörden nachweisen können, dass sie die Datenschutzvorschriften einhalten. Auch Auftragsverarbeiter müssen einige ausdrücklich mit der Rechenschaftspflicht verbundene Verpflichtungen einhalten (wie das Führen eines Verzeichnisses der Verarbeitungstätigkeiten und die Benennung eines Datenschutzbeauftragten).

In der DSGVO und im Modernisierten Übereinkommen Nr. 108 ist festgelegt, dass der Verantwortliche für die Einhaltung der im vorliegenden Kapitel beschriebenen Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten verantwortlich ist und deren Einhaltung nachweisen können muss.³²⁶ Hierfür setzt der Verantwortliche geeignete technische und organisatorische Maßnahmen um.³²⁷ Obgleich sich der in Artikel 5 Absatz 2 DSGVO verankerte Grundsatz der Verantwortlichkeit nur an Verantwortliche richtet, wird auch von Auftragsverarbeitern eine Rechenschaftspflicht erwartet, da sie mehrere Verpflichtungen einhalten müssen, die eng mit der Rechenschaftspflicht verknüpft sind.

Auch das Datenschutzrecht der EU und des Europarates setzen fest, dass der Verantwortliche für die Einhaltung der in den [Abschnitten 3.1 bis 3.6](#) erörterten Datenschutzgrundsätze verantwortlich ist und deren Einhaltung gewährleisten muss.³²⁸ Die Artikel-29-Datenschutzgruppe hebt hervor, dass „sich die Art dieser Verfahren und Mechanismen nach den durch die Verarbeitung und die Art der Daten erwachsenden Risiken richten [würde]“.³²⁹

Verantwortliche können sich die Erfüllung dieses Erfordernisses auf verschiedene Arten erleichtern. Dazu zählen beispielsweise:

- die Aufzeichnung der Verarbeitungstätigkeiten und deren auf Anfrage erfolgende Bereitstellung an die Aufsichtsbehörde;³³⁰
- die in bestimmten Situationen erfolgende Benennung eines Datenschutzbeauftragten, der in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird;³³¹

326 a.a.O., Artikel 5 Absatz 2; Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 1.

327 Datenschutz-Grundverordnung, Artikel 24.

328 a.a.O., Artikel 5 Absatz 2; Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 1.

329 Artikel-29-Datenschutzgruppe, *Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht*, WP 173, Brüssel, 13. Juli 2010, Absatz 12.

330 Datenschutz-Grundverordnung, Artikel 30.

331 a.a.O., Artikel 37–39.

- die Durchführung einer Datenschutz-Folgenabschätzung für Formen der Verarbeitung, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge haben;³³²
- die Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen;³³³
- die Einrichtung von Modalitäten und Verfahren für die Ausübung der Rechte der betroffenen Personen;³³⁴
- die Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren.³³⁵

Während sich der in Artikel 5 Absatz 2 DSGVO verankerte Grundsatz der Verantwortlichkeit nicht ausdrücklich an Auftragsverarbeiter richtet, gibt es Bestimmungen im Zusammenhang mit der Rechenschaftspflicht, die auch Verpflichtungen für Auftragsverarbeiter enthalten, wie beispielsweise das Führen eines Verzeichnisses der Verarbeitungstätigkeiten und die Benennung eines Datenschutzbeauftragten sofern die Verarbeitungstätigkeiten dies erfordern.³³⁶ Darüber hinaus müssen die Auftragsverarbeiter sicherstellen, dass alle für die Gewährleistung der Sicherheit der Daten erforderlichen Maßnahmen getroffen wurden.³³⁷ Der rechtlich bindende Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter sieht vor, dass der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung einiger Erfordernisse unterstützt, wie bei der Durchführung einer Datenschutz-Folgenabschätzung oder der Benachrichtigung des Verantwortlichen über Verletzungen des Schutzes personenbezogener Daten wenn ihm solche bekannt werden.³³⁸

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat 2013 Leitlinien zum Schutz der Privatsphäre angenommen, in denen die wichtige Rolle von Verantwortlichen bei der Datenschutzarbeit in der Praxis

332 a.a.O., Artikel 35; Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 2.

333 Datenschutz-Grundverordnung, Artikel 25, Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 2 und 3.

334 a.a.O., Artikel 12 und Artikel 24.

335 a.a.O., Artikel 40 und Artikel 42.

336 a.a.O., Artikel 5 Absatz 2, Artikel 30 und Artikel 37.

337 a.a.O., Artikel 28 Absatz 3 Buchstabe c.

338 a.a.O., Artikel 28 Absatz 3 Buchstabe d.

unterstrichen wird. In diesen Leitlinien wird ein Grundsatz der Verantwortlichkeit entwickelt, der besagt, dass „ein für die Verarbeitung Verantwortlicher darüber Rechenschaft ablegen sollte, dass er Maßnahmen ergriffen hat, mit denen er die oben genannten [materiellen] Prinzipien umsetzt.“³³⁹

Beispiel: Ein Beispiel für einen Rechtstext, in dem der Grundsatz der Verantwortlichkeit hervorgehoben wird, ist die Änderung³⁴⁰ der ePrivacy-Richtlinie 2002/58/EG aus dem Jahr 2009. Gemäß Artikel 4 in der geänderten Fassung sieht die Richtlinie die Verpflichtung zur „Sicherstellung der Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten“ vor. Im Hinblick auf die Sicherheitsbestimmungen in dieser Richtlinie beschloss der Gesetzgeber also, explizit das Erfordernis der Ausarbeitung und Umsetzung eines Sicherheitskonzepts vorzusehen.

Gemäß der Stellungnahme der Artikel-29-Datenschutzgruppe³⁴¹ liegt das Wesen des Grundsatzes der Verantwortlichkeit in der Verpflichtung des für die Verarbeitung Verantwortlichen,

- Maßnahmen vorzusehen, die unter normalen Umständen garantieren, dass bei den Verarbeitungen die Datenschutzvorschriften eingehalten werden, und
- Unterlagen vorlegen zu können, denen betroffene Personen und Datenschutzbehörden entnehmen können, welche Maßnahmen ergriffen wurden, um den Datenschutzvorschriften Genüge zu tun.

Der Grundsatz der Verantwortlichkeit verlangt also von den Verantwortlichen, aktiv die Einhaltung der Vorschriften zu belegen und nicht darauf zu warten, dass betroffene Personen oder Datenschutzbehörden Defizite aufdecken.

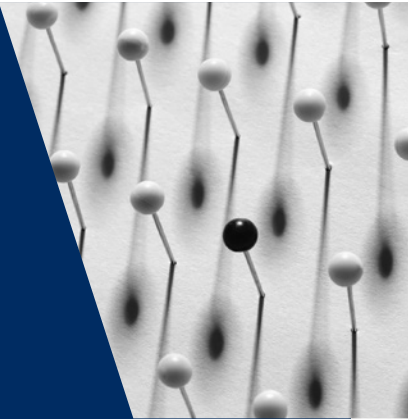
339 OECD (2013), Leitlinien für den Schutz der Privatsphäre und die grenzüberschreitende Übermittlung personenbezogener Daten, Artikel 14.

340 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. L 337 vom 18.12.2009, S. 11.

341 Artikel-29-Datenschutzgruppe, *Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht*, WP 173, Brüssel, 13. Juli 2010.

4

Vorschriften des europäischen Datenschutzrechts



EU	Behandelte Themen	Europarat
Vorschriften über die rechtmäßige Verarbeitung von Daten		
DSGVO, Artikel 6 Absatz 1 Buchstabe a EuGH, C-543/09, <i>Deutsche Telekom AG / Bundesrepublik Deutschland</i> , 2011 EuGH, C-536/15, <i>Tele2 (Netherlands) BV und andere / Autoriteit Consument en Markt (AMC)</i> , 2017	Einwilligung	Profiling-Empfehlung, Artikel 3.4 Buchstabe b und Artikel 3.6 Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 2
DSGVO, Artikel 6 Absatz 1 Buchstabe b	(Vor-)Vertragliche Beziehung	Profiling-Empfehlung, Artikel 3.4 Buchstabe b
DSGVO, Artikel 6 Absatz 1 Buchstabe c	Rechtliche Verpflichtungen des Verantwortlichen	Profiling-Empfehlung, Artikel 3.4 Buchstabe a
DSGVO, Artikel 6 Absatz 1 Buchstabe d	Lebenswichtige Interessen der betroffenen Person	Profiling-Empfehlung, Artikel 3.4 Buchstabe b
DSGVO, Artikel 6 Absatz 1 Buchstabe e EuGH, C-524/06, <i>Huber / Bundesrepublik Deutschland [GK]</i> , 2008	Öffentliches Interesse und Ausübung öffentlicher Gewalt	Profiling-Empfehlung, Artikel 3.4 Buchstabe b

EU	Behandelte Themen	Europarat
DSGVO, Artikel 6 Absatz 1 Buchstabe f EuGH, C-13/16, <i>Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde / Rīgas pašvaldības SIA 'Rīgas satiksme'</i> , 2017 EuGH, Verbundene Rechtssachen C-468/10 und C-469/10, <i>Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECMD) / Administración del Estado</i> , 2011	Berechtigte Interessen anderer	Profiling-Empfehlung, Artikel 3.4 Buchstabe b EGMR, Y / <i>Türkei</i> , Nr. 648/10, 2015
DSGVO, Artikel 6 Absatz 4	Ausnahme von der Zweckbindung: Weiterverarbeitung für andere Zwecke	Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe b
Vorschriften über die rechtmäßige Verarbeitung sensibler Daten		
DSGVO, Artikel 9 Absatz 1	Allgemeines Verarbeitungsverbot	Modernisiertes Übereinkommen Nr. 108, Artikel 6
DSGVO, Artikel 9 Absatz 2	Ausnahmen vom allgemeinen Verarbeitungsverbot	Modernisiertes Übereinkommen Nr. 108, Artikel 6
Vorschriften über die Sicherheit der Verarbeitung		
DSGVO, Artikel 32	Verpflichtung zur Gewährleistung einer sicheren Verarbeitung	Modernisiertes Übereinkommen Nr. 108, Artikel 7 Absatz 1 EGMR, I / <i>Finnland</i> , Nr. 20511/03, 2008
DSGVO, Artikel 28 und Artikel 32 Absatz 1 Buchstabe b	Verpflichtung zur Vertraulichkeit	Modernisiertes Übereinkommen Nr. 108, Artikel 7 Absatz 1
DSGVO, Artikel 34 Datenschutzrichtlinie für elektronische Kommunikation, Artikel 4 Absatz 2	Meldungen von Verletzungen des Schutzes personenbezogener Daten	Modernisiertes Übereinkommen Nr. 108, Artikel 7 Absatz 2

EU	Behandelte Themen	Europarat
Vorschriften über die Rechenschaftspflicht und die Förderung der Einhaltung der Vorschriften		
DSGVO, Artikel 12, 13 und 14	Transparenz im Allgemeinen	Modernisiertes Übereinkommen Nr. 108, Artikel 8
DSGVO, Artikel 37, 38 und 39	Datenschutzbeauftragte	Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 1
DSGVO, Artikel 30	Verzeichnis von Verarbeitungstätigkeiten	
DSGVO, Artikel 35 und 36	Folgenabschätzung und vorherige Konsultation	Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 2
DSGVO, Artikel 33 und 34	Meldungen von Verletzungen des Schutzes personenbezogener Daten	Modernisiertes Übereinkommen Nr. 108, Artikel 7 Absatz 2
DSGVO, Artikel 40 und 41	Verhaltensregeln	
DSGVO, Artikel 42 und 43	Zertifizierung	
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen		
DSGVO, Artikel 25 Absatz 1 Buchstabe a	Datenschutz durch Technikgestaltung	Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 2
DSGVO, Artikel 25 Absatz 1 Buchstabe b	Datenschutz durch datenschutzfreundliche Voreinstellungen	Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 3

Grundsätze sind zwangsläufig allgemeiner Art. Ihre Anwendung auf konkrete Situationen lässt einen gewissen Spielraum für die Interpretation und die Wahl der Mittel. Nach dem **Recht des Europarates** ist es Sache der Vertragsparteien des Modernisierten Übereinkommens Nr. 108, in ihrem innerstaatlichen Recht diesen Interpretationsspielraum festzulegen. Im **EU-Recht** stellt sich die Lage anders dar: Im Hinblick auf die Einführung des Datenschutzes im Binnenmarkt wurden detailliertere Vorschriften auf EU-Ebene für erforderlich gehalten, um das Datenschutzniveau in den nationalen Rechtsvorschriften der Mitgliedstaaten zu harmonisieren. Die DSGVO enthält gemäß den Grundsätzen

in Artikel 5 ein detailliertes Regelwerk, das in der innerstaatlichen Rechtsordnung unmittelbar Anwendung findet. Die nachstehenden Ausführungen zu einzelnen Datenschutzvorschriften auf europäischer Ebene beziehen sich daher überwiegend auf das EU-Recht.

4.1. Vorschriften über die Rechtmäßigkeit der Verarbeitung

Kernpunkte

- Personenbezogene Daten dürfen rechtmäßig verarbeitet werden, wenn eines der nachstehenden Kriterien erfüllt ist:
 - die Verarbeitung beruht auf der Einwilligung der betroffenen Person;
 - die Verarbeitung personenbezogener Daten ist aufgrund einer Vertragsbeziehung erforderlich;
 - die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, welcher der Verantwortliche unterliegt;
 - lebenswichtige Interessen betroffener oder anderer Personen erfordern die Verarbeitung ihrer Daten;
 - die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt;
 - berechnete Interessen der Verantwortlichen oder Dritter sind der Grund für die Verarbeitung, jedoch nur so lange, wie die Interessen oder Grundrechte der betroffenen Personen diese nicht überwiegen.
- Die Verarbeitung sensibler personenbezogener Daten unterliegt besonderen, strengeren Regeln.

4.1.1. Rechtmäßige Gründe für die Datenverarbeitung

Kapitel II der DSGVO mit dem Titel „Grundsätze“ sieht vor, dass jede Verarbeitung personenbezogener Daten zunächst mit den in Artikel 5 DSGVO dargelegten Grundsätzen übereinstimmen muss. Einer dieser Grundsätze besteht darin, dass personenbezogene Daten „auf rechtmäßige Weise, nach Treu und Glauben und in einer [...] nachvollziehbaren Weise verarbeitet“ werden sollten. Zur rechtmäßigen Datenverarbeitung muss die Verarbeitung

zweitens mit einem der rechtmäßigen Gründe für die Zulässigkeit der Datenverarbeitung übereinstimmen, die in Bezug auf nicht sensible personenbezogene Daten in Artikel 6³⁴² und in Bezug auf besondere Datenkategorien (oder „sensible Daten“) in Artikel 9 dargelegt sind. Ebenso setzt Kapitel II des Modernisierten Übereinkommens Nr. 108, das die „Grundsätze für den Schutz personenbezogener Daten“ darlegt, Nachstehendes fest: um rechtmäßig zu sein, muss die Datenverarbeitung „zu dem verfolgten rechtmäßigen Zweck im Verhältnis stehen“.

Abgesehen vom rechtmäßigen Grund für die Verarbeitung, auf den sich ein Verantwortlicher für den Beginn einer Verarbeitung personenbezogener Daten beruft, muss der Verantwortliche auch die im allgemeinen Datenschutzrecht vorgesehenen Garantien anwenden.

Einwilligung

Im Recht des Europarates befasst sich Artikel 5 Absatz 2 des Modernisierten Übereinkommens Nr. 108 mit der Einwilligung. Auch in der Rechtsprechung des EGMR und in mehreren Empfehlungen des Europarates wird darauf verwiesen.³⁴³ **Im EU-Recht** ist die Einwilligung als Grundlage für eine rechtmäßige Datenverarbeitung in Artikel 6 DSGVO fest verankert und auch in Artikel 8 der Charta ausdrücklich angeführt. Die Merkmale einer gültigen Einwilligung sind in der Definition des Begriffs „Einwilligung“ in Artikel 4 erläutert, während die Bedingungen für den Erhalt einer gültigen Einwilligung in Artikel 7 und die Sondervorschriften für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft in Artikel 8 der DSGVO dargelegt sind.

Wie bereits in [Abschnitt 2.4](#) erläutert, muss die Einwilligung ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich erteilt werden. Die Einwilligung muss in Form einer Erklärung oder einer sonstigen

342 EuGH, Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Rechnungshof / Österreichischer Rundfunk und andere und Christa Neukomm und Joseph Lauermann / Österreichischer Rundfunk*, 20. Mai 2003, Randnr. 65; EuGH, C-524/06, *Heinz Huber / Bundesrepublik Deutschland* [GK], 16. Dezember 2008, Randnr. 48; EuGH, Verbundene Rechtssachen C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24. November 2011, Randnr. 26.

343 Siehe beispielsweise Europarat, Ministerkomitee (2010), Empfehlung CM/Rec(2010)13 des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling, 23. November 2010, Artikel 3.4 Buchstabe b.

eindeutigen bestätigenden Handlung erfolgen, die das Einverständnis mit der Verarbeitung bedeutet, und die Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Die Verantwortlichen müssen im Besitz eines überprüfbareren Nachweises über die Einwilligung sein.

Einwilligung ohne Zwang

Im Rahmen des Modernisierten Übereinkommens Nr. 108 des **Europarates** muss die Einwilligung der betroffenen Person „die freie Äußerung einer bewussten Wahl darstellen“. ³⁴⁴ Eine freiwillige Einwilligung liegt nur dann vor, „wenn die betroffene Person eine tatsächliche Wahlmöglichkeit hat und kein Risiko einer Täuschung, Einschüchterung, Nötigung oder beträchtlicher negativer Folgen besteht, wenn sie die Einwilligung nicht erteilt“. ³⁴⁵ Diesbezüglich setzt das **EU-Recht** fest, dass nur dann davon ausgegangen werden kann, dass die betroffene Person ihre Einwilligung freiwillig gegeben hat, „wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“. ³⁴⁶ Die DSGVO hebt hervor: „Bei der Beurteilung, ob die Einwilligung ohne Zwang erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind“. ³⁴⁷ Im erläuternden Bericht zum Modernisierten Übereinkommen Nr. 108 heißt es: „Auf die betroffene Person darf kein unzulässiger Einfluss oder Druck (sei es wirtschaftlicher oder anderer Art) ausgeübt werden und es kann nur dann davon ausgegangen werden, dass die Einwilligung ohne Zwang gegeben wurde, wenn die betroffene Person eine echte Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“. ³⁴⁸

344 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 42.

345 Siehe auch Artikel-29-Datenschutzgruppe (2011), *Stellungnahme 15/2011 zur Definition von Einwilligung*, WP 187, Brüssel, 13. Juli 2011, S. 12.

346 Datenschutz-Grundverordnung, Erwägungsgrund 42.

347 a.a.O., Artikel 7 Absatz 4.

348 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 42.

Beispiel: Einige Gemeinden im Staat A beschlossen die Erstellung von Aufenthaltskarten mit integriertem Chip. Für die Bewohner ist der Erwerb dieser elektronischen Karten nicht verpflichtend. Bewohner, die sich nicht im Besitz dieser Karte befinden, haben jedoch keinen Zugang zu einer Reihe von wichtigen Verwaltungsdiensten wie der Möglichkeit zur Online-Entrichtung der Gemeindesteuern, zur elektronischen Einreichung von Beschwerden mit einer Antwortgarantie der Behörde innerhalb einer Frist von drei Tagen und sogar zur Umgehung von Warteschlangen und zum Erwerb ermäßigter Eintrittskarten beim Besuch des Konzertsals der Gemeinde und der Nutzung der Scanner im Eingangsbereich.

In diesem Beispiel kann die seitens der Gemeinden erfolgende Verarbeitung personenbezogener Daten nicht auf Einwilligung gründen. Da die Bewohner zumindest einem indirekten Druck in Bezug auf den Erwerb der elektronischen Karte und die Zustimmung zur Verarbeitung ausgesetzt sind, wird die Einwilligung nicht ohne Zwang erteilt. Die seitens der Gemeinden erfolgende Entwicklung eines elektronischen Kartensystems sollte sich folglich auf einen anderen rechtmäßigen Grund zur Rechtfertigung der Verarbeitung stützen. Sie könnten sich beispielsweise darauf berufen, dass die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt, was gemäß Artikel 6 Absatz 1 Buchstabe e DSGVO eine rechtmäßige Grundlage für die Verarbeitung darstellt.³⁴⁹

Die Freiwilligkeit der Einwilligung könnte auch dann angezweifelt werden, wenn ein erhebliches wirtschaftliches oder sonstiges Ungleichgewicht zwischen dem für die Verarbeitung Verantwortlichen, der die Einwilligung sucht, und der betroffenen Person, die die Einwilligung gibt, besteht.³⁵⁰ Ein typisches Beispiel für solche Ungleichgewichte und Unterordnungen ist die Verarbeitung personenbezogener Daten eines Arbeitnehmers im Rahmen eines Arbeitsverhältnisses. Nach Ansicht der Artikel-29-Datenschutzgruppe befinden

349 Artikel-29-Datenschutzgruppe, *Stellungnahme 15/2011 zur Definition von Einwilligung*, WP 187, Brüssel, 13. Juli 2011, S. 16. Weitere Beispiele von Fällen, in denen die Datenverarbeitung nicht auf einer Einwilligung gründen kann, sondern für ihre Rechtmäßigkeit einer anderen Rechtsgrundlage bedarf, sind auf den Seiten 14 und 17 der Stellungnahme zu finden.

350 Siehe auch Artikel-29-Datenschutzgruppe (2001), *Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten*, WP 48, Brüssel, 13. September 2001; Artikel-29-Datenschutzgruppe (2005), Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114, Brüssel, 25. November 2005; Artikel-29-Datenschutzgruppe (2017), *Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz*, WP 249, Brüssel, 8. Juni 2017.

sich „Beschäftigte [...] angesichts der Abhängigkeit von ihren Arbeitgebern praktisch nie in einer Lage, in der sie ihre Einwilligung ohne Zwang erteilen, verweigern oder widerrufen könnten. Angesichts der ungleichen Machtverhältnisse ist festzustellen, dass Beschäftigte eine Einwilligung ohne Zwang nur in den Ausnahmefällen treffen können, in denen mit der Annahme oder Ablehnung eines Angebots keine Folgen verbunden sind.“³⁵¹

Beispiel: Ein großes Unternehmen plant die Erstellung eines Verzeichnisses mit den Namen aller Beschäftigten, ihrer Funktion im Unternehmen und ihrer Büroadresse mit dem alleinigen Ziel, die unternehmensinterne Kommunikation zu verbessern. Der Leiter der Personalabteilung schlägt vor, in das Verzeichnis Fotos aller Beschäftigten aufzunehmen, um das Erkennen von Kollegen bei Sitzungen zu erleichtern. Die Arbeitnehmervertreter fordern, dass dies nur geschehen darf, wenn der betreffende Beschäftigte eingewilligt hat.

In einer solchen Situation sollte die Einwilligung des Beschäftigten als Rechtsgrundlage für die Verarbeitung der Fotos im Verzeichnis angesehen werden, da es glaubhaft ist, dass es für den Beschäftigten keine Folgen haben wird, ob er sich mit der Veröffentlichung seines Fotos im Verzeichnis einverstanden erklärt oder nicht.

Beispiel: Firma A plant ein Treffen zwischen drei ihrer Beschäftigten und den Geschäftsführern von Firma B zur Besprechung einer potenziellen künftigen Zusammenarbeit im Rahmen eines Projekts. Das Treffen wird in den Räumlichkeiten von Firma B stattfinden, die Firma A dazu auffordert, ihr die Namen, Lebensläufe und Fotos der Teilnehmer des Treffens per E-Mail zu übermitteln. Firma B argumentiert, dass sie die Namen und Fotos der Teilnehmer benötigt, damit das Sicherheitspersonal am Gebäudeeingang überprüfen kann, dass es sich um die richtigen Personen handelt, während die Lebensläufe den Geschäftsführern zur besseren Vorbereitung auf das Treffen dienen. In diesem Fall kann die seitens Firma A erfolgende Übermittlung der personenbezogenen Daten ihrer Beschäftigten nicht auf Einwilligung gründen. Es kann nicht davon ausgegangen werden, dass die Einwilligung ohne Zwang gegeben wurde, da es sein kann, dass die Ablehnung des Vorschlags für die Beschäftigten negative Folgen hat (sie

351 Artikel-29-Datenschutzgruppe, *Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz*, WP 249, Brüssel, 8. Juni 2017.

könnten beispielsweise nicht nur in Bezug auf die Teilnahme am Treffen sondern auch in Bezug auf die Zusammenarbeit mit Firma B und die Mitwirkung am Projekt im Allgemeinen durch einen anderen Kollegen ersetzt werden. Demnach muss die Verarbeitung auf einem anderen rechtmäßigen Verarbeitungsgrund beruhen.

Das bedeutet allerdings nicht, dass eine Einwilligung niemals gültig sein kann, wenn die Verweigerung der Einwilligung negative Folgen haben könnte. Hat beispielsweise eine verweigerte Einwilligung, Inhaber der Kundenkarte eines Supermarktes zu werden, nur zur Folge, dass man bei bestimmten Waren keine kleine Preisermäßigung erhält, bleibt die Einwilligung dennoch eine gültige Rechtsgrundlage für die Verarbeitung personenbezogener Daten derjenigen Kunden, die eine solche Karte akzeptiert haben. Es liegt hier keine Unterordnung zwischen Unternehmen und Kunde vor, und die Folgen der nicht gegebenen Einwilligung sind nicht so schwerwiegend, dass sie die freie Auswahl der betroffenen Person behinderten.

Wenn hingegen Waren oder Dienstleistungen nur erlangt werden können, wenn bestimmte personenbezogene Daten an den Verantwortlichen oder an Dritte weitergegeben werden, kann man nicht davon ausgehen, dass die betroffene Person die Einwilligung in die Offenlegung ihrer für den Vertrag nicht erforderlichen Daten ohne Zwang gegeben hat, und eine derartige Einwilligung ist daher nach dem Datenschutzrecht nicht gültig.³⁵² Die DSGVO verfolgt einen recht strengen Ansatz in Bezug auf das Verbot der Verknüpfung der Einwilligung mit der Bereitstellung von Waren und Dienstleistungen.³⁵³

Beispiel: Die von Fluggästen gegenüber einer Fluggesellschaft bekundete Zustimmung zur Offenlegung so genannter Fluggastdatensätze (d. h. Angaben zu ihrer Identität, ihren Essgewohnheiten oder Gesundheitsproblemen) an die Einwanderungsbehörden eines bestimmten Drittlandes kann aus datenschutzrechtlicher Sicht nicht als gültige Einwilligung betrachtet werden, da die Reisenden, wollen sie in dieses Land reisen, keine andere Wahl haben. Sollen solche Daten rechtmäßig übermittelt werden, ist hierfür eine andere Rechtsgrundlage als die Einwilligung erforderlich, vermutlich ein entsprechendes Gesetz.

³⁵² Datenschutz-Grundverordnung, Artikel 7 Absatz 4.

³⁵³ a.a.O.

Einwilligung in Kenntnis der Sachlage

Bevor die betroffene Person ihre Entscheidung trifft, muss sie über ausreichende Informationen verfügen. Bei einer Einwilligung in Kenntnis der Sachlage muss normalerweise eine genaue und leicht verständliche Beschreibung des Sachverhalts vorliegen, zu dem die Einwilligung gegeben werden soll. Den Erläuterungen der Artikel-29-Datenschutzgruppe zufolge, muss die Einwilligung nach der bewussten Erfassung und Würdigung der Fakten und Auswirkungen der in der Einwilligung zu der Verarbeitung bestehenden Handlung der betroffenen Person erfolgen. Demnach „muss [die betroffene Person] in klarer und verständlicher Form genau und umfassend über alle relevanten Aspekte, [...] wie Art und Zweckbestimmung der verarbeiteten Daten, Personen, an die die Daten möglicherweise weitergegeben werden, und ihre Rechte, aufgeklärt werden.“³⁵⁴ Damit die Einwilligung in Kenntnis der Sachlage gegeben werden kann, müssen die Personen auch über die möglichen Folgen bei Verweigerung der Einwilligung zu der jeweiligen Verarbeitung aufgeklärt sein.

In Anbetracht der Bedeutung einer Einwilligung in Kenntnis der Sachlage, bemühten sich die DSGVO und der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 um eine Erläuterung des Begriffs. In den Erwägungsgründen der DSGVO heißt es: „Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen“.³⁵⁵

Damit eine Einwilligung im Sonderfall ihrer Verwendung als Ausnahme zur Gewährleistung eines rechtmäßigen Grundes für eine internationale Datenübermittlung als gültig betrachtet werden kann, muss der Verantwortliche die betroffene Person über die für sie bestehenden möglichen Risiken derartiger Übermittlungen ohne Vorliegen einer Angemessenheitsentscheidung und ohne geeignete Garantien unterrichten.³⁵⁶

354 Artikel-29-Datenschutzgruppe (2007), [Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten \(EPA\)](#), WP 131, Brüssel, 15. Februar 2007.

355 Datenschutz-Grundverordnung, Erwägungsgrund 42.

356 a.a.O., Artikel 49 Absatz 1 Buchstabe a.

In dem erläuternden Bericht zum Modernisierten Übereinkommen Nr. 108 wird präzisiert, dass die betroffene Person über die Auswirkungen ihrer Entscheidung unterrichtet werden muss, und zwar darüber, „was die Tatsache der Einwilligungserteilung zur Folge hat und welchen Umfang die erteilte Einwilligung hat“.³⁵⁷

Die Qualität der Information ist wichtig. Mit der Qualität der Information ist gemeint, dass die Sprache der Information auf ihre voraussichtlichen Empfänger abgestimmt werden sollte. Die Information ist ohne die Verwendung von Jargon, in einer klaren und einfachen Sprache zu erteilen, die ein durchschnittlicher Nutzer verstehen müsste.³⁵⁸ Die betroffene Person muss außerdem leicht an die Informationen herankommen. Zugänglichkeit und Sichtbarkeit der Informationen sind wesentliche Faktoren: die Informationen müssen gut sichtbar sein und ins Auge stechen. In einem Online-Umfeld können Informationsvermerke in mehreren Schichten eine Lösung sein, da die betroffenen Personen dadurch zwischen einer Kurzfassung oder einer ausführlicheren Fassung wählen können

Einwilligung für den konkreten Fall

Damit eine Einwilligung gültig ist, muss sie auch für den konkreten Verarbeitungszweck gegeben werden, der klar und in unmissverständlichen Worten zu beschreiben ist. Dies steht in engem Zusammenhang mit der Qualität der Informationen über den Zweck der Einwilligung. In diesem Zusammenhang sind die begründeten Erwartungen einer durchschnittlichen betroffenen Person von Bedeutung. Werden Verarbeitungsvorgänge hinzugefügt oder in einer Weise abgeändert, die bei Erteilung der ursprünglichen Einwilligung nach menschlichem Ermessen nicht vorhersehbar waren und demnach zu einer Zweckänderung führen, muss erneut die Einwilligung der betroffenen Person eingeholt werden. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden.³⁵⁹

357 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 42.

358 Artikel-29-Datenschutzgruppe (2011), *Stellungnahme 15/2011 zur Definition von Einwilligung*, WP187, Brüssel, 13. Juli 2011, S. 19.

359 Datenschutz-Grundverordnung, Erwägungsgrund 32.

Beispiele: In der *Rechtssache Deutsche Telekom AG*³⁶⁰ prüfte der EuGH, ob ein Telekomanbieter, der personenbezogene Daten von Teilnehmern für elektronische Kommunikation zur Veröffentlichung in Teilnehmerverzeichnissen weitergeben musste, erneut die Einwilligung der betroffenen Personen einholen musste,³⁶¹ da die Empfänger der Daten namentlich nicht genannt wurden, als die Einwilligung ursprünglich gegeben wurde.

Der EuGH stellte fest, dass gemäß Artikel 12 der Datenschutzrichtlinie für elektronische Kommunikation das erneute Einholen einer Einwilligung vor der Offenlegung der Daten nicht erforderlich ist. Da die betroffenen Personen nur die Möglichkeit hätten, dem Zweck der Verarbeitung zuzustimmen, der in der Veröffentlichung ihrer Daten bestand, konnten sie nicht zwischen verschiedenen Verzeichnissen wählen, in denen diese Daten veröffentlicht werden konnten.

Der EuGH betonte, „aus einer wörtlichen und systematischen Auslegung des Artikels 12 der Datenschutzrichtlinie für elektronische Kommunikation geht hervor, dass sich die Zustimmung nach Artikel 12 Absatz 2 auf den Zweck der Veröffentlichung der personenbezogenen Daten in einem öffentlichen Teilnehmerverzeichnis und nicht auf einen bestimmten Anbieter eines Verzeichnisses bezieht.“³⁶² Auch ist „es gerade die Veröffentlichung der personenbezogenen Daten in einem Teilnehmerverzeichnis, das einen besonderen Zweck verfolgt, [...] die sich für einen Teilnehmer nachteilig auswirken kann“,³⁶³ unabhängig von der Identität des Herausgebers.

In der Rechtssache *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV gegen Autoriteit Consument en Markt (AMC)*³⁶⁴ beantragte eine belgische Gesellschaft, die Auskunftsdienste und Teilnehmerverzeichnisse anbietet, von Unternehmen, die Teilnehmern in den Niederlanden Telefonnummern zuweisen, ihr ihre Teilnehmerdaten zur Verfügung zu

360 EuGH, C-543/09, *Deutsche Telekom AG / Bundesrepublik Deutschland*, 5. Mai 2011. Siehe insbesondere Randnrn. 53 und 54.

361 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

362 EuGH, C-543/09, *Deutsche Telekom AG / Bundesrepublik Deutschland*, 5. Mai 2011, Randnr. 61.

363 a.a.O., Randnr. 62.

364 EuGH, C-536/15, *Tele2 (Netherlands) BV und andere / Autoriteit Consument en Markt (AMC)*, 15. März 2017.

stellen. Die belgische Gesellschaft berief sich dabei auf eine Verpflichtung im Rahmen der Universaldienstrichtlinie.³⁶⁵ Diese verlangt von Unternehmen, die Telefonnummern zuweisen, diese Nummern auf Antrag Teilnehmerverzeichnisse zur Verfügung zu stellen, sofern die Teilnehmer ihre Einwilligung zur Veröffentlichung ihrer Nummern erteilt haben. Die niederländischen Unternehmen verweigerten dies mit der Erklärung, dass sie nicht dazu verpflichtet seien, die betreffenden Daten einer in einem anderen Mitgliedstaat ansässigen Gesellschaft bereitzustellen. Sie argumentierten, dass die Nutzer ihre Einwilligung zur Veröffentlichung ihrer Nummern unter der Voraussetzung geben würden, dass diese in einem niederländischen Teilnehmerverzeichnis veröffentlicht werden würden. Der EuGH entschied, dass die Universaldienstrichtlinie alle Anträge von Auskunftsdiensten umfasst, unabhängig davon, in welchem Mitgliedstaat sie ansässig sind. Der EuGH befand auch, dass die ohne erneute Zustimmung der Teilnehmer vorgenommene Weitergabe derselben Daten an ein anderes Unternehmen, das ein öffentliches Teilnehmerverzeichnis veröffentlichen möchte, das Recht auf Schutz personenbezogener Daten nicht in seinem Wesensgehalt berühren kann.³⁶⁶ Folglich ist es für das Unternehmen, das seinen Teilnehmern Telefonnummern zuweist, nicht angezeigt, das an den Teilnehmer gerichtete Ersuchen um Einwilligung so zu formulieren, dass er bei seiner Einwilligung danach differenziert, in welchen Mitgliedstaat die ihn betreffenden Daten übermittelt werden können.³⁶⁷

Unmissverständliche Einwilligung

Jede Einwilligung muss unmissverständlich abgegeben werden.³⁶⁸ Es darf also kein berechtigter Zweifel daran bestehen, dass die betroffene Person ihr Einverständnis zur Verarbeitung ihrer Daten kundtun wollte. So kann beispielsweise aus der Untätigkeit der betroffenen Person nicht auf ihre unmissverständliche Einwilligung geschlossen werden.

365 Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und diensten (Universaldienstrichtlinie) (ABl. L 108 vom 24.4.2002, S. 51) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (Universaldienstrichtlinie) (ABl. L 337 vom 18.12.2009, S. 11), geänderten Fassung.

366 EuGH, C-536/15, *Tele2 (Netherlands) BV und andere / Autoriteit Consument en Markt (AMC)*, 15. März 2017, Randnr. 36.

367 a.a.O., Randnrn. 40 und 41.

368 Datenschutz-Grundverordnung, Artikel 4 Absatz 11.

Dies wäre der Fall bei Verantwortlichen, die die Einwilligung mit Aussagen wie der nachstehenden in ihren Datenschutzbestimmungen einholen: „Durch die Nutzung unserer Dienstleistung stimmen Sie der Verarbeitung Ihrer personenbezogenen Daten zu“. In diesem Fall müssten die Verantwortlichen sicherstellen, dass die Nutzer diesen Datenschutzbestimmungen manuell und einzeln zustimmen.

Sofern die Einwilligung in schriftlicher Form als Teil eines Vertrags erfolgt, ist die Einwilligung zur Verarbeitung personenbezogener Daten zu individualisieren und in jedem Fall „sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt.“³⁶⁹

Anforderungen an die Einwilligung im Falle von Kindern

Die DSGVO sieht im Zusammenhang mit der Bereitstellung von Diensten der Informationsgesellschaft einen besonderen Schutz für Kinder vor, da „Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind“.³⁷⁰ Wenn Anbieter von Diensten der Informationsgesellschaft eine auf Einwilligung beruhende Verarbeitung personenbezogener Daten von Kindern unter 16 Jahren durchführen, ist diese Verarbeitung im **EU-Recht** folglich nur rechtmäßig, „sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird“.³⁷¹ Die Mitgliedstaaten können durch nationale Rechtsvorschriften eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.³⁷² Die Einwilligung des Trägers der elterlichen Verantwortung ist „im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden“ nicht erforderlich.³⁷³ Wenn sich die Verarbeitung an Kinder richtet, sollten Informationen und Hinweise in einer klaren und einfachen Sprache erfolgen, die ein Kind leicht verstehen kann.³⁷⁴

369 a.a.O., Erwägungsgrund 42.

370 a.a.O., Erwägungsgrund 38.

371 a.a.O. Artikel 8 Absatz 1 erster Spiegelstrich. Der Begriff „Dienste der Informationsgesellschaft“ ist in Artikel 4 Absatz 25 der Datenschutz-Grundverordnung definiert.

372 Datenschutz-Grundverordnung, Artikel 8 Absatz 1 zweiter Gedankenstrich.

373 a.a.O., Erwägungsgrund 38.

374 a.a.O., Erwägungsgrund 58. Siehe auch Modernisiertes Übereinkommen Nr. 108, Artikel 15 Absatz 2; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absätze 68 und 125.

Das Recht, die Einwilligung jederzeit zu widerrufen

Die DSGVO enthält ein allgemeines Recht, eine Einwilligung jederzeit zu widerrufen.³⁷⁵ Die betroffene Person wird vor Abgabe der Einwilligung über dieses Recht in Kenntnis gesetzt und kann dieses Recht nach eigenem Ermessen ausüben. Es sollte kein Erfordernis zur Angabe von Gründen für den Widerruf bestehen und keine Gefahr negativer Folgen, die über die Beendigung jedweder aus der zuvor vereinbarten Datennutzung möglicherweise entstandenen Vorteile hinausgehen. Der Widerruf der Einwilligung sollte so einfach wie die Erteilung der Einwilligung sein.³⁷⁶ Es kann keine Einwilligung ohne Zwang vorliegen, wenn die betroffene Person ihre Einwilligung nicht widerrufen kann ohne Nachteile zu erleiden, oder der Widerruf der Einwilligung nicht so einfach ist wie deren Erteilung war.³⁷⁷

Beispiel: Ein Kunde stimmt der Zusendung von Werbesendungen an eine Adresse zu, die er einem Verantwortlichen angegeben hat. Widerruft der Kunde seine Zustimmung, muss der Verantwortliche die Versendung des Werbematerials unverzüglich einstellen. Dies darf keine Sanktionen wie zum Beispiel Gebühren zur Folge haben. Der Widerruf wird jedoch für die Zukunft ausgeübt und ist nicht rückwirkend. Im Zeitraum, in dem die personenbezogenen Daten des Kunden aufgrund dessen Einwilligung rechtmäßig verarbeitet wurden, war die Verarbeitung berechtigt. Der Widerruf verhindert jede weitere Verarbeitung dieser Daten, es sei denn, eine solche Verarbeitung steht im Einklang mit dem Recht auf Löschung.³⁷⁸

Notwendigkeit für die Erfüllung eines Vertrags

Im EU-Recht liefert Artikel 6 Absatz 1 Buchstabe b DSGVO eine weitere Grundlage für die rechtmäßige Verarbeitung, und zwar sofern es „für die Erfüllung eines Vertrags [erforderlich ist], dessen Vertragspartei die betroffene Person ist“. Diese Bestimmung erfasst auch vorvertragliche Beziehungen. Beispielsweise in Fällen, in denen eine Partei einen Vertrag abschließen möchte,

³⁷⁵ Datenschutz-Grundverordnung, Artikel 7 Absatz 3; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 45.

³⁷⁶ Datenschutz-Grundverordnung, Artikel 7 Absatz 3.

³⁷⁷ Datenschutz-Grundverordnung, Erwägungsgrund 42; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 42.

³⁷⁸ Datenschutz-Grundverordnung, Artikel 17 Absatz 1 Buchstabe b.

dies aber noch nicht getan hat, weil möglicherweise noch ein paar Dinge zu überprüfen sind. Muss nun eine Partei für diesen Zweck Daten verarbeiten, ist eine solche Verarbeitung rechtmäßig, sofern sie „zur Durchführung vorvertraglicher Maßnahmen erforderlich [ist], die auf Anfrage der betroffenen Person erfolgen“.³⁷⁹

Der Begriff der Datenverarbeitung als „zulässige Rechtsgrundlage“ in Artikel 5 Absatz 2 des Modernisierten Übereinkommens Nr. 108, umfasst auch die „Datenverarbeitung zur Erfüllung eines Vertrags (oder auf Antrag der betroffenen Person erfolgende vorvertragliche Maßnahmen), dessen Vertragspartei die betroffene Person ist“.³⁸⁰

Rechtliche Verpflichtungen des Verantwortlichen

Das **EU-Recht** legt einen weiteren Grund für die Rechtmäßigkeit der Verarbeitung dar, nämlich „die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt“ (Artikel 6 Absatz 1 Buchstabe c DSGVO). Diese Bestimmung gilt für Verantwortliche im privaten und im öffentlichen Sektor; die rechtlichen Verpflichtungen von Verantwortlichen im öffentlichen Sektor können auch unter die Bestimmungen von Artikel 6 Absatz 1 Buchstabe e DSGVO fallen. Es gibt viele Beispiele von Situationen, in denen Verantwortliche im privaten Sektor gesetzlich dazu verpflichtet sind, Daten konkreter betroffener Personen zu verarbeiten. Arbeitgeber müssen beispielsweise Daten über ihre Beschäftigten für die Sozialversicherung und das Finanzamt verarbeiten und Unternehmen müssen zu Steuerzwecken Daten über ihre Kunden verarbeiten.

Die rechtliche Verpflichtung kann sich aus dem Unionsrecht oder aus dem Recht eines Mitgliedstaates ergeben, das die Grundlage für eine oder mehrere Verarbeitungstätigkeiten darstellen könnte. Es sollte rechtlich geregelt werden, für welche Zwecke die Daten verarbeitet werden dürfen, es sollte festgelegt werden, wie der Verantwortliche zu bestimmen ist, welche Art von personenbezogenen Daten verarbeitet werden, welche Personen betroffen sind, welchen Einrichtungen die personenbezogenen Daten offengelegt, für welche

379 a.a.O., Artikel 6 Absatz 1 Buchstabe b.

380 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 46; Europarat, Ministerkomitee (2010), Empfehlung CM/Rec(2010)13 des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling, 23. November 2010, Artikel 3.4 Buchstabe b.

Zwecke und wie lange sie gespeichert werden dürfen und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung rechtmäßig und nach Treu und Glauben erfolgt.³⁸¹ Jedwedes solche Gesetz, das die Grundlage für die Verarbeitung personenbezogener Daten darstellt, muss mit den Bestimmungen aus Artikel 7 und 8 der Charta und Artikel 8 EMRK übereinstimmen.

Die rechtlichen Verpflichtungen des Verantwortlichen dienen auch nach dem **Recht des Europarates** als Grundlage für eine rechtmäßige Verarbeitung.³⁸² Wie bereits erläutert, sind die rechtlichen Verpflichtungen eines Verantwortlichen, der im privaten Sektor tätig ist, nur ein besonderer Fall der in Artikel 8 Absatz 2 EMRK erwähnten berechtigten Interessen anderer. Das Beispiel der Arbeitgeber, die die Daten ihrer Beschäftigten verarbeiten, ist also auch für das Recht des Europarates relevant.

Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person

Im **EU-Recht** sieht Artikel 6 Absatz 1 Buchstabe d DSGVO vor, dass die Verarbeitung personenbezogener Daten rechtmäßig ist, wenn sie „erforderlich [ist], um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen“. Auf diesen rechtmäßigen Grund kann man sich für die Verarbeitung personenbezogener Daten aufgrund der lebenswichtigen Interessen einer anderen natürlichen Person nur dann berufen, wenn diese Verarbeitung „offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann“.³⁸³ Zuweilen kann es sein, dass sich eine Verarbeitungsart auf Gründe des öffentlichen Interesses und auf Gründe der lebenswichtigen Interessen der betroffenen Person oder einer anderen Person stützt. Dies ist beispielsweise bei der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen der Fall.

Im **Recht des Europarates** werden in Artikel 8 EMRK lebenswichtige Interessen der betroffenen Person nicht erwähnt. Die lebenswichtigen Interessen der betroffenen Person gelten jedoch als im Begriff der „Rechtsgrundlage“ aus

381 Datenschutz-Grundverordnung, Erwägungsgrund 45.

382 Europarat, Ministerkomitee (2010), Empfehlung CM/Rec(2010)13 des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling, 23. November 2010, Artikel 3.4 Buchstabe a.

383 Datenschutz-Grundverordnung, Erwägungsgrund 46.

Artikel 5 Absatz 2 des Modernisierten Übereinkommens Nr. 108 enthalten, der sich mit der Rechtmäßigkeit der Verarbeitung personenbezogener Daten beschäftigt.³⁸⁴

Öffentliches Interesse und Ausübung öffentlicher Gewalt

In Anbetracht der vielen möglichen Organisationsformen staatlichen Handelns bestimmt Artikel 6 Absatz 1 Buchstabe e DSGVO, dass personenbezogene Daten rechtmäßig verarbeitet werden dürfen, wenn dies „für die Wahrnehmung einer Aufgabe erforderlich [ist], die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“.³⁸⁵

Beispiel: In der Rechtssache *Huber gegen Bundesrepublik Deutschland*³⁸⁶ forderte Herr Huber, ein in Deutschland lebender österreichischer Staatsbürger, das Bundesamt für Migration und Flüchtlinge auf, ihn betreffende Daten aus dem Ausländerzentralregister („AZR“) zu löschen. Dieses Register, das personenbezogene Daten ausländischer EU-Bürger enthält, die sich länger als drei Monate in Deutschland aufhalten, wird für statistische Zwecke sowie von Strafverfolgungs- und Justizbehörden bei der Bekämpfung und Aufklärung strafbarer oder die öffentliche Sicherheit gefährdender Handlungen genutzt. Das vorlegende Gericht wollte wissen, ob die Verarbeitung personenbezogener Daten in einem Register wie dem Ausländerzentralregister, auf das auch andere Behörden Zugriff haben, in Anbetracht der Tatsache, dass für deutsche Staatsbürger ein solches Register nicht besteht, mit dem EU-Recht vereinbar ist.

Der EuGH stellte fest, dass gemäß Artikel 7 Buchstabe e der Richtlinie 95/46/EG³⁸⁷ die Verarbeitung personenbezogener Daten zulässig ist, wenn sie erforderlich für die Wahrnehmung einer Aufgabe ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt.

384 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 46.

385 Datenschutz-Grundverordnung, Erwägungsgrund 45.

386 EuGH, C-524/06, *Heinz Huber / Bundesrepublik Deutschland* [GK], 16. Dezember 2008.

387 Frühere Datenschutzrichtlinie, Artikel 7 Buchstabe e, nun Datenschutz-Grundverordnung, Artikel 6 Absatz 1 Buchstabe e.

Weiter führte der EuGH aus: „Angesichts des Zieles der Gewährleistung eines gleichwertigen Schutzniveaus in allen Mitgliedstaaten kann daher der Begriff der Erforderlichkeit im Sinne von Artikel 7 Buchstabe e der Richtlinie 95/46/³⁸⁸ [...] in den einzelnen Mitgliedstaaten keinen variablen Inhalt haben. Es handelt sich somit um einen autonomen Begriff des Gemeinschaftsrechts, der so auszulegen ist, dass er in vollem Umfang dem Ziel dieser Richtlinie, so wie es in ihrem Artikel 1 Absatz 1 definiert wird, entspricht“.³⁸⁹

Der EuGH wies darauf hin, dass das Aufenthaltsrecht eines Unionsbürgers im Hoheitsgebiet eines Mitgliedstaats, dessen Staatsangehörigkeit er nicht besitzt, nicht uneingeschränkt besteht und den im Vertrag zur Gründung der Europäischen Gemeinschaft und in den Bestimmungen zu seiner Durchführung vorgesehenen Beschränkungen und Bedingungen unterworfen werden darf. Folglich ist zwar der Gebrauch eines Registers wie des AZR zur Unterstützung der mit der Anwendung aufenthaltsrechtlicher Vorschriften betrauten Behörden grundsätzlich legitim, doch darf ein solches Register keine anderen Informationen enthalten als die, die zu dem genannten Zweck erforderlich sind. Nach Auffassung des EuGH ist ein solches System für die Verarbeitung personenbezogener Daten mit dem EU-Recht vereinbar, wenn es nur die Daten enthält, die für die Anwendung der entsprechenden Vorschriften erforderlich sind, und sein zentralisierter Charakter eine effizientere Anwendung dieser Vorschriften erlaubt. Es ist Sache des vorlegenden Gerichts, diese Umstände im vorliegenden Fall zu prüfen. Jedenfalls lassen sich die Speicherung und Verarbeitung personenbezogener Daten im Rahmen eines Registers wie des AZR zu statistischen Zwecken nicht als erforderlich im Sinne von Artikel 7 Buchstabe e³⁹⁰ der Richtlinie 95/46/EG ansehen.³⁹¹

Zur Frage der Verwendung der Daten in dem Register zur Bekämpfung der Kriminalität stellte der Gerichtshof fest, dass sich dieses Ziel „zwingend auf die Verfolgung von Verbrechen und Vergehen unabhängig von der Staatsangehörigkeit der Täter“ bezieht. Das fragliche Register enthält keine personenbezogenen Daten von Staatsangehörigen des betreffenden Mitgliedstaats, und diese unterschiedliche Behandlung ist eine durch Artikel 18 AEUV untersagte Diskriminierung. Folglich ist nach Auffassung

388 a.a.O.

389 EuGH, C-524/06, *Heinz Huber / Bundesrepublik Deutschland* [GK], 16. Dezember 2008, Randnr. 52.

390 Frühere Datenschutzrichtlinie, Artikel 7 Buchstabe e, nun Datenschutz-Grundverordnung, Artikel 6 Absatz 1 Buchstabe e.

391 EuGH, C-524/06, *Heinz Huber / Bundesrepublik Deutschland* [GK], 16. Dezember 2008, Randnrn. 54, 58–59 und 66–68.

des Gerichtshofes diese Bestimmung dahin auszulegen, dass sie „es einem Mitgliedstaat verwehrt, zur Bekämpfung der Kriminalität ein System zur Verarbeitung personenbezogener Daten zu errichten, das nur Unionsbürger erfasst, die keine Staatsangehörigen dieses Mitgliedstaats sind.“³⁹²

Die Verwendung personenbezogener Daten durch im öffentlichen Bereich tätige Behörden ist auch Gegenstand von Artikel 8 EMRK und soll, wo angemessen, durch Artikel 5 Absatz 2 des Modernisierten Übereinkommens 108 abgedeckt werden.³⁹³

Berechtigte Interessen des Verantwortlichen oder eines Dritten

Im **EU-Recht** hat nicht nur die betroffene Person berechtigte Interessen. Gemäß Artikel 6 Absatz 1 Buchstabe f DSGVO dürfen personenbezogene Daten rechtmäßig verarbeitet werden, wenn die Verarbeitung „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten oder Dritter (mit Ausnahme von Behörden in Erfüllung ihrer Aufgaben) erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen [...]“.³⁹⁴

Das Bestehen eines berechtigten Interesses ist in jedem Einzelfall besonders sorgfältig abzuwägen.³⁹⁵ Wenn die berechtigten Interessen des Verantwortlichen ermittelt sind, sind diese Interessen gegen die Interessen oder Grundrechte und Freiheiten der betroffenen Person abzuwägen.³⁹⁶ Im Rahmen einer solchen Abwägung sind die begründeten Erwartungen der betroffenen Person zu berücksichtigen, um ermitteln zu können, ob die Interessen des Verantwortlichen die Interessen oder Grundrechte der betroffenen Person überwiegen.³⁹⁷ Sofern die Rechte der betroffenen Person die berechtigten Interessen des Verantwortlichen überwiegen, kann der Verantwortliche Maßnahmen ergreifen

³⁹² a.a.O., Randnm. 78 und 81.

³⁹³ Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 46–47.

³⁹⁴ Im Vergleich zur Richtlinie 95/46/EG liefert die Datenschutz-Grundverordnung mehr Beispiele von Fällen, die als berechtigtes Interesse angesehen werden.

³⁹⁵ Datenschutz-Grundverordnung, Erwägungsgrund 47.

³⁹⁶ Artikel-29-Datenschutzgruppe (2014), *Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG*, 4. April 2014.

³⁹⁷ a.a.O.

und Sicherheitsmaßnahmen umsetzen, um zu gewährleisten, dass die Auswirkungen auf die Rechte der betroffenen Person minimiert werden (wie die Pseudonymisierung der Daten), und die „Abwägung“ umkehren, bevor er sich rechtmäßig auf diese Rechtsgrundlage für die Verarbeitung berufen kann. In ihrer Stellungnahme zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen betonte die Artikel-29-Datenschutzgruppe die bei der Abwägung der berechtigten Interessen des Verantwortlichen gegen die Interessen der Grundrechte der betroffenen Person entscheidende Rolle des Grundsatzes der Verantwortlichkeit und der Transparenz und der Rechte der betroffenen Person, gegen die Verarbeitung ihrer Daten Widerspruch einzulegen, Zugang zu ihren Daten zu erhalten, diese zu modifizieren, zu löschen oder zu übertragen.³⁹⁸

In den Erwägungsgründen der DSGVO werden einige Beispiele dafür angeführt, was ein berechtigtes Interesse des betreffenden Verantwortlichen darstellt. Beispielsweise ist die Verarbeitung personenbezogener Daten ohne Einwilligung der betroffenen Person erlaubt, um Direktwerbung zu betreiben oder wenn eine solche Verarbeitung „im für die Verhinderung von Betrug unbedingt erforderlichen Umfang“ erfolgt.³⁹⁹

Der EuGH ist in seiner Rechtsprechung auf die Prüfung zur Bestimmung eines berechtigten Interesses näher eingegangen.

Beispiel: In der Rechtssache *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*⁴⁰⁰ ging es um den Schaden, den das unerwartete Öffnen einer Taxitür seitens eines Fahrgastes an einem Oberleitungsbus eines Transportunternehmens aus Riga verursachte. Rīgas satiksme wollte den Fahrgast auf Schadensersatz verklagen. Die Polizei gab jedoch nur den Namen des Fahrgastes heraus und lehnte es ab, die persönliche Identifikationsnummer und den Wohnsitz dieser Person mitzuteilen, da diese Übermittlung ihrer Ansicht nach nach Maßgabe der nationalen Datenschutzgesetze rechtswidrig wäre.

398 a.a.O.

399 Datenschutz-Grundverordnung, Erwägungsgrund 47.

400 EuGH, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde / Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4. Mai 2017.

Das lettische vorlegende Gericht bat den EuGH, eine Vorabentscheidung darüber zu treffen, ob die Datenschutzvorschriften der EU eine Pflicht zur Übermittlung sämtlicher personenbezogenen Daten auferlegen, die für die Erhebung einer zivilrechtlichen Klage gegen die für eine Ordnungswidrigkeit mutmaßlich verantwortliche Person erforderlich sind.⁴⁰¹

Der EuGH erläuterte, dass das Datenschutzrecht der EU die Möglichkeit, nicht jedoch die Verpflichtung enthält, Daten an einen Dritten zu übermitteln, die zur Verwirklichung von dessen berechtigtem Interesse erforderlich sind.⁴⁰² Der EuGH legte drei kumulative Voraussetzungen dar, die erfüllt sein müssen, damit die Verarbeitung personenbezogener Daten nach Maßgabe der Rechtsgrundlage des „berechtigten Interesses“ rechtmäßig ist.⁴⁰³ Erstens muss der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse verfolgen. Im vorliegenden Fall bedeutet dies, dass die Anforderung personenbezogener Daten um gegen eine Person eine Klage wegen Eigentumsverletzung einzureichen, ein berechtigtes Interesse eines Dritten darstellt. Zweitens muss die Verarbeitung personenbezogener Daten zur Verwirklichung des berechtigten Interesses erforderlich sein. Im vorliegenden Fall ist der Erhalt personenbezogener Daten wie die Anschrift und/oder die Identifikationsnummer zur Identifizierung dieser Person unbedingt erforderlich. Drittens dürfen die Grundrechte und Freiheiten der betroffenen Person nicht gegenüber den berechtigten Interessen des Verantwortlichen oder des Dritten überwiegen. Die Abwägung der Interessen muss für den jeweiligen Einzelfall unter Berücksichtigung der Stärke der Beeinträchtigung der Rechte der betroffenen Person oder unter bestimmten Umständen selbst unter Berücksichtigung des Alters der betroffenen Person erfolgen. Im vorliegenden Fall betrachtete es der EuGH als nicht gerechtfertigt, die Übermittlung nur deshalb abzulehnen, weil die betroffene Person minderjährig war.

Im Urteil in der Rechtssache *ASNEF und FECEMD* äußerte sich der EuGH ausdrücklich zur Verarbeitung von Daten auf der Rechtsgrundlage der „berechtigten Interessen“, die zum damaligen Zeitpunkt in Artikel 7 Buchstabe f der Datenschutzrichtlinie verankert war.⁴⁰⁴

401 a.a.O., Randnr. 23.

402 a.a.O., Randnr. 26.

403 a.a.O., Randnrn. 28-34.

404 Frühere Datenschutzrichtlinie, Artikel 7 Buchstabe f, nun Datenschutz-Grundverordnung, Artikel 6 Absatz 1 Buchstabe f.

Beispiel: In der Rechtssache *ASNEF und FECEMD*⁴⁰⁵ stellte der EuGH klar, dass das einzelstaatliche Recht den in Artikel 7 Buchstabe f der Richtlinie genannten Bedingungen für eine rechtmäßige Verarbeitung von Daten keine weiteren Bedingungen hinzufügen darf.⁴⁰⁶ Es ging darum, dass das spanische Datenschutzrecht eine Bestimmung enthielt, der zufolge andere private Parteien ein berechtigtes Interesse an der Verarbeitung personenbezogener Daten nur dann geltend machen konnten, wenn die Daten bereits in öffentlich zugänglichen Quellen enthalten waren.

Der EuGH wies zunächst darauf hin, dass die Richtlinie 95/46⁴⁰⁷ bezweckt, in allen Mitgliedstaaten ein gleichwertiges Schutzniveau hinsichtlich der persönlichen Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten herzustellen. Die Angleichung der nationalen Rechtsvorschriften in diesem Bereich darf auch nicht zu einer Verringerung des durch sie garantierten Schutzes führen. Sie muss im Gegenteil darauf abzielen, in der Union ein hohes Schutzniveau sicherzustellen.⁴⁰⁸ Folglich befand der Gerichtshof: „Daher ergibt sich aus dem Ziel, ein gleichwertiges Schutzniveau in allen Mitgliedstaaten sicherzustellen, dass Artikel 7 der Richtlinie 95/46⁴⁰⁹ eine erschöpfende und abschließende Liste der Fälle vorsieht, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann“. Und weiter: „Folglich dürfen die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Artikel 7 der Richtlinie 95/46⁴¹⁰ einführen, noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs in diesem Artikel vorgesehenen Grundsätze verändern würden.“⁴¹¹ Der

405 EuGH, Verbundene Rechtssachen C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24. November 2011.

406 Frühere Datenschutzrichtlinie, Artikel 7 Buchstabe f, nun Datenschutz-Grundverordnung, Artikel 6 Absatz 1 Buchstabe f.

407 Frühere Datenschutzrichtlinie, nun Datenschutz-Grundverordnung.

408 EuGH, Verbundene Rechtssachen C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24. November 2011, Randnr. 28. Siehe Datenschutz-Grundverordnung, Erwägungsgründe 8 und 10.

409 Frühere Datenschutzrichtlinie, Artikel 7, nun Datenschutz-Grundverordnung, Artikel 6 Absatz 1 Buchstabe f.

410 Frühere Datenschutzrichtlinie, Artikel 7, nun Datenschutz-Grundverordnung, Artikel 6.

411 a.a.O.

EuGH räumte ein: „Bei der nach Artikel 7 Buchstabe f der Richtlinie 95/46 erforderlichen Abwägung kann berücksichtigt werden, dass die Grundrechte der betroffenen Person durch diese Datenverarbeitung unterschiedlich stark verletzt sein können, je nachdem, ob die in Rede stehenden Daten bereits in öffentlich zugänglichen Quellen enthalten sind oder nicht.“

Allerdings „verbietet Artikel 7 Buchstabe f der Richtlinie 95/46, dass ein Mitgliedstaat kategorisch und verallgemeinernd die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließt, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen.“

Aufgrund dieser Erwägungen, so der EuGH, ist Artikel 7 Buchstabe f der Richtlinie 95/46⁴¹² dahin auszulegen, „dass er einer nationalen Regelung entgegensteht, die für die Verarbeitung personenbezogener Daten, die zur Verwirklichung eines berechtigten Interesses, das von dem für diese Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen diese Daten übermittelt werden, erforderlich ist, ohne Einwilligung der betroffenen Person nicht nur verlangt, dass deren Grundrechte und Grundfreiheiten nicht verletzt werden, sondern auch, dass diese Daten in öffentlich zugänglichen Quellen enthalten sind, und damit kategorisch und verallgemeinernd jede Verarbeitung von Daten ausschließt, die nicht in solchen Quellen enthalten sind.“⁴¹³

Wann immer personenbezogene Daten nach Maßgabe der Rechtsgrundlage „berechtigter Interessen“ verarbeitet werden, hat die Person gemäß Artikel DSGVO das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Widerspruch einzulegen. Der Verantwortliche beendet die Verarbeitung, es sei denn, er kann zwingende schutzwürdige Gründe für deren Fortsetzung nachweisen.

412 Frühere Datenschutzrichtlinie, Artikel 7 Buchstabe f, nun Datenschutz-Grundverordnung, Artikel 6 Absatz 1 Buchstabe f.

413 EuGH, Verbundene Rechtssachen C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECMD) / Administración del Estado*, 24. November 2011, Randnrn. 40, 44 und 48–49.

Was das **Recht des Europarates** anbelangt, so finden sich ähnliche Formulierungen im Modernisierten Übereinkommen 108⁴¹⁴ und in den Empfehlungen des Europarates. Gemäß der Profiling-Empfehlung gilt die Verarbeitung personenbezogener Daten zu Zwecken des Profiling als rechtmäßig, wenn sie für die berechtigten Interessen anderer erforderlich ist, „soweit die Grundrechte und -freiheiten der betroffenen Person nicht vorrangig sind“.⁴¹⁵ Darüber hinaus wird der „Schutz der Rechte und Freiheiten anderer“ in Artikel 8 Absatz 2 EMRK als einer der berechtigten Gründe für die Einschränkung des Rechts auf Datenschutz genannt.

Beispiel: In der Rechtssache *Y gegen Türkei*⁴¹⁶ war der Beschwerdeführer HIV-positiv. Da er bei seiner Ankunft im Krankenhaus nicht bei Bewusstsein war, setzten die Rettungssanitäter die Mitarbeiter des Krankenhauses darüber in Kenntnis, dass er HIV-positiv war. Der Beschwerdeführer argumentierte vor dem EGMR, dass die Offenlegung dieser Information gegen sein Recht auf Achtung des Privatlebens verstoßen habe. In Anbetracht des Erfordernisses zum Schutz der Sicherheit der Krankenhausmitarbeiter wurde die Offenlegung dieser Information jedoch nicht als Verletzung seiner Rechte betrachtet.

4.1.2. Verarbeitung besonderer Datenkategorien (sensible Daten)

Das **Recht des Europarates** überlässt es dem innerstaatlichen Recht, für den angemessenen Schutz bei der Verwendung sensibler Daten zu sorgen, vorausgesetzt, die Bedingungen aus Artikel 6 des Modernisierten Übereinkommens Nr. 108 sind erfüllt, insbesondere dass angemessene Schutzvorkehrungen zur Ergänzung der anderen Übereinkommensbestimmungen im Gesetz festgelegt sind. Das **EU-Recht** enthält in Artikel 9 DSGVO eine detaillierte Regelung für die Verarbeitung besonderer Datenkategorien (auch als „sensible Daten“ bezeichnet). Dies sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit

⁴¹⁴ Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 46.

⁴¹⁵ Europarat, Ministerkomitee (2010), *Empfehlung CM/Rec(2010)13 und Begründung über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling*, 23. November 2010, Artikel 3.4 Buchstabe b (Profiling-Empfehlung).

⁴¹⁶ EGMR, *Y / Türkei*, Nr. 648/10, 17. Februar 2015.

hervorgehen, sowie für die Verarbeitung von genetischen und biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person und Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person. Die Verarbeitung sensibler Daten ist grundsätzlich untersagt.⁴¹⁷

In Artikel 9 Absatz 2 der Verordnung findet sich jedoch eine taxative Aufzählung von Ausnahmen von diesem Verbot, die den Rechtsgrundlagen für die Verarbeitung sensibler Daten entsprechen. Zu diesen Ausnahmen zählen Situationen, in denen:

- die betroffene Person ausdrücklich in die Datenverarbeitung einwilligt;
- die Verarbeitung durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten erfolgt und sich ausschließlich auf ihre (ehemaligen) Mitglieder oder auf Personen bezieht, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten;
- sich die Verarbeitung auf Daten bezieht, die die betroffene Person ausdrücklich öffentlich gemacht hat;
- die Verarbeitung für die nachstehenden Zwecke erforderlich ist:
 - damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann;
 - zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person (sofern die betroffene Person ihre Einwilligung nicht geben kann);
 - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit;

⁴¹⁷ Frühere Datenschutzrichtlinie, Artikel 7 Buchstabe f, nun Datenschutz-Grundverordnung, Artikel 9 Absatz 1.

- für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin: „für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs“;
- für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
- aus Gründen eines erheblichen öffentlichen Interesses.

Zur Verarbeitung besonderer Datenkategorien wird eine vertragliche Beziehung mit der betroffenen Person demnach nicht als Rechtsgrundlage für die rechtmäßige Verarbeitung sensibler Daten betrachtet, es sei denn, es handelt sich um einen dem Berufsgeheimnis unterliegenden Vertrag mit einem Angehörigen eines Gesundheitsberufs.⁴¹⁸

Ausdrückliche Einwilligung der betroffenen Person

Im **EU-Recht** ist die Einwilligung der betroffenen Person der erste mögliche Rechtsgrund für eine rechtmäßige Verarbeitung aller Daten, unabhängig davon, ob es sich dabei um nicht sensible oder sensible Daten handelt. Handelt es sich um sensible Daten, muss die Einwilligung ausdrücklich gegeben werden. Nach Unionsrecht oder dem Recht der Mitgliedstaaten kann es jedoch sein, dass das Verbot der Verarbeitung besonderer Datenkategorien durch die Einwilligung der betroffenen Person nicht aufgehoben werden kann.⁴¹⁹ Dies könnte beispielsweise der Fall sein, wenn die Verarbeitung ungewöhnliche Risiken für die betroffene Person birgt.

⁴¹⁸ Datenschutz-Grundverordnung, Artikel 9 Absatz 2 Buchstaben h und i.

⁴¹⁹ a.a.O., Artikel 9 Absatz 2 Buchstabe a.

Arbeitsrecht oder Recht der sozialen Sicherheit und des Sozialschutzes

Im **EU-Recht** kann das in Artikel 9 Absatz 1 dargelegte Verbot aufgehoben werden, wenn die Verarbeitung erforderlich ist, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann. Die Verarbeitung muss jedoch nach EU-Recht, nationalem Recht oder einer Kollektivvereinbarung nach nationalem Recht, das bzw. die geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig sein.⁴²⁰ Sich im Besitz eines Unternehmens befindende Aufzeichnungen über die Beschäftigten können unter bestimmten Bedingungen, die in der DSGVO und im einschlägigen nationalen Recht präzisiert sind, sensible personenbezogene Daten enthalten. Als Beispiele sensibler Daten können die Gewerkschaftszugehörigkeit oder Gesundheitsdaten angeführt werden.

Lebenswichtige Interessen der betroffenen Person oder einer anderen Person

Im **EU-Recht** dürfen sensible Daten ebenso wie nicht sensible Daten zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person verarbeitet werden.⁴²¹ Wenn die Verarbeitung auf den lebenswichtigen Interessen einer anderen Person gründet, kann sich auf diese Rechtsgrundlage nur berufen werden, wenn die Verarbeitung „offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann“.⁴²² In einigen Fällen kann die Verarbeitung personenbezogener Daten sowohl individuelle als auch öffentliche Interessen schützen, beispielsweise wenn die Verarbeitung für humanitäre Zwecke erforderlich ist.⁴²³

Damit eine Verarbeitung auf dieser Grundlage rechtmäßig ist, muss es unmöglich gewesen sein, die betroffene Person um eine Einwilligung zu bitten, weil die betroffene Person z. B. bewusstlos oder abwesend war und nicht erreicht werden konnte. Anders ausgedrückt, wenn die Person aus körperlichen oder rechtlichen Gründen außerstande war, ihre Einwilligung zu geben.

420 Datenschutz-Grundverordnung, Artikel 9 Absatz 2 Buchstabe b.

421 a.a.O., Artikel 9 Absatz 2 Buchstabe c.

422 a.a.O., Erwägungsgrund 46.

423 a.a.O.

Wohltätigkeitsorganisationen oder Organisationen ohne Gewinnerzielungsabsicht

Die Verarbeitung personenbezogener Daten ist ebenfalls erlaubt, wenn sie durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten erfolgt. Die Verarbeitung darf sich jedoch ausschließlich auf die Mitglieder oder ehemaligen Mitglieder der Organisation oder auf Personen beziehen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten.⁴²⁴ Ohne Einwilligung der betroffenen Person können die sensiblen Daten jedoch nicht außerhalb dieser Organisationen offengelegt werden.

Daten, die die betroffene Person offensichtlich öffentlich gemacht hat

Artikel 9 Absatz 2 Buchstabe e DSGVO sieht vor, dass die Verarbeitung nicht untersagt ist, wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat. Die Verordnung enthält zwar keine Definition der Bedeutung von „die die betroffene Person offensichtlich öffentlich gemacht hat“, doch da es sich dabei um eine Ausnahme vom Verbot der Verarbeitung sensibler Daten handelt, ist die Bedeutung restriktiv auszulegen und erfordert, dass die betroffene Person ihre personenbezogenen Daten vorsätzlich öffentlich gemacht hat. Wenn im Fernsehen ein Video von einer Videoüberwachungskamera übertragen wird, auf dem unter anderem zu sehen ist, wie ein Feuerwehrmann beim Versuch der Evakuierung eines Gebäudes verletzt wird, kann folglich nicht in Betracht gezogen werden, dass der Feuerwehrmann die Daten offensichtlich öffentlich gemacht hat. Sofern der Feuerwehrmann andererseits jedoch beschließt, den Vorfall zu beschreiben und das Video mit Fotos auf einer öffentlichen Internetseite zu veröffentlichen, wäre dies eine vorsätzliche, bestätigende Handlung zur Veröffentlichung der personenbezogenen Daten gewesen. Diesbezüglich sei darauf hingewiesen, dass die Veröffentlichung der eigenen Daten keine Einwilligung, sondern eine weitere Erlaubnis für die Verarbeitung besonderer Datenkategorien darstellt.

Die Tatsache, dass die betroffene Person die verarbeiteten personenbezogenen Daten öffentlich gemacht hat, befreit die Verantwortlichen nicht von ihren Verpflichtungen im Rahmen des Datenschutzgesetzes. Der Grundsatz der

424 a.a.O., Artikel 9 Absatz 2 Buchstabe d.

Zweckbeschränkung findet beispielsweise weiterhin auf personenbezogene Daten Anwendung, auch wenn diese Daten öffentlich verfügbar gemacht wurden.⁴²⁵

Rechtsansprüche

Die Verarbeitung besonderer Datenkategorien, „wenn sie erforderlich ist, um rechtliche Ansprüche sei es in einem Gerichtsverfahren oder in einem Verwaltungsverfahren oder einem außergerichtlichen Verfahren, geltend zu machen, auszuüben oder zu verteidigen“,⁴²⁶ ist gemäß DSGVO ebenfalls erlaubt.⁴²⁷ In diesem Fall muss die Verarbeitung für ein bestimmtes rechtliches Ziel und dessen Ausübung bzw. Verteidigung maßgeblich sein und kann von beiden Streitparteien beantragt werden.

Wenn Gerichte im Rahmen ihrer justiziellen Tätigkeit handeln, können sie besondere Datenkategorien im Rahmen der Beilegung einer Rechtsstreitigkeit verarbeiten.⁴²⁸ Beispiele für in diesem Zusammenhang verarbeitete besondere Datenkategorien könnten genetische Daten zur Feststellung der Abstammung sein, oder der Gesundheitszustand, wenn ein Teil des Beweises Einzelheiten einer seitens eines Opfers einer Straftat erlittenen Verletzung betrifft.

Gründe eines erheblichen öffentlichen Interesses

Gemäß Artikel 9 Absatz 2 Buchstabe g DSGVO können die Mitgliedstaaten weitere Umstände einführen, unter denen sensible Daten verarbeitet werden dürfen, vorausgesetzt:

- die Datenverarbeitung erfolgt aus Gründen eines erheblichen öffentlichen Interesses;
- sie ist im europäischen oder nationalen Recht vorgesehen;
- das europäische oder nationale Recht ist verhältnismäßig, wahrt das Recht auf Datenschutz und sieht angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Interessen der betroffenen Person vor.⁴²⁹

425 Artikel-29-Datenschutzgruppe (2013), *Opinion 3/13 on purpose limitation*, WP 203, Brüssel, 2. April 2013, S. 14.

426 Datenschutz-Grundverordnung, Erwägungsgrund 52.

427 a.a.O., Artikel 9 Absatz 2 Buchstabe f.

428 a.a.O.

429 a.a.O., Artikel 9 Absatz 2 Buchstabe g.

Ein bekanntes Beispiel sind die elektronischen Patientenakten. In solchen Akten können Gesundheitsdaten, die von Erbringern von Gesundheitsleistungen im Verlauf der Behandlung eines Patienten erhoben werden, anderen Erbringern von Gesundheitsleistungen dieses Patienten in großem Maßstab, meist landesweit, zur Verfügung gestellt werden.

Nach Auffassung der Artikel-29-Datenschutzgruppe können solche Systeme im Rahmen des bestehenden Datenschutzregelwerks nicht aufgebaut werden, weil darin Daten über Patienten verarbeitet werden.⁴³⁰ Gleichwohl kann es elektronische Patientenakten geben, sofern sie auf „Gründe eines erheblichen öffentlichen Interesses“ gestützt sind.⁴³¹ Dies würde eine eigene Rechtsgrundlage für ihre Errichtung verlangen, die auch die erforderlichen Garantien für einen sicheren Betrieb des Systems bietet.⁴³²

Weitere Rechtsgrundlagen für die Verarbeitung sensibler Daten

Die DSGVO sieht vor, dass sensible Daten verarbeitet werden können, sofern die Verarbeitung für die nachstehenden Zwecke erforderlich ist:⁴³³

- für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des EU-Rechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des EU-Rechts oder des Rechts eines Mitgliedstaats. Das Recht muss angemessene und spezifische Maßnahmen zur Wahrung der Rechte der betroffenen Person vorsehen;

430 Artikel-29-Datenschutzgruppe (2007), *Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)*, WP 131, Brüssel, 15. Februar 2007. Siehe auch Datenschutz-Grundverordnung, Artikel 9 Absatz 3.

431 Datenschutz-Grundverordnung, Artikel 9 Absatz 2 Buchstabe g.

432 Artikel-29-Datenschutzgruppe (2007), *Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)*, WP 131, Brüssel, 15. Februar 2007.

433 Datenschutz-Grundverordnung, Artikel 9 Absatz 2 Buchstaben h, i und j.

- für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke auf der Grundlage des EU-Rechts oder des Rechts eines Mitgliedstaats. Das Recht muss in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Interessen der betroffenen Person vorsehen.

Zusätzliche Bedingungen gemäß nationalem Recht

Die DSGVO erlaubt den Mitgliedstaaten die Einführung oder Aufrechterhaltung zusätzlicher Bedingungen, einschließlich Beschränkungen in Bezug auf die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten.⁴³⁴

4.2. Vorschriften über die Sicherheit der Verarbeitung

Kernpunkte

- Die Vorschriften über die Sicherheit der Verarbeitung verpflichten den Verantwortlichen und den Auftragsverarbeiter, geeignete technische und organisatorische Maßnahmen zu treffen, um unbefugte Eingriffe in Datenverarbeitungsvorgänge zu verhindern.
- Das erforderliche Niveau der Datensicherheit wird durch folgende Elemente bestimmt:
 - die auf dem Markt für die einzelnen Verarbeitungsarten verfügbaren Sicherheitsmerkmale,
 - die Kosten,
 - die Risiken der Datenverarbeitung für die Grundrechte und Freiheiten der betroffenen Personen.
- Die Gewährleistung der Vertraulichkeit personenbezogener Daten ist Bestandteil eines in der DSGVO anerkannten allgemeinen Grundsatzes.

434 a.a.O., Artikel 9 Absatz 2 Buchstabe h und Artikel 9 Absatz 4.

Sowohl im EU-Recht als auch im Recht des Europarates unterliegen die Verantwortlichen bei der Verarbeitung personenbezogener Daten den allgemeinen Grundsätzen der Transparenz und der Verantwortlichkeit, was insbesondere im Falle von Verletzungen des Schutzes personenbezogener Daten gilt. Im Falle von Verletzungen des Schutzes personenbezogener Daten müssen die Verantwortlichen die Aufsichtsbehörden darüber unterrichten, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen. Auch die betroffenen Personen sind über die Verletzung des Schutzes personenbezogener Daten zu unterrichten, wenn diese voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt.

4.2.1. Elemente der Datensicherheit

Die einschlägige Vorschrift im **EU-Recht** besagt:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten natürlicher Personen, treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten [...]“⁴³⁵

Diese Maßnahmen schließen unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;⁴³⁶
- die Sicherstellung, dass das System und der Dienst die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit aufrechterhalten;⁴³⁷
- im Falle des Datenverlusts die rasche Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und des Zugangs zu ihnen;⁴³⁸

⁴³⁵ a.a.O., Artikel 32 Absatz 1.

⁴³⁶ a.a.O., Artikel 32 Absatz 1 Buchstabe a.

⁴³⁷ a.a.O., Artikel 32 Absatz 1 Buchstabe b.

⁴³⁸ a.a.O., Artikel 32 Absatz 1 Buchstabe c.

- ein Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.⁴³⁹

Eine ähnliche Bestimmung gibt es auch im **Recht des Europarates**:

„Jede Vertragspartei sieht vor, dass der Verantwortliche und gegebenenfalls auch der Auftragsverarbeiter geeignete Sicherheitsmaßnahmen gegen Risiken wie den zufälligen oder unbefugten Zugang oder Verlust, die zufällige oder unbefugte Zerstörung, Nutzung, Änderung oder Offenlegung personenbezogener Daten treffen.“⁴⁴⁰

Im EU-Recht und im Recht des Europarates verpflichtet eine Verletzung des Datenschutzes, die sich auf die persönlichen Rechte und Freiheiten der Personen auswirken könnte, den Verantwortlichen zur Unterrichtung der Aufsichtsbehörde über diese Verletzung (siehe [Abschnitt 4.2.3](#)).

Häufig gibt es auch Industriestandards, nationale und internationale Normen, die für die sichere Verarbeitung von Daten entwickelt wurden. Das europäische Datenschutzgütesiegel EuroPriSe (European Privacy Seal) beispielsweise ist ein eTEN (Transeuropäische Telekommunikationsnetzwerke)-Projekt der EU, das sich mit den Möglichkeiten beschäftigt, Produkte, insbesondere Software, zu zertifizieren, um deren Einklang mit dem europäischen Datenschutzrecht zu vereinfachen. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) wurde errichtet, um die Fähigkeit der EU, der EU-Mitgliedstaaten und der Wirtschaft zu verbessern, Probleme im Bereich der Netz- und Informationssicherheit zu verhüten, zu bewältigen und zu beheben.⁴⁴¹ Die ENISA veröffentlicht regelmäßig Analysen aktueller Sicherheitsbedrohungen und berät bei deren Bewältigung.⁴⁴²

439 a.a.O., Artikel 32 Absatz 1 Buchstabe d.

440 Modernisiertes Übereinkommen Nr. 108, Artikel 7 Absatz 1.

441 Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004, Abl. L 165 vom 18. Juni 2013.

442 Zum Beispiel ENISA, (2016), *Cyber Security and Resilience of smart cars Good practices and recommendations*; ENISA (2016), *Security of Mobile Payments and Digital Wallets*.

Datensicherheit wird aber nicht nur mit der geeigneten Ausrüstung – Hardware und Software – erreicht. Sie bedarf auch geeigneter interner organisatorischer Vorschriften. Solche internen Vorschriften befassen sich im Idealfall mit folgenden Fragen:

- regelmäßige Unterrichtung aller Beschäftigten über Datensicherheitsvorschriften und ihre sich aus dem Datenschutzrecht ergebenden Verpflichtungen, vor allem ihre Pflicht zur Wahrung der Vertraulichkeit;
- eindeutige Verteilung der Verantwortlichkeiten und klare Abgrenzung der Zuständigkeiten bei der Datenverarbeitung, insbesondere im Hinblick auf Entscheidungen über die Verarbeitung personenbezogener Daten und die Übermittlung von Daten an Dritte oder betroffene Personen;
- Verwendung personenbezogener Daten nur aufgrund von Weisungen der zuständigen Person oder im Einklang mit allgemein geltenden Regeln;
- Schutz des Zugangs zu den Räumlichkeiten sowie zur Hard- und Software des Verantwortlichen oder Auftragsverarbeiters einschließlich Überprüfungen der Zugangsberechtigung;
- Gewährleistung, dass Genehmigungen zum Zugriff auf personenbezogene Daten von der zuständigen Person erteilt wurden, und Anforderung der entsprechenden Dokumentation;
- automatisierte Protokolle über den elektronischen Zugriff auf personenbezogene Daten und regelmäßige Überprüfungen dieser Protokolle durch die interne Aufsicht (weshalb sämtliche Datenverarbeitungstätigkeiten aufzuzeichnen sind);
- sorgfältige Dokumentation anderer Formen der Offenlegung (also nicht automatisierter Zugriff auf Daten), um beweisen zu können, dass keine gesetzeswidrigen Datenübermittlungen stattgefunden haben.

Ein Angebot an geeigneten Datensicherheitsschulungen und Kursen für Beschäftigte sind ebenfalls Beiträge zu wirksamen Sicherheitsvorkehrungen. Es sind ferner Überprüfungsverfahren einzurichten, damit gewährleistet ist, dass die geeigneten Maßnahmen nicht nur auf dem Papier bestehen, sondern

auch tatsächlich umgesetzt werden und sich in der Praxis bewähren (beispielsweise interne oder externe Audits).

Zu den Maßnahmen, mit denen ein Verantwortlicher oder Auftragsverarbeiter sein Sicherheitsniveau verbessern kann, gehören Datenschutzbeauftragte, Sicherheitsschulungen für Beschäftigte, regelmäßige Audits, Eindringungstests und Gütesiegel.

Beispiel: In der Rechtssache *I gegen Finnland*⁴⁴³ konnte die Beschwerdeführerin nicht beweisen, dass andere Beschäftigte des Krankenhauses, in dem sie arbeitete, rechtswidrig Einblick in ihre Patientenakte genommen hatten. Die innerstaatlichen Gerichte hatten daher ihre Klage wegen Verletzung ihres Rechts auf Datenschutz zurückgewiesen. Der EGMR kam zu dem Schluss, dass eine Verletzung von Artikel 8 EMRK vorlag, da das Registriersystem des Krankenhauses für Patientenakten „dergestalt war, dass es unmöglich war, rückwirkend die Verwendung von Patientenakten zu klären, da dort nur die fünf letzten Konsultationen vermerkt waren und diese Informationen nach Rückgabe der Akten an das Archiv gelöscht wurden“. Für den Gerichtshof bestand das entscheidende Element darin, dass das im Krankenhaus bestehende Aufbewahrungssystem eindeutig nicht im Einklang mit den Anforderungen des innerstaatlichen Rechts stand, eine Tatsache, denen die innerstaatlichen Gerichte nicht das gebührende Gewicht eingeräumt hatten.

Die EU hat die Richtlinie zur Netz- und Informationssicherheit (die NIS-Richtlinie) eingeführt,⁴⁴⁴ bei der es sich um das erste EU-weite Rechtsinstrument zur Cybersicherheit handelt. Die Richtlinie zielt einerseits auf die Verbesserung der Cybersicherheit auf nationaler Ebene ab, und andererseits auf die Ausdehnung der Zusammenarbeit innerhalb der EU. Darüber hinaus legt sie den Betreibern wesentlicher Dienste (darunter Betreibern in den Bereichen Energie, Gesundheitswesen, Bankwesen, Verkehr, digitale Infrastruktur, usw.) und den Anbietern digitaler Dienste Verpflichtungen in Bezug auf das Risikomanagement, die Gewährleistung der Sicherheit ihrer Netz- und Informationssysteme und die Meldung von Sicherheitsvorfällen auf.

443 EGMR, I / *Finnland*, Nr. 20511/03, 17. Juli 2008.

444 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194 vom 19. Juli 2016.

Ausblick

Im September 2017 schlug die Europäische Kommission den Entwurf einer Verordnung vor, die auf die Reform des Mandats der ENISA abzielte, um die in der NIS-Richtlinie begründeten neuen Befugnisse und Zuständigkeiten der Agentur zu berücksichtigen. Die vorgeschlagene Verordnung zielt darauf ab, die Aufgaben der ENISA auszubauen und ihre Rolle als „Referenz im EU Cybersicherheitsökosystem“ zu stärken.⁴⁴⁵ Die Grundsätze der DSGVO sollten von der vorgeschlagenen Verordnung unberührt bleiben. Durch die Präzisierung der erforderlichen Bestandteile der europäischen Cybersicherheitszertifizierungssysteme sollte die vorgeschlagene Verordnung auch die Sicherheit personenbezogener Daten stärken. Wie in Artikel 16 Absatz 8 der NIS-Richtlinie gefordert, schlug die Europäische Kommission parallel dazu im September 2017 einen Entwurf einer Durchführungsverordnung vor, in der die Parameter bestimmt sind, die Anbieter digitaler Dienste zur Gewährleistung der Sicherheit ihrer Netz- und Informationssysteme zu berücksichtigen haben. Zum Zeitpunkt der Abfassung des vorliegenden Handbuchs wurden diese beiden Vorschläge noch erörtert.

4.2.2. Vertraulichkeit

Im EU-Recht erkennt die DSGVO die Vertraulichkeit personenbezogener Daten als Bestandteil eines allgemeinen Grundsatzes an.⁴⁴⁶ Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste müssen Vertraulichkeit gewährleisten. Sie sind auch dazu verpflichtet, die Sicherheit ihrer Dienste zu gewährleisten.⁴⁴⁷

Beispiel: Eine Mitarbeiterin einer Versicherung erhält an ihrem Arbeitsplatz einen Anruf von jemandem, der sich als Kunde ausgibt und Informationen zu seinem Versicherungsvertrag möchte.

⁴⁴⁵ [Vorschlag](#) für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“), COM(2017)477, 13. September 2017, S. 6.

⁴⁴⁶ DSGVO, Artikel 5 Absatz 1 Buchstabe f.

⁴⁴⁷ Datenschutzrichtlinie für elektronische Kommunikation, Artikel 5 Absatz 1.

Aufgrund ihrer Verpflichtung, die Daten von Kunden vertraulich zu behandeln, muss die Angestellte zumindest minimale Sicherheitsvorkehrungen treffen, bevor sie personenbezogene Daten weitergibt. So könnte sie beispielsweise einen Rückruf an eine in der Kundenakte vermerkte Telefonnummer anbieten.

Gemäß Artikel 5 Absatz 1 Buchstabe f müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Gemäß Artikel 32 treffen der Verantwortliche und der Auftragsverarbeiter technische und organisatorische Maßnahmen, um ein hohes Schutzniveau zu gewährleisten. Diese Maßnahmen umfassen unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitung auf Dauer sicherzustellen, die Evaluierung und Überprüfung der Wirksamkeit der Maßnahmen und die Fähigkeit, die Verarbeitung bei einem physischen oder technischen Zwischenfall wiederherzustellen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung des Grundsatzes der Integrität und Vertraulichkeit nachzuweisen. Darüber hinaus sieht der den Verantwortlichen an den Auftragsverarbeiter bindende Vertrag gemäß Artikel 28 DSGVO vor, dass der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Die Vertraulichkeitspflicht gilt nicht für Situationen, in denen Daten einer Person in ihrer Eigenschaft als Privatperson und nicht als Angestellte eines Verantwortlichen oder Auftragsverarbeiters zur Kenntnis gelangen. In diesem Fall finden Artikel 32 und Artikel 28 DSGVO keine Anwendung, da die Verwendung personenbezogener Daten durch Privatpersonen vom Geltungsbereich der Verordnung ausgenommen ist; sie fällt dort unter die so genannte Ausnahmeregelung für familiäre Tätigkeiten.⁴⁴⁸ Diese Ausnahmeregelung für fami-

⁴⁴⁸ DSGVO, Artikel 2 Absatz 2 Buchstabe c.

liäre Tätigkeiten umfasst die Verarbeitung personenbezogener Daten „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“.⁴⁴⁹ Seit der Entscheidung des EuGH in der Rechtssache *Bodil Lindqvist*⁴⁵⁰ muss diese Ausnahme allerdings restriktiv ausgelegt werden, vor allem im Hinblick auf die Offenlegung von Daten. So gilt die Ausnahmeregelung für familiäre Tätigkeiten insbesondere nicht für die Weitergabe personenbezogener Daten an eine unbegrenzte Zahl von Empfängern im Internet und für die Datenverarbeitung unter beruflichen oder kommerziellen Aspekten (für nähere Einzelheiten zu der Rechtssache siehe die [Abschnitte 2.1.2, 2.2.2 und 2.3.1](#)).

Die „Vertraulichkeit der Kommunikation“ ist ein weiterer Aspekt der Vertraulichkeit, der *lex specialis* unterliegt. Die besonderen Vorschriften für die Sicherstellung der Vertraulichkeit elektronischer Kommunikation nach Maßgabe der ePrivacy-Richtlinie verlangen von den Mitgliedstaaten, dass sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Metadaten durch andere Personen als die Nutzer, oder wenn keine Einwilligung der Nutzer vorliegt, untersagen.⁴⁵¹ Das nationale Recht kann Ausnahmen von diesem Grundsatz ausschließlich aus Gründen der nationalen Sicherheit, der Landesverteidigung oder der Verhütung oder Feststellung von Straftaten zulassen, sofern diese Maßnahmen zur Erreichung der verfolgten Ziele notwendig und verhältnismäßig sind.⁴⁵² Dieselben Vorschriften werden unter der künftigen ePrivacy-Verordnung Anwendung finden, wobei der Anwendungsbereich des Rechtsakts zum Thema ePrivacy von öffentlich zugänglichen elektronischen Kommunikationsdiensten auch auf Kommunikation mittels Over-the-Top-Diensten (wie mobile Apps) ausgedehnt wird.

Im **Recht des Europarates** ist die Pflicht zur Wahrung der Vertraulichkeit im Begriff der Datensicherheit in Artikel 7 Absatz 1 des Modernisierten Übereinkommens Nr. 108 enthalten, der sich mit Datensicherheit befasst.

449 a.a.O.

450 EuGH, C-101/01, *Strafverfahren / Bodil Lindqvist*, 6. November 2003.

451 Datenschutzrichtlinie für elektronische Kommunikation, Artikel 5 Absatz 1.

452 a.a.O., Artikel 15 Absatz 1.

Für Auftragsverarbeiter bedeutet Vertraulichkeit, dass sie Daten ohne Genehmigung nicht gegenüber Dritten oder anderen Empfängern offenlegen dürfen. Für die Angestellten eines Verantwortlichen oder Auftragsverarbeiters bedeutet Vertraulichkeit, dass sie personenbezogene Daten nur im Einklang mit den Weisungen ihrer zuständigen Vorgesetzten verwenden dürfen.

Die Pflicht zur Wahrung der Vertraulichkeit muss in allen Verträgen zwischen Verantwortlichen und ihren Auftragsverarbeitern geregelt sein. Darüber hinaus müssen Verantwortliche und Auftragsverarbeiter für ihre Beschäftigten konkret eine Verpflichtung zur Wahrung der Vertraulichkeit festlegen; normalerweise geschieht dies mit Vertraulichkeitsklauseln in den Arbeitsverträgen der Beschäftigten.

Verstöße gegen die Verpflichtung zur Wahrung der Vertraulichkeit im Beruf sind in vielen EU-Mitgliedstaaten und Vertragsparteien des Modernisierten Übereinkommens Nr. 108 strafbar.

4.2.3. Meldungen von Verletzungen des Schutzes personenbezogener Daten

Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die verarbeitet wurden.⁴⁵³ Wenngleich neue Technologien wie die Verschlüsselung nun mehr Möglichkeiten für die Gewährleistung der Sicherheit der Verarbeitung bieten, sind Verletzungen des Schutzes personenbezogener Daten nach wie vor ein verbreitetes Phänomen. Die Ursachen für Verletzungen des Schutzes personenbezogener Daten können von unbeabsichtigten Fehlern von Unternehmensmitarbeitern bis hin zu externen Bedrohungen wie Hackern und cyberkriminellen Organisationen reichen.

Verletzungen personenbezogener Daten können sich als sehr nachteilig für die Privatsphäre und die Datenschutzrechte der Personen erweisen, die infolge der Verletzung die Kontrolle über ihre personenbezogenen Daten verlieren. Verletzungen können zu einem Identitätsdiebstahl oder -betrug, einem finanziellen

⁴⁵³ Datenschutz-Grundverordnung, Artikel 4 Absatz 12; Siehe auch Artikel-29-Datenschutzgruppe (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP250, 3. Oktober 2017, S. 8.

Verlust oder Sachschäden, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten und zu einer Schädigung des Rufs der betroffenen Person führen. In ihren *Guidelines on Personal data breach notification under Regulation 2016/679* erläutert die Artikel-29-Datenschutzgruppe, dass sich Verletzungen auf dreierlei Art auf die personenbezogenen Daten auswirken können: Offenlegung, Verlust und/oder Veränderung.⁴⁵⁴ Neben der in [Abschnitt 4.2](#) erläuterten Verpflichtung zum Treffen von Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, ist es ebenso wichtig, beim Auftreten einer Verletzung rechtzeitig und angemessen zu reagieren.

Aufsichtsbehörden und natürliche Personen sind sich des Auftretens einer Verletzung personenbezogener Daten oftmals nicht bewusst, was natürliche Personen daran hindert, Maßnahmen einzuleiten, um sich vor den negativen Folgen der Verletzung zu schützen. Zur Bekräftigung der Rechte der Einzelnen und zur Begrenzung der Auswirkungen von Verletzungen personenbezogener Daten, ordnen die **EU und der Europarat** den Verantwortlichen unter bestimmten Umständen eine Meldepflicht an.

Nach Maßgabe des Modernisierten Übereinkommens Nr. 108 des **Europarates** müssen die Vertragsparteien von den Verantwortlichen mindestens verlangen, Verletzungen personenbezogener Daten, die einen ernsthaften Eingriff in die Rechte der betroffenen Personen darstellen, der zuständigen Aufsichtsbehörde zu melden. Diese Meldung sollte „unverzüglich“ erfolgen.⁴⁵⁵

Im **EU-Recht** wurde ein detailliertes System zur Regelung des zeitlichen Ablaufs und des Inhalts der Meldungen eingerichtet.⁴⁵⁶ Demgemäß müssen Verantwortliche bestimmte Verletzungen personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihnen die Verletzung bekannt wurde, an die Aufsichtsbehörden melden. Sofern sie den Zeitrahmen von 72 Stunden überschreiten, so ist der Meldung eine Begründung für die Verzögerung beizufügen. Von der Meldepflicht befreit sind Verantwortliche nur dann, wenn sie nachweisen können, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der betreffenden Personen führt.

454 Artikel-29-Datenschutzgruppe (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP250, 3. Oktober 2017, S. 6.

455 Modernisiertes Übereinkommen Nr. 108, Artikel 7 Absatz 2, Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 64–66.

456 Datenschutz-Grundverordnung, Artikel 33 und 34.

Damit die Aufsichtsbehörde die erforderlichen Maßnahmen ergreifen kann, präzisiert die Verordnung das Mindestmaß der der Meldung beizufügenden Informationen.⁴⁵⁷ Die Meldung muss mindestens eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten und der Kategorien und ungefähren Zahlen der betroffenen Personen enthalten, sowie eine Beschreibung der möglichen Folgen der Verletzung und der vom Verantwortlichen ergriffenen Maßnahmen zur Behebung und Abmilderung ihrer Folgen. Darüber hinaus sollten der Name und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle bereitgestellt werden, um der Aufsichtsbehörde bei Bedarf die Einholung weiterer Informationen zu ermöglichen.

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigen die Verantwortlichen diese Personen (die betroffenen Personen) unverzüglich von der Verletzung.⁴⁵⁸ Die Benachrichtigung der betroffenen Personen enthält die Beschreibung der Verletzung des Schutzes personenbezogener Daten, muss in klarer und einfacher Sprache abgefasst sein und vergleichbare Informationen wie die Meldungen an die Aufsichtsbehörden enthalten. Unter bestimmten Umständen können die Verantwortlichen von der Verpflichtung zur Unterrichtung der betroffenen Personen von diesen Verletzungen befreit werden. Diese Ausnahmen finden Anwendung, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung. Seitens des Verantwortlichen nach der Verletzung ergriffene Maßnahmen zur Sicherstellung, dass der Schaden für die Rechte der betroffenen Personen nicht mehr besteht, können den Verantwortlichen ebenfalls von der Verpflichtung zur Unterrichtung der betroffenen Personen befreien. Sofern die Benachrichtigung für den Verantwortlichen schließlich mit einem unverhältnismäßigen Aufwand verbunden ist, können die betroffenen Personen auf anderem Wege wie durch eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme benachrichtigt werden.⁴⁵⁹

457 a.a.O., Artikel 33 Absatz 3.

458 a.a.O., Artikel 34.

459 a.a.O., Artikel 34 Absatz 3 Buchstabe c.

Die Verpflichtung zur Benachrichtigung der Aufsichtsbehörde und der betroffenen Personen über die Verletzungen des Schutzes personenbezogener Daten richtet sich an die Verantwortlichen. Verletzungen des Schutzes personenbezogener Daten können jedoch unabhängig davon auftreten, ob die Verarbeitung von einem Verantwortlichen oder von einem Auftragsverarbeiter durchgeführt wird. Aus diesem Grund ist es von wesentlicher Bedeutung, sicherzustellen, dass Auftragsverarbeiter ebenfalls zur Meldung von Verletzungen des Schutzes personenbezogener Daten verpflichtet sind. In diesem Fall müssen die Auftragsverarbeiter Verletzungen des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen melden.⁴⁶⁰ Im Anschluss daran obliegt dem Verantwortlichen nach Maßgabe der vorgenannten Vorschriften und innerhalb des genannten Zeitrahmens die Benachrichtigung der Aufsichtsbehörden und der betroffenen Personen.

4.3. Vorschriften über den Grundsatz der Verantwortlichkeit und über die Förderung der Einhaltung der Vorschriften

Kernpunkte

- Zur Gewährleistung des Grundsatzes der Verantwortlichkeit bei der Verarbeitung personenbezogener Daten führen die Verantwortlichen und die Auftragsverarbeiter Verzeichnisse aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, und stellen sie der Aufsichtsbehörde auf Anfrage zur Verfügung.
- Die DSGVO nennt mehrere Instrumente zur Förderung der Einhaltung der Vorschriften:
 - die in bestimmten Situationen erforderliche Benennung eines Datenschutzbeauftragten;
 - die Durchführung einer Folgenabschätzung vor Beginn von Verarbeitungstätigkeiten, die wahrscheinlich hohe Risiken für die Rechte und Freiheiten natürlicher Personen mit sich bringen;

⁴⁶⁰ a.a.O., Artikel 33 Absatz 2.

- vorherige Konsultation der zuständigen Aufsichtsbehörde, wenn aus der Folgenabschätzung hervorgeht, dass die Verarbeitung nicht einzudämmende Risiken birgt;
- Verhaltensregeln für Verantwortliche und Auftragsverarbeiter, die die Anwendung der Verordnung in verschiedenen Bereichen der Datenverarbeitung präzisieren;
- Zertifizierungsverfahren, Siegel und Prüfzeichen.
- Das Recht des Europarates schlägt im Modernisierten Übereinkommen Nr. 108 ähnliche Instrumente zur Förderung der Einhaltung der Vorschriften vor.

Der Grundsatz der Verantwortlichkeit ist zur Gewährleistung der Durchsetzung der Datenschutzvorschriften in Europa besonders wichtig. Der Verantwortliche ist für die Einhaltung der Datenschutzvorschriften verantwortlich und muss diese Einhaltung nachweisen können. Der Grundsatz der Verantwortlichkeit sollte jedoch nicht erst ins Spiel kommen, nachdem eine Verletzung stattgefunden hat. Die Verantwortlichen sind vielmehr auf allen Stufen der Datenverarbeitung proaktiv zur Befolgung angemessener Datenverwaltungsstrategien verpflichtet. Das europäische Datenschutzrecht verlangt von den Verantwortlichen die Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung und zum Nachweis, dass die Verarbeitung in Übereinstimmung mit dem Gesetz erfolgt. Zu diesen Maßnahmen zählt die Benennung eines Datenschutzbeauftragten, das Führen von Verzeichnissen und Dokumentationen im Zusammenhang mit der Verarbeitung und die Durchführung von Datenschutz-Folgenabschätzungen.

4.3.1. Datenschutzbeauftragte

Datenschutzbeauftragte (DSB) sind Personen, die datenverarbeitende Unternehmen über die Einhaltung der Datenschutzvorschriften beraten. Sie sind „ein Eckpfeiler der Rechenschaftspflicht“, da sie die Einhaltung der Vorschriften erleichtern und gleichzeitig als Vermittler zwischen den Aufsichtsbehörden, den betroffenen Personen und dem Unternehmen agieren, das sie benannt hat.

Im Recht des Europarates legt Artikel 10 Absatz 1 des Modernisierten Übereinkommens Nr. 108 den Verantwortlichen und Auftragsverarbeitern eine allgemeine Rechenschaftspflicht auf. Diese verlangt von den Verantwortlichen und Auftragsverarbeitern das Ergreifen aller geeigneten Maßnahmen zur Einhaltung der im Übereinkommen festgesetzten Datenschutzvorschriften und den Nachweis, dass die unter ihrer Aufsicht erfolgende Datenverarbeitung mit den Bestimmungen des Übereinkommens übereinstimmt. Obgleich das Übereinkommen die seitens der Verantwortlichen und Auftragsverarbeiter anzunehmenden konkreten Maßnahmen nicht präzisiert, geht aus dem erläuternden Bericht zum Modernisierten Übereinkommen Nr. 108 hervor, dass die Benennung eines DSB eine mögliche förderliche Maßnahme zum Nachweis der Einhaltung der Vorschriften wäre. Die DSB sollten mit allen erforderlichen Mitteln zur Erfüllung ihrer Aufträge ausgestattet werden.⁴⁶¹

Im Gegensatz zum Recht des Europarates liegt die Benennung eines DSB **im EU-Recht** nicht immer im Ermessen der Verantwortlichen und Auftragsverarbeiter, sondern ist unter bestimmten Bedingungen zwingend erforderlich. Die DSGVO erkennt die entscheidende Rolle des DSB im neuen Steuerungssystem an und enthält detaillierte Bestimmungen in Bezug auf die Benennung, die Stellung, die Pflichten und die Aufgaben des Beauftragten.⁴⁶²

In drei spezifischen Fällen ist die Benennung eines DSB laut DSGVO zwingend erforderlich: wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.⁴⁶³ Obgleich Begriffe wie „umfangreiche systematische Überwachung“ und „Kerntätigkeit“ in der Verordnung nicht definiert sind, hat die Artikel-29-Datenschutzgruppe Leitlinien in Bezug auf deren Interpretation herausgegeben.⁴⁶⁴

461 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 87.

462 Datenschutz-Grundverordnung, Artikel 37–39.

463 a.a.O., Artikel 37 Absatz 1.

464 Artikel-29-Datenschutzgruppe (2017), *Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)*, WP 243 rev.01, zuletzt überarbeitet und angenommen am 5. April 2017.

Beispiel: Social Media-Unternehmen und Suchmaschinen werden wahrscheinlich als Verantwortliche betrachtet, deren Verarbeitungsvorgänge die umfangreiche regelmäßige und systematische Überwachung der betroffenen Personen erfordern. Das Geschäftsmodell solcher Unternehmen gründet auf der Verarbeitung großer Mengen personenbezogener Daten und sie erwirtschaften bedeutende Erträge, indem sie gezielte Werbedienstleistungen anbieten und Unternehmen erlauben, auf ihren Webseiten Werbung zu schalten. Gezielte Werbung ist eine Form der Veröffentlichung von Werbeanzeigen auf Grundlage demographischer Kriterien und der früheren Kaufhistorie oder des früheren Kaufverhaltens. Folglich erfordert sie die systematische Überwachung der Online-Gewohnheiten und des Online-Verhaltens der betroffenen Personen.

Beispiel: Ein Krankenhaus und eine Krankenkasse sind typische Beispiele für Verantwortliche, deren Tätigkeiten in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten bestehen. Daten, die Informationen in Bezug auf die Gesundheit einer Person offenlegen, stellen sowohl im EU-Recht als auch im Recht des Europarates besondere Kategorien personenbezogener Daten dar, die erhöhtes Schutzes bedürfen. Das EU-Recht erkennt darüber hinaus auch genetische und biometrische Daten als besondere Datenkategorien an. Da medizinische Einrichtungen und Versicherungsunternehmen solche Daten in großem Umfang verarbeiten, sind sie nach Maßgabe der DSGVO zur Benennung eines Datenschutzbeauftragten verpflichtet.

Überdies sieht Artikel 37 Absatz 4 DSGVO vor, dass der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, in anderen als den drei in Artikel 37 Absatz 1 DSGVO zwingend erforderlichen Fällen einen Datenschutzbeauftragten benennen können; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen.

Alle übrigen Einrichtungen sind rechtlich nicht zur Benennung eines DSB verpflichtet. Die DSGVO sieht jedoch vor, dass sich Verantwortliche und Auftragsverarbeiter freiwillig für die Benennung eines DSB entscheiden können, und

räumt den Mitgliedstaaten auch die Möglichkeit ein, eine solche Benennung für mehr als die in der Verordnung vorgesehenen Arten von Organisationen zwingend erforderlich zu machen.⁴⁶⁵

Sobald ein Verantwortlicher einen DSB benennt, stellt er sicher, dass dieser im Unternehmen „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird“.⁴⁶⁶ DSB sollten beispielsweise in die Beratung im Zusammenhang mit der Durchführung von Datenschutz-Folgenabschätzungen und in die Erstellung und Führung von Verzeichnissen der Verarbeitungstätigkeiten in einem Unternehmen eingebunden werden. Zur wirksamen Wahrnehmung ihrer Aufgaben sind die DSB seitens der Verantwortlichen und Auftragsverarbeiter mit den erforderlichen Mitteln, einschließlich Finanzmitteln, Infrastrukturen und Geräten auszustatten. Zu den weiteren Anforderungen zählen, dass den DSB genügend Zeit für die Erfüllung ihrer Aufgaben und eine kontinuierliche Fortbildung gewährt wird, damit sie ihre Fähigkeiten ausbauen und sich in Bezug auf sämtliche Entwicklungen im Datenschutzrecht auf dem aktuellen Stand halten können.⁴⁶⁷

Die DSGVO setzt einige grundlegende Garantien fest, um sicherzustellen, dass die DSB in vollständiger Unabhängigkeit handeln. Verantwortliche und Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben in Bezug auf den Datenschutz keine Anweisungen vom Unternehmen einschließlich dessen höchster Managementebene erhält. Überdies dürfen sie wegen der Erfüllung ihrer Aufgaben in keiner Weise abberufen oder benachteiligt werden.⁴⁶⁸ Betrachten wir beispielsweise einen Fall, in dem der DSB einem Verantwortlichen oder Auftragsverarbeiter zur Durchführung einer Datenschutz-Folgenanalyse rät, da die Verarbeitung seiner Ansicht nach voraussichtlich ein hohes Risiko für die betroffenen Personen zur Folge hat. Das Unternehmen ist mit dem Ratschlag des DSB nicht einverstanden, erachtet ihn als unbegründet und entscheidet folglich, keine Folgenabschätzung durchzuführen. Das Unternehmen kann den Ratschlag zwar ignorieren, den DSB für dessen Erteilung jedoch nicht abberufen oder benachteiligen.

465 Datenschutz-Grundverordnung, Artikel 37 Absatz 3 und 4.

466 a.a.O., Artikel 38 Absatz 1.

467 Artikel-29-Datenschutzgruppe (2017), *Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)*, WP 243 rev.01, zuletzt überarbeitet und angenommen am 5. April 2017, Absatz 3.2.

468 Datenschutz-Grundverordnung, Artikel 38 Absatz 2 und 3.

Die Aufgaben und Pflichten des DSB sind ausführlich in Artikel 39 DSGVO dargelegt. Diese umfassen das Erfordernis zur Unterrichtung und Beratung der Unternehmen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer gesetzlichen Pflichten, sowie die Überwachung der Einhaltung der Datenschutzvorschriften der EU und der Mitgliedstaaten durch die Durchführung von Überprüfungen und Schulungen der an den Verarbeitungsvorgängen beteiligten Mitarbeiter. Die DSB sind auch zur Zusammenarbeit mit der Aufsichtsbehörde verpflichtet und handeln als deren Anlaufstelle in mit der Datenverarbeitung zusammenhängenden Angelegenheiten wie beispielsweise einer Verletzung des Schutzes personenbezogener Daten.

In Bezug auf die seitens der Organe und Einrichtungen der EU verarbeiteten personenbezogenen Daten sieht die Verordnung (EG) Nr. 45/2001 vor, dass jedes Organ und jede Einrichtung der Gemeinschaft einen DSB bestellt. Der DSB ist damit betraut, zu gewährleisten, dass die Bestimmungen der Verordnung in den Organen und Einrichtungen der EU richtig angewandt werden, und die betroffenen Personen sowie die für die Verarbeitung Verantwortlichen über ihre Rechte und Pflichten unterrichtet sind.⁴⁶⁹ Darüber hinaus kommt der DSB Anfragen des EDSB nach und arbeitet mit diesem bei Bedarf zusammen. Ähnlich wie die DSGVO enthält auch die Verordnung (EG) Nr. 45/2001 Bestimmungen in Bezug auf die Unabhängigkeit der DSB bei der Durchführung ihrer Aufgaben und das Erfordernis zu deren Ausstattung mit dem erforderlichen Personal und den erforderlichen Mitteln.⁴⁷⁰ Die DSB sind vor der Durchführung von Verarbeitungsvorgängen seitens eines Organs oder einer Einrichtung der EU (oder seitens einer Abteilung dieser Einrichtungen) darüber zu unterrichten und führen ein Register aller gemeldeten Verarbeitungen.⁴⁷¹

4.3.2. Verzeichnis von Verarbeitungstätigkeiten

Um die Einhaltung der Vorschriften nachweisen zu können und zur Rechenschaft gezogen werden zu können, sind Unternehmen oft gesetzlich zur Dokumentation und Aufzeichnung ihrer Tätigkeiten verpflichtet. Ein wichtiges Beispiel in diesem Zusammenhang sind das Steuerrecht und die Wirtschaftsprüfung, die alle Unternehmen zum Führen umfangreicher Dokumentationen

469 Siehe Artikel 24 Absatz 1 der Verordnung (EG) Nr. 45/2001 für die vollständige Liste der Aufgaben der DSB.

470 Verordnung (EG) Nr. 45/2001, Artikel 24 Absatz 6 und 7.

471 a.a.O., Artikel 25 und 26.

und Verzeichnisse verpflichten. Die Festsetzung ähnlicher Erfordernisse in anderen Rechtsbereichen und insbesondere im Datenschutzrecht ist ebenfalls wichtig, da das Führen von Verzeichnissen ein wesentliches Instrument zur Erleichterung der Einhaltung der Datenschutzvorschriften darstellt. Das **EU-Recht** sieht demnach vor, dass Verantwortliche oder deren Vertreter ein Verzeichnis der Verarbeitungstätigkeiten führen, die ihrer Verantwortung unterliegen.⁴⁷² Durch diese Verpflichtung soll sichergestellt werden, dass die Aufsichtsbehörden bei Bedarf über die erforderliche Dokumentation zur Bestätigung der Rechtmäßigkeit der Verarbeitung verfügen.

Zu den zu dokumentierenden Informationen zählen:

- der Name und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie des DSB;
- die Zwecke der Verarbeitung;
- eine Beschreibung der mit der Verarbeitung verbundenen Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- Informationen über die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
- Informationen darüber, ob personenbezogene Daten an Drittländer oder internationale Organisationen übermittelt worden sind oder noch übermittelt werden;
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Kategorien personenbezogener Daten, sowie ein Überblick über die zur Gewährleistung der Sicherheit der Verarbeitung angenommenen technischen Maßnahmen.⁴⁷³

Die in der DSGVO enthaltene Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten betrifft nicht nur Verantwortliche, sondern auch

⁴⁷² Datenschutz-Grundverordnung, Artikel 30.

⁴⁷³ a.a.O., Artikel 30 Absatz 1.

Auftragsverarbeiter. Dies stellt eine wichtige Entwicklung dar, da vor der Annahme der Verordnung in erster Linie der zwischen dem Verantwortlichen und dem Auftragsverarbeiter abgeschlossene Vertrag die Pflichten des Auftragsverarbeiters enthielt. Dessen Pflicht zum Führen eines Verzeichnisses ist nun unmittelbar im Rahmen des Gesetzes vorgesehen.

Die DSGVO sieht eine Ausnahme von dieser Pflicht vor. Das Erfordernis zum Führen eines Verzeichnisses gilt nicht für Unternehmen oder Einrichtungen (Verantwortlicher oder Auftragsverarbeiter), die weniger als 250 Mitarbeiter beschäftigen. Diese Ausnahme unterliegt jedoch den Voraussetzungen, dass die betreffende Einrichtung keine Verarbeitung vornimmt, die voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat, dass die Verarbeitung nur gelegentlich erfolgt und nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Durch das Führen eines Verzeichnisses von Verarbeitungstätigkeiten sollten die Verantwortlichen und die Auftragsverarbeiter zum Nachweis der Einhaltung der Verordnung in der Lage sein. Darüber hinaus sollte es den Aufsichtsbehörden die Überwachung der Rechtmäßigkeit der Verarbeitung ermöglichen. Sofern eine Aufsichtsbehörde um Zugang zu diesen Verzeichnissen ersucht, sind die Verantwortlichen und die Auftragsverarbeiter zu deren Bereitstellung und zur Zusammenarbeit verpflichtet.

4.3.3. Datenschutz-Folgenabschätzung und vorherige Konsultation

Die Verarbeitungsvorgänge weisen einige Risiken für die Rechte der Personen auf. Personenbezogene Daten können verloren gehen, gegenüber Unbefugten offengelegt oder auf unrechtmäßige Weise verarbeitet werden. Die Risiken unterscheiden sich natürlich in Abhängigkeit von der Art und dem Umfang der Verarbeitung. Umfangreiche Vorgänge, die die Verarbeitung sensibler Daten umfassen, weisen beispielsweise einem wesentlich höheren Risikograd für die betroffenen Personen auf als potenzielle Risiken, die auftreten, wenn ein kleines Unternehmen die Anschriften und privaten Telefonnummern seiner Beschäftigten verarbeitet.

Angesichts des Aufkommens neuer Technologien und der zunehmenden Komplexität der Verarbeitung müssen sich die Verantwortlichen mit derartigen

Risiken vor Beginn des Verarbeitungsvorgangs durch die Untersuchung der voraussichtlichen Auswirkungen der beabsichtigten Verarbeitung auseinandersetzen. Dadurch können die Unternehmen diese Risiken bereits im Vorfeld ordnungsgemäß ermitteln, angehen und eindämmen, was die Wahrscheinlichkeit einer negativen Auswirkung der Verarbeitung auf die Personen erheblich begrenzt.

Datenschutz-Folgenabschätzungen sind **sowohl im Recht des Europarates als auch im EU-Recht** vorgesehen. Im Rechtsrahmen des Europarates verpflichtet Artikel 10 des Modernisierten Übereinkommens Nr. 108 die Vertragsparteien zur Sicherstellung, dass Verantwortliche und Auftragsverarbeiter „die wahrscheinlichen Auswirkungen der beabsichtigten Datenverarbeitung auf die Rechte und Grundfreiheiten der betroffenen Personen vor Beginn dieser Verarbeitung untersuchen“, und im Anschluss an die Abschätzung die Verarbeitung derart gestalten, dass sie die mit der Verarbeitung verbundenen Risiken verhindern oder auf ein Mindestmaß reduzieren.

Im EU-Recht wird den Verantwortlichen eine ähnliche, detailliertere Pflicht auferlegt, die unter den Anwendungsbereich der DSGVO fällt. Artikel 35 sieht vor, dass eine Folgenabschätzung durchzuführen ist, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die Verordnung definiert nicht, wie die Eintrittswahrscheinlichkeit eines Risikos abzuschätzen ist, gibt hingegen an, worin diese Risiken bestehen könnten.⁴⁷⁴ Sie enthält eine Liste von als mit hohem Risiko verbunden betrachteten Verarbeitungsvorgängen, für die eine vorherige Folgenabschätzung besonders erforderlich ist. Dies betrifft insbesondere Fälle, in denen:

- die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte dieser Personen verarbeitet werden (Profiling);
- sensible Daten oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten in großem Umfang verarbeitet werden;
- die Verarbeitung die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche beinhaltet.

⁴⁷⁴ Datenschutz-Grundverordnung, Erwägungsgrund 75.

Die Aufsichtsbehörden erstellen eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlichen diese. Sie können des Weiteren eine Liste der von dieser Pflicht befreiten Verarbeitungsvorgänge erstellen.⁴⁷⁵

Wenn eine Folgenabschätzung erforderlich ist, bewerten die Verantwortlichen die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung und deren mögliche Risiken für die Rechte der Personen. Die Folgenabschätzung enthält darüber hinaus die geplanten Sicherheitsvorkehrungen zur Bewältigung der ermittelten Risiken. Die Erstellung der Listen erfordert die Zusammenarbeit der Aufsichtsbehörden der Mitgliedstaaten untereinander und deren Zusammenarbeit mit dem Europäischen Datenschutzausschuss. Dadurch wird in Bezug auf die eine Folgenabschätzung erfordernden Verarbeitungsvorgänge EU-weit eine einheitliche Vorgehensweise gewährleistet und die Verantwortlichen sind unabhängig von ihrem Standort denselben Erfordernissen unterworfen.

Sofern sich im Anschluss an eine Folgenabschätzung herausstellt, dass die Verarbeitung ein hohes Risiko für die Rechte der Personen zur Folge hat und keine Maßnahmen zur Eindämmung des Risikos getroffen wurden, konsultiert der Verantwortliche vor Beginn des Verarbeitungsvorgangs die zuständige Aufsichtsbehörde.⁴⁷⁶

Die Artikel-29-Datenschutzgruppe hat Leitlinien zur Datenschutz-Folgenabschätzung und zur Beantwortung der Frage herausgegeben, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“.⁴⁷⁷ Sie arbeitete die nachstehenden neun Kriterien aus, die helfen sollen, zu bestimmen, ob eine Datenschutz-Folgenabschätzung im jeweiligen Fall erforderlich ist:⁴⁷⁸ (1) Bewerten oder Einstufen; (2) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung; (3) Systematische Überwachung; (4) Vertrauliche Daten; (5) Datenverarbeitung in großem Umfang; (6) Datensätze, die abgeglichen oder zusammengeführt

475 a.a.O., Artikel 35 Absatz 4 und 5.

476 a.a.O., Artikel 36 Absatz 1; Artikel-29-Datenschutzgruppe (2017), *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“*, WP 248 rev.01, Brüssel, 4. Oktober 2017.

477 Artikel-29-Datenschutzgruppe (2017), *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“*, WP 248 rev.01, Brüssel, 4. Oktober 2017.

478 a.a.O., S. 9–11.

wurden; (7) Daten zu schutzbedürftigen Betroffenen; (8) Innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen; (9) Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert“. Die Artikel-29-Datenschutzgruppe führte die Daumenregel ein, wonach Verarbeitungsvorgänge, die weniger als zwei der genannten Kriterien erfüllen, niedrigere Risikostufen darstellen und keiner Datenschutz-Folgenabschätzung bedürfen, wohingegen Verarbeitungsvorgänge, die mindestens zwei Kriterien erfüllen, einer solchen Abschätzung bedürfen. Für den Fall, dass unklar ist, ob eine Datenschutz-Folgenabschätzung erforderlich ist, empfiehlt die Artikel-29-Datenschutzgruppe die Durchführung einer solchen Abschätzung, weil „den für die Verarbeitung Verantwortlichen damit ein hilfreiches Instrument für die Einhaltung der Datenschutzgesetze zur Verfügung steht“.⁴⁷⁹ Wenn eine neue Datenverarbeitungstechnologie eingeführt wird, ist es wichtig, eine Datenschutz-Folgenabschätzung durchzuführen.⁴⁸⁰

4.3.4. Verhaltensregeln

Verhaltensregeln sind für den Einsatz in verschiedenen Wirtschaftssektoren bestimmt, um die Anwendung der DSGVO in diesen spezifischen Sektoren zu erläutern und zu präzisieren. Für Verantwortliche und Auftragsverarbeiter kann die Erstellung solcher Regeln zu einer deutlich verbesserten Einhaltung der Vorschriften führen und die Umsetzung der EU-Datenschutzvorschriften verbessern. Dank des Fachwissens der Angehörigen des jeweiligen Sektors können Lösungen gefunden werden, die praxisnah sind und daher wahrscheinlich auch befolgt werden. Die DSGVO erkennt die Bedeutung solcher Regeln für die wirksame Anwendung des Datenschutzgesetzes an und appelliert an die Mitgliedstaaten, die Aufsichtsbehörden, die Kommission und den Europäischen Datenschutzausschuss, die Ausarbeitung von Verhaltensregeln zu fördern, die EU-weit zur ordnungsgemäßen Anwendung der Verordnung beitragen sollen.⁴⁸¹ Die Regeln könnten die Anwendung der Verordnung in spezifischen Sektoren präzisieren und Themen wie die Erhebung personenbezogener Daten, die den betroffenen Personen und der Öffentlichkeit zu übermittelnden Informationen und die Ausübung der Rechte der betroffenen Personen umfassen.

⁴⁷⁹ a.a.O., S. 9.

⁴⁸⁰ a.a.O.

⁴⁸¹ Datenschutz-Grundverordnung, Artikel 40 Absatz 1.

Zur Gewährleistung der Übereinstimmung der Verhaltensregeln mit den im Rahmen der DSGVO festgesetzten Vorschriften, sind diese vor ihrer Annahme der zuständigen Aufsichtsbehörde vorzulegen. Im Anschluss daran gibt die Aufsichtsbehörde eine Stellungnahme darüber ab, ob der vorgelegte Entwurf der Verhaltensregeln die Einhaltung der Verordnung unterstützt und genehmigt die Verhaltensregeln, wenn sie der Auffassung ist, dass sie geeignete Garantien bieten.⁴⁸² Die Aufsichtsbehörden veröffentlichen die genehmigten Verhaltensregeln und die Kriterien, auf die ihre Genehmigung gründete. Bezieht sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so legt die zuständige Aufsichtsbehörde – bevor sie den Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung genehmigt – ihn dem Europäischen Datenschutzausschuss vor, der zu der Frage Stellung nimmt, ob sie mit der DSGVO vereinbar sind. Die Kommission kann im Wege von Durchführungsrechtsakten beschließen, dass die ihr übermittelten genehmigten Verhaltensregeln allgemeine Gültigkeit in der Union besitzen.

Die Einhaltung von Verhaltensregeln ist sowohl für die betroffenen Personen als auch für die Verantwortlichen und Auftragsverarbeiter mit bedeutenden Vorteilen verbunden. Derartige Verhaltensregeln bieten eine detaillierte Anleitung, die die gesetzlichen Anforderungen an die spezifischen Sektoren anpasst und die Transparenz der Verarbeitungstätigkeiten unterstützt. Die Verantwortlichen und Auftragsverarbeiter können die Einhaltung der Verhaltensregeln darüber hinaus auch als nachweislichen Beleg für ihre Einhaltung der Vorschriften des EU-Rechts und als Mittel zur Ankurbelung ihres öffentlichen Ansehens als Einrichtung verwenden, die den Datenschutz im Zuge ihrer Tätigkeiten priorisiert und sich zu dessen Einhaltung verpflichtet. Genehmigte Verhaltensregeln können zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen als geeignete Garantien für die Übermittlung von Daten an Drittländer verwendet werden. Zur Sicherstellung, dass Einrichtungen, die Verhaltensregeln befolgen, diese auch tatsächlich einhalten, kann eine spezielle Stelle ernannt werden (die von der zuständigen Aufsichtsbehörde akkreditiert wurde), die die Einhaltung der Verhaltensregeln überwacht und sicherstellt. Zur wirksamen Erfüllung ihrer Aufgaben muss diese Stelle unabhängig sein, über nachweisliches Fachwissen hinsichtlich der durch die Verhaltensregeln

482 a.a.O., Artikel 40 Absatz 5.

geregelten Themen verfügen und transparente Verfahren und Strukturen aufweisen, mit denen sie Beschwerden über Verletzungen der Verhaltensregeln nachgeht.⁴⁸³

Im **Recht des Europarates** sieht das Modernisierte Übereinkommen Nr. 108 vor, dass das durch nationales Recht garantierte Datenschutzniveau durch freiwillige Regulierungsmaßnahmen wie Verhaltenskodizes oder Berufsordnungen zweckmäßig verstärkt werden kann. Dabei handelt es sich nach Maßgabe des Modernisierten Übereinkommens Nr. 108 jedoch lediglich um freiwillige Maßnahmen, von denen keinerlei rechtliche Verpflichtung zu deren Einrichtung abgeleitet werden kann, wenngleich dies empfehlenswert ist, und solche Maßnahmen sind für sich genommen nicht ausreichend, um die vollständige Einhaltung des Übereinkommens zu gewährleisten.⁴⁸⁴

4.3.5. Zertifizierung

Zusätzlich zu den Verhaltensregeln sind Zertifizierungsverfahren, Datenschutzsiegel und Prüfzeichen weitere Mittel, durch die Verantwortliche und Auftragsverarbeiter ihre Einhaltung der DSGVO nachweisen können. Zu diesem Zweck sieht die Verordnung ein freiwilliges Zertifizierungssystem vor, in dessen Rahmen bestimmte Stellen oder Aufsichtsbehörden Zertifizierungen erteilen können. Verantwortliche und Auftragsverarbeiter, die sich für die Einhaltung eines Zertifizierungsverfahrens entscheiden, können mehr Sichtbarkeit und Glaubwürdigkeit gewinnen, da es Zertifizierungen, Siegel und Prüfzeichen den betroffenen Personen ermöglichen, das Schutzniveau einer Einrichtung bei der Datenverarbeitung schnell zu beurteilen. Wichtig ist auch, dass die Tatsache, dass ein Verantwortlicher oder Auftragsverarbeiter eine solche Zertifizierung besitzt, dessen Pflichten und Verantwortungen in Bezug auf die Einhaltung sämtlicher Erfordernisse der Verordnung in keiner Weise verringert.

⁴⁸³ a.a.O., Artikel 41 Absatz 1 und 2.

⁴⁸⁴ Ad-hoc-Ausschuss Datenschutz (CAHDATA), *Erläuternder Bericht zum Modernisierten Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten*, Absatz 33.

4.4. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Datenschutz durch Technikgestaltung

Das **EU-Recht** schreibt vor, dass der Verantwortliche Maßnahmen zur wirksamen Umsetzung der Datenschutzgrundsätze trifft und die notwendigen Garantien aufnimmt, um den Anforderungen der Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.⁴⁸⁵ Diese Maßnahmen sollten sowohl zum Zeitpunkt der Verarbeitung als auch zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung getroffen werden. Der Verantwortliche trifft diese Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs und der Zwecke der Verarbeitung personenbezogener Daten sowie der Risiken und Schwere für die Rechte und Freiheiten der betroffenen Person.⁴⁸⁶

Das **Recht des Europarates** schreibt vor, dass Verantwortliche und Auftragsverarbeiter vor Beginn der Verarbeitung die wahrscheinlichen Auswirkungen der Verarbeitung personenbezogener Daten auf die Rechte und Freiheiten der betroffenen Personen beurteilen. Darüber hinaus sind Verantwortliche und Auftragsverarbeiter dazu verpflichtet, die Datenverarbeitung derart zu gestalten, dass das Risiko des Eingriffs in diese Rechte und Freiheiten verhindert oder minimiert wird; zudem sind sie verpflichtet, technische und organisatorische Maßnahmen einzuführen, die während aller Stufen der Datenverarbeitung die Implikationen des Rechts auf den Schutz personenbezogener Daten berücksichtigen.⁴⁸⁷

485 Datenschutz-Grundverordnung, Artikel 25 Absatz 1.

486 Siehe Artikel-29-Datenschutzgruppe (2017), *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“*, WP 248 rev.01, 4. Oktober 2017. Siehe auch ENISA (2015), *Privacy and Data Protection by Design—from policy to engineering*, 12. Januar 2015.

487 Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 2 und 3; Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 89.

Datenschutz durch datenschutzfreundliche Voreinstellungen

Das **EU-Recht** schreibt vor, dass der Verantwortliche geeignete Maßnahmen trifft, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für die jeweiligen Zwecke erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.⁴⁸⁸ Eine derartige Maßnahme muss beispielsweise gewährleisten, dass nicht alle Beschäftigten des Verantwortlichen Zugang zu den personenbezogenen Daten der betroffenen Person haben. Eine weitere Anleitung lieferte der EDSB im *Necessity Toolkit*.⁴⁸⁹

Das **Recht des Europarates** schreibt vor, dass Verantwortliche und Auftragsverarbeiter technische und organisatorische Maßnahmen zur Prüfung der Auswirkungen des Rechts auf Datenschutz treffen und technische und organisatorische Maßnahmen einführen, die während aller Stufen der Datenverarbeitung die Implikationen des Rechts auf den Schutz personenbezogener Daten berücksichtigen.⁴⁹⁰

2016 veröffentlichte die ENISA einen Bericht über die verfügbaren Instrumente und Dienstleistungen im Bereich des Datenschutzes.⁴⁹¹ Diese Beurteilung enthält unter anderem ein Verzeichnis der Kriterien und Parameter, die Indikatoren für gute oder schlechte Datenschutzpraktiken darstellen. Während sich einige Kriterien wie der Einsatz von Pseudonymisierung und genehmigten Zertifizierungsverfahren unmittelbar auf die Bestimmungen der DSGVO beziehen, liefern andere innovative Initiativen für die Gewährleistung von Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen. Das Kriterium der Benutzerfreundlichkeit beispielsweise bezieht sich zwar nicht unmittelbar auf den Datenschutz, kann diesen jedoch verbessern, da es die großflächigere Einführung eines Instruments oder einer Dienstleistung im Bereich Datenschutz ermöglichen kann. Datenschutzinstrumente, die in der Praxis schlecht umsetzbar sind, werden von der breiten Öffentlichkeit selbst dann nur in sehr geringem Maße eingesetzt, wenn

488 Datenschutz-Grundverordnung, Artikel 25 Absatz 2.

489 Europäischer Datenschutzbeauftragter (EDSB), (2017), *Necessity Toolkit*, Brüssel, 11. April 2017.

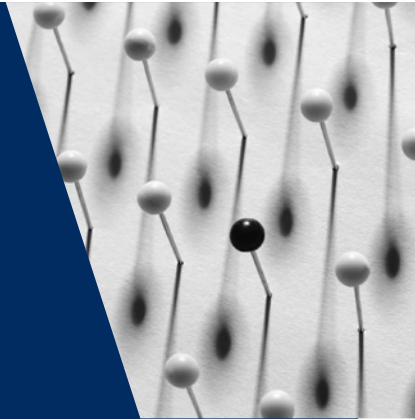
490 Modernisiertes Übereinkommen Nr. 108, Artikel 10 Absatz 3 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 29.

491 ENISA, *PEs controls matrix: A systematic approach for assessing online and mobile privacy tools*, 20. Dezember 2016.

sie sehr hohe Datenschutzgarantien bieten. Darüber hinaus ist das Kriterium der Reife und Stabilität des Datenschutzinstruments von entscheidender Bedeutung, das angibt, wie sich ein Instrument im Laufe der Zeit entwickelt und auf bestehende oder neue Herausforderungen im Zusammenhang mit dem Datenschutz reagiert. Andere Datenschutztechnologien, wie beispielsweise im Zusammenhang mit sicherer Kommunikation, umfassen die Ende-zu-Ende-Verschlüsselung (eine Kommunikationsart, bei der nur die Kommunikationspartner die Nachrichten lesen können), die Client-zu-Server-Verschlüsselung (Verschlüsselung des zwischen einem Client und einem Server errichteten Kommunikationskanals), die Authentifizierung (Prüfung der Identitäten der Kommunikationsparteien) und die anonyme Kommunikation (kein Dritter kann die Kommunikationsparteien identifizieren).

5

Unabhängige Aufsicht



EU	Behandelte Themen	Europarat
Die Charta, Artikel 8 Absatz 3 Vertrag über die Arbeitsweise der EU, Artikel 16 Absatz 2 DSGVO, Artikel 51–59 EuGH, C-518/07, <i>Europäische Kommission / Bundesrepublik Deutschland</i> [GK], 2010 EuGH, C-614/10, <i>Europäische Kommission / Republik Österreich</i> [GK], 2012 EuGH, C-288/12, <i>Europäische Kommission / Ungarn</i> [GK], 2014 EuGH, C-362/14, <i>Maximillian Schrems / Data Protection Commissioner</i> [GK], 2015	Aufsichtsbehörden	Modernisiertes Übereinkommen Nr. 108, Artikel 15
DSGVO, Artikel 60–67	Zusammenarbeit zwischen den Aufsichtsbehörden	Modernisiertes Übereinkommen Nr. 108, Artikel 16–21
DSGVO, Artikel 68–76	Europäischer Datenschutzausschuss	

Kernpunkte

- Die unabhängige Aufsicht ist ein wesentlicher Bestandteil des europäischen Datenschutzrechts und in Artikel 8 Absatz 3 der Charta verankert.
- Um einen wirksamen Datenschutz zu gewährleisten, müssen nach einzelstaatlichem Recht unabhängige Aufsichtsbehörden eingerichtet werden.
- Aufsichtsbehörden müssen in völliger Unabhängigkeit handeln, die im Gründungsrechtsakt gewährleistet wird und in der jeweiligen Organisationsstruktur der Aufsichtsbehörde zum Ausdruck kommen muss.
- Aufsichtsbehörden haben spezifische Befugnisse und Aufgaben. Dazu zählen unter anderem:
 - den Datenschutz auf nationaler Ebene zu überwachen und zu fördern;
 - betroffene Personen und Verantwortliche sowie die Regierung und die breite Öffentlichkeit zu beraten;
 - Beschwerden entgegenzunehmen und den betroffenen Personen bei mutmaßlichen Verletzungen von Datenschutzrechten zur Seite zu stehen;
 - Verantwortliche und Auftragsverarbeiter zu beaufsichtigen.
- Aufsichtsbehörden haben auch die Befugnis, bei Bedarf zu intervenieren, durch:
 - Verwarnungen, Abmahnungen oder sogar Verhängung von Geldstrafen gegen Verantwortliche und Auftragsverarbeiter;
 - Anordnung der Berichtigung, Sperrung oder Löschung von Daten;
 - Verhängung eines Verarbeitungsverbots oder einer Geldbuße;
 - Anrufung der Gerichte.
- Da die Verarbeitung personenbezogener Daten häufig Verantwortliche, Auftragsverarbeiter und betroffene Personen einbezieht, die in verschiedenen Staaten ansässig sind, sind Aufsichtsbehörden bei grenzüberschreitenden Fragen zur gegenseitigen Zusammenarbeit verpflichtet, um den wirksamen Schutz der Personen in Europa sicherzustellen.
- In der EU führt die DSGVO für grenzüberschreitende Verarbeitungsfälle den sogenannten „One-Stop-Shop-Mechanismus“ ein. Einige Unternehmen führen die grenzüberschreitende Verarbeitung personenbezogener Daten aufgrund der Tätigkeiten von Niederlassungen in mehr als einem Mitgliedstaat oder im Rahmen der Tätigkeiten einer einzelnen Niederlassung in der Union, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat. Nach Maßgabe des „One-Stop-Shop“ haben es solche

Unternehmen nur mit einer nationalen Datenschutzaufsichtsbehörde als zentralen Ansprechpartner zu tun.

- Ein Verfahren der Zusammenarbeit und Kohärenz ermöglicht eine koordinierte Vorgehensweise aller in den Fall verwickelten Aufsichtsbehörden. Die federführende Aufsichtsbehörde, bei der es sich um die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung handelt, unterbreitet ihren Beschlussentwurf den anderen betroffenen Aufsichtsbehörden und beratschlagt ihn mit diesen.
- Ebenso wie die gegenwärtige Artikel-29-Datenschutzgruppe, werden die Aufsichtsbehörde jedes Mitgliedstaats und der Europäische Datenschutzbeauftragte Bestandteil des Europäischen Datenschutzausschusses.
- Zu den Aufgaben des Europäischen Datenschutzausschusses zählen beispielsweise die Überwachung der ordnungsgemäßen Anwendung der Verordnung, die Beratung der Kommission in Bezug auf die maßgeblichen Fragen und die Bereitstellung von Stellungnahmen, Leitlinien oder „bestpractice“-Empfehlungen in Bezug auf eine Vielzahl von Themen.
- Der Hauptunterschied besteht darin, dass der Europäische Datenschutzausschuss nicht nur Stellungnahmen bereitstellen wird, wie dies nach Maßgabe der Richtlinie 95/46/EG der Fall war. Er wird darüber hinaus verbindliche Beschlüsse in Fällen erlassen, in denen eine Aufsichtsbehörde im Rahmen eines Verfahrens der Zusammenarbeit und Kohärenz einen maßgeblichen und begründeten Einspruch in den Fällen des „One-Stop-Shop“ erhoben hat, in denen es widersprüchliche Standpunkte dazu gibt, welche der Aufsichtsbehörden die federführende Aufsichtsbehörde ist, und schließlich in Fällen, in denen die zuständige Aufsichtsbehörde die Stellungnahme des EDSB nicht einholt oder dieser nicht folgt. Ziel ist es, die einheitliche Anwendung der Verordnung in allen Mitgliedstaaten sicherzustellen.

Die unabhängige Aufsicht ist ein wesentlicher Bestandteil des europäischen Datenschutzrechts. Sowohl im EU-Recht als auch im Recht des Europarates werden die Aufsichtsbehörden als unerlässlich für den wirksamen Schutz der Rechte und Freiheiten der betroffenen Personen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten betrachtet. Da die Datenverarbeitung nunmehr allgegenwärtig und für den Einzelnen zunehmend schwieriger zu verstehen ist, sind diese Behörden die Wächter des digitalen Zeitalters. In der EU werden unabhängige Aufsichtsbehörden als eines der wichtigsten Bestandteile des im Primärrecht der EU verankerten Rechts auf Schutz personenbezogener Daten betrachtet. Artikel 8 Absatz 3 der Charta der Grundrechte der EU und Artikel 16 Absatz 2 AEUV erkennen den Schutz personenbezogener Daten als Grundrecht an und bekräftigen, dass die Einhaltung der Datenschutzvorschriften von unabhängigen Behörden zu überwachen ist.

Auch die Rechtsprechung bestätigt die Bedeutung der unabhängigen Aufsicht für das Datenschutzrecht.

Beispiel: In der Rechtssache *Schrems*⁴⁹² prüfte der EuGH, ob die Übermittlung personenbezogener Daten an die Vereinigten Staaten (USA) im Rahmen des ersten Safe-Harbor-Abkommens zwischen der EU und den USA angesichts der Enthüllungen von Edward Snowden über die Massenüberwachung seitens der National Security Agency im Einklang mit dem EU-Datenschutzrecht war. Die Übermittlung der personenbezogenen Daten an die USA gründete auf einer im Jahr 2000 angenommenen Entscheidung der Europäischen Kommission, die die Übermittlung personenbezogener Daten von der EU an solche US-Unternehmen erlaubte, die über eine Selbstzertifizierung im Rahmen der Safe-Harbor-Regelung verfügten, da diese Regelung ein angemessenes Schutzniveau für personenbezogene Daten gewährleiste. Als die irische Aufsichtsbehörde zur Untersuchung der seitens des Beschwerdeführers eingelegten Beschwerde in Bezug auf die Rechtmäßigkeit der Datenübermittlungen nach den Snowden-Enthüllungen aufgefordert wurde, wies sie die Beschwerde mit der Begründung zurück, dass die Entscheidung der Kommission über die Angemessenheit der in den Grundsätzen des „sicheren Hafens“ wiedergegebenen US-Datenschutzregelung (die „Safe-Harbor-Entscheidung“) sie an einer weiteren Untersuchung der Beschwerde hindere.

Der EuGH befand jedoch, dass das Vorliegen einer Entscheidung der Europäischen Kommission, die Datenübermittlungen an Drittländer erlaubt, die angemessene Schutzniveaus garantieren, die Befugnisse nationaler Aufsichtsbehörden weder beseitigt noch beschränkt. Der EuGH stellte fest, dass sich die Befugnisse dieser Behörden zur Überwachung und Gewährleistung der Einhaltung der Datenschutzvorschriften der EU aus dem Primärrecht der EU ergeben, und hierbei insbesondere aus Artikel 8 Absatz 3 der Charta und aus Artikel 16 Absatz 2 AEUV. „Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten stellt daher [...] ein wesentliches Element zur Wahrung des Schutzes der Personen bei der Verarbeitung personenbezogener Daten dar.“⁴⁹³

492 EuGH, C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015.

493 a.a.O., Randnr. 41.

Daher entschied der EuGH, dass selbst wenn die Übermittlung personenbezogener Daten aufgrund einer Angemessenheitsentscheidung der Kommission erfolgte, die nationale Aufsichtsbehörde im Falle der Einlegung einer Beschwerde diese Beschwerde mit Sorgfalt zu prüfen hat. Sofern die Aufsichtsbehörde der Meinung ist, dass die Beschwerde unbegründet ist, kann sie sie zurückweisen. Für diesen Fall betonte der EuGH, dass es das Recht auf einen wirksamen Rechtsbehelf erfordert, dass der Beschwerdeführer eine solche Entscheidung vor den nationalen Gerichten anfechten kann und diese eine Vorabentscheidung über die Gültigkeit der Kommissionsentscheidung beim EuGH erwirken können. Hält die Aufsichtsbehörde die Beschwerde für begründet, muss sie über ein Klagerecht verfügen und die Angelegenheit vor die nationalen Gerichte bringen können. Die nationalen Gerichte müssen die Rechtsfrage dem EuGH vorlegen, da er allein über die Befugnis zur Entscheidung über die Gültigkeit einer Angemessenheitsentscheidung der Kommission verfügt.⁴⁹⁴

Im Anschluss daran untersuchte der EuGH die Gültigkeit der Safe-Harbor-Entscheidung, um festzustellen, ob das Übermittlungssystem mit den Datenschutzvorschriften der EU übereinstimmte. Er stellte fest, dass Artikel 3 der Safe-Harbor-Entscheidung die (im Rahmen der Datenschutzrichtlinie garantierten) Befugnisse der nationalen Aufsichtsbehörden in Bezug auf das Tätigwerden zur Verhinderung von Datenübermittlungen im Falle eines unangemessenen Schutzniveaus personenbezogener Daten in den USA einschränkte. In Anbetracht der Bedeutung der unabhängigen Aufsichtsbehörden für die Gewährleistung der Einhaltung des Datenschutzrechts befand der EuGH, dass die Kommission nach Maßgabe der Datenschutzrichtlinie und im Licht der Charta keine Berechtigung hatte, die Befugnisse der unabhängigen Aufsichtsbehörden derart zu beschränken. Die Einschränkung der Befugnisse der Aufsichtsbehörden war einer der Gründe, weshalb der EuGH die Safe-Harbor-Entscheidung für ungültig erklärte.

Eine unabhängige Aufsicht ist daher nach europäischem Recht ein wichtiger Mechanismus, um einen wirksamen Datenschutz zu gewährleisten. Im Falle von Datenschutzverletzungen sind unabhängige Aufsichtsbehörden die erste Anlaufstelle für die betroffenen Personen.⁴⁹⁵ Nach EU-Recht und nach dem Recht des Europarates ist die Einrichtung von Aufsichtsbehörden zwingend

494 a.a.O., Randnrn. 53–66.

495 DSGVO, Artikel 13 Absatz 2 Buchstabe d.

erforderlich. Beide Rechtsrahmen beschreiben die Aufgaben und Befugnisse dieser Behörden auf ähnliche Weise wie die DSGVO. Daher sollten Aufsichtsbehörden im EU-Recht und im Recht des Europarates grundsätzlich auf die gleiche Weise arbeiten.⁴⁹⁶

5.1. Unabhängigkeit

Nach **EU-Recht** und nach dem **Recht des Europarates** muss jede Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig handeln.⁴⁹⁷ Die Unabhängigkeit der Aufsichtsbehörde und ihrer Mitglieder und Bediensteten von direkter oder indirekter Einflussnahme von außen ist für die Gewährleistung völliger Objektivität bei der Entscheidung über Datenschutzangelegenheiten von grundlegender Bedeutung. Nicht nur der Rechtsakt zur Errichtung einer Aufsichtsbehörde muss Bestimmungen enthalten, die ihre Unabhängigkeit garantieren, sondern auch die Organisationsstruktur der Behörde muss ihre Unabhängigkeit widerspiegeln. 2010 untersuchte der EuGH zum ersten Mal den Umfang der Unabhängigkeit von Datenschutzaufsichtsbehörden.⁴⁹⁸ Die nachstehenden Beispiele veranschaulichen, wie der EuGH die Bedeutung des Ausdrucks „völlige Unabhängigkeit“ definiert.

Beispiel: In der Rechtssache *Europäische Kommission gegen Bundesrepublik Deutschland*⁴⁹⁹ beantragte die Europäische Kommission beim EuGH, festzustellen, dass Deutschland das Erfordernis der „völligen Unabhängigkeit“ der für den Datenschutz zuständigen Aufsichtsbehörden falsch umgesetzt und damit gegen seine Verpflichtungen aus Artikel 28 Absatz 1 der Datenschutzrichtlinie verstoßen hat. Nach Auffassung der Kommission verstieß die Tatsache, dass Deutschland die für die Überwachung der Verarbeitung personenbezogener Daten zuständigen Aufsichtsbehörden in den Bundesländern staatlicher Aufsicht unterworfen hat, um die Beachtung des Datenschutzrechts sicher zu stellen, gegen das Erfordernis der Unabhängigkeit.

496 a.a.O., Artikel 51; Modernisiertes Übereinkommen Nr. 108, Artikel 15.

497 DSGVO, Artikel 52 Absatz 1; Modernisiertes Übereinkommen Nr. 108, Artikel 15 Absatz 5.

498 FRA (2010), *Grundrechte: Herausforderungen und Erfolge in 2010, Jahresbericht 2010*, S. 59; FRA (2010), *Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden*, Mai 2010.

499 EuGH, C-518/07, *Europäische Kommission / Bundesrepublik Deutschland* [GK], 9. März 2010, Randnr. 27.

Der EuGH unterstrich, dass die Worte „in völliger Unabhängigkeit“ anhand des Wortlauts dieser Bestimmung und der Ziele und der Systematik des Datenschutzrechts der EU auszulegen sind.⁵⁰⁰ Der EuGH betonte, dass die Aufsichtsbehörden die „Hüter“ der Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten seien. Ihre Errichtung in den Mitgliedstaaten gelte daher „als ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten“.⁵⁰¹ Der EuGH stellte fest: „Folglich müssen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen. Hierzu müssen sie vor jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein“.⁵⁰²

Der EuGH befand ferner, dass die „völlige Unabhängigkeit“ im Lichte der Unabhängigkeit des EDSB ausgelegt werden sollte, wie sie in der Datenschutzverordnung für die EU-Organen festgelegt ist. In dieser Verordnung erfordert der Begriff der Unabhängigkeit, dass der EDSB „niemanden um Weisung ersucht und keine Weisungen entgegennimmt“.

Der EuGH stellte daher fest, dass die Aufsichtsbehörden in Deutschland nicht vollständig unabhängig im Sinne des Datenschutzrechts der EU seien, da sie der staatlichen Aufsicht unterlägen.

Beispiel: In der Rechtssache *Europäische Kommission gegen Republik Österreich*⁵⁰³ wies der EuGH auf ähnliche Probleme bezüglich der Unabhängigkeit bestimmter Mitglieder und Bediensteter der österreichischen Datenschutzkommission (DSK) hin. Der EuGH befand, dass die Tatsache, dass das Bundeskanzleramt Personal an die DSK entsende, das im Datenschutzrecht der EU dargelegte Erfordernis der Unabhängigkeit untergrabe. Der EuGH stellte auch fest, dass das Erfordernis der jederzeitigen Unterrichtung des Kanzleramts über ihre Arbeit die völlige Unabhängigkeit der Aufsichtsbehörde zunichtemacht.

500 a.a.O., Randnrn. 17 und 29.

501 a.a.O., Randnr. 23.

502 a.a.O., Randnr. 25.

503 EuGH, C-614/10, *Europäische Kommission / Republik Österreich* [GK], 16. Oktober 2012, Randnrn. 59 und 63.

Beispiel: In der Rechtssache *Europäische Kommission gegen Ungarn*⁵⁰⁴ wurden ähnliche nationale Praktiken verboten, die die Unabhängigkeit des Personals beeinträchtigten. Der EuGH wies darauf hin, dass „die Vorgabe [...], nach der zu gewährleisten ist, dass die Kontrollstellen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen, die Verpflichtung des betreffenden Mitgliedstaats einschließt, die Dauer des Mandats einer solchen Stelle bis zu seinem ursprünglich vorgesehenen Ablauf zu beachten.“ Infolgedessen entschied der EuGH, dass Ungarn „dadurch gegen seine Verpflichtungen aus der Richtlinie 95/46/EG [...] verstoßen [hat], dass es das Mandat der Kontrollstelle für den Schutz personenbezogener Daten vorzeitig beendet hat.“

Der Begriff und die Kriterien der „völligen Unabhängigkeit“ sind nun in der DSGVO nach Maßgabe der vorstehenden EuGH-Rechtsprechung ausdrücklich vorgesehen. Nach Maßgabe der Verordnung beinhaltet die völlige Unabhängigkeit bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse, dass:⁵⁰⁵

- die Mitglieder jeder Aufsichtsbehörde weder direkter noch indirekter Einflussnahme von außen unterliegen und keine Weisungen entgegennehmen dürfen;
- die Mitglieder jeder Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab, um Interessenkonflikte zu vermeiden;
- die Mitgliedstaaten jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen und Infrastrukturen ausstatten, die sie benötigt, um ihre Aufgaben effektiv wahrnehmen zu können;
- die Mitgliedstaaten sicherstellen, dass jede Aufsichtsbehörde ihr eigenes Personal auswählt;
- die Finanzkontrolle, der jede Aufsichtsbehörde nach Maßgabe der nationalen Rechtsvorschriften unterliegt, ihre Unabhängigkeit nicht beeinträchtigt. Die Aufsichtsbehörden verfügen über eigene, öffentliche, jährliche Haushaltspläne, die ihnen den ordnungsgemäßen Betrieb ermöglichen.

504 EuGH, C-288/12, *Europäische Kommission / Ungarn* [GK], 8. April 2014, Randnrn. 50 und 67.

505 DSGVO, Artikel 52.

Auch das Recht des Europarates betont die Unabhängigkeit der Aufsichtsbehörden als wesentliche Voraussetzung. Das Modernisierte Übereinkommen Nr. 108 fordert, dass die Aufsichtsbehörden „bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse in völliger Unabhängigkeit und Unparteilichkeit handeln“, und weder um Weisungen ersuchen noch diese entgegennehmen.⁵⁰⁶ Dadurch erkennt das Übereinkommen an, dass diese Behörden die Rechte und Freiheiten der Personen im Zusammenhang mit der Datenverarbeitung nur dann wirksam schützen können, wenn sie ihre Aufgaben in völliger Unabhängigkeit ausüben. Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 legt eine Reihe von Faktoren dar, die zum Schutz dieser Unabhängigkeit beitragen. Zu diesen Faktoren zählen die Möglichkeit der Aufsichtsbehörden, ihr eigenes Personal einzustellen und Entscheidungen zu treffen, ohne Einflussnahme von außen, sowie Faktoren im Zusammenhang mit der Dauer der Ausübung ihrer Funktion und den Bedingungen, unter denen sie ihre Funktion beenden können.⁵⁰⁷

5.2. Zuständigkeit und Befugnisse

Im EU-Recht legt die DSGVO die Zuständigkeiten und die Organisationsstruktur der Aufsichtsbehörden fest und ordnet an, dass sie für die Erfüllung der im Rahmen der Verordnung erforderlichen Aufgaben befähigt und über die notwendigen Voraussetzungen verfügen müssen.

Die Aufsichtsbehörde ist das wichtigste Organ im nationalen Recht, das die Einhaltung des Datenschutzrechts der EU gewährleistet. Die Aufsichtsbehörden haben neben der Überwachung einen umfangreichen Katalog an Aufgaben und Befugnissen, zu denen auch proaktive und vorbeugende Aufsichtstätigkeiten zählen. Zur Ausführung dieser Aufgaben müssen die Aufsichtsbehörden über passende, in Artikel 58 DSGVO aufgeführte, Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse verfügen, wie beispielsweise:⁵⁰⁸

- Verantwortliche und betroffenen Personen in Bezug auf alle Angelegenheiten des Datenschutzes beraten;
- Standarddatenschutzklauseln, verbindliche interne Datenschutzvorschriften oder Verwaltungsvereinbarungen genehmigen;

⁵⁰⁶ Modernisiertes Übereinkommen Nr. 108, Artikel 15 Absatz 5.

⁵⁰⁷ Erläuternder Bericht zum Modernisierten Übereinkommen 108.

⁵⁰⁸ DSGVO, Artikel 58. Siehe auch Übereinkommen Nr. 108, Zusatzprotokoll, Artikel 1.

- Verarbeitungsvorgänge untersuchen und angemessen einschreiten;
- sämtliche Informationen anfordern, die für die Überwachung der Tätigkeiten der Verantwortlichen erforderlich sind;
- Verantwortliche warnen oder verwarnen und die Übermittlung von Mitteilungen über eine Datenschutzverletzung an die betroffenen Personen verlangen;
- Berichtigung, Sperrung, Löschung oder Vernichtung von Daten anordnen;
- ein vorübergehendes oder endgültiges Verarbeitungsverbots oder Geldbußen verhängen;
- die Angelegenheit vor Gericht bringen.

Um ihre Aufgaben auszuüben muss eine Aufsichtsbehörde Zugang zu allen für eine Ermittlung erforderlichen personenbezogenen Daten und Informationen sowie Zugang zu allen Geschäftsräumen haben, in denen ein Verantwortlicher die maßgeblichen Informationen aufbewahrt. Nach Ansicht des EuGH sind die Befugnisse der Aufsichtsbehörde weit auszulegen, um betroffenen Personen in der EU die volle Wirksamkeit des Datenschutzes zu gewährleisten.

Beispiel: In der Rechtssache *Schrems* prüfte der EuGH, ob die Übermittlung personenbezogener Daten an die Vereinigten Staaten (USA) im Rahmen des ersten Safe-Harbor-Abkommens angesichts der Enthüllungen von Edward Snowden im Einklang mit dem EU-Datenschutzrecht erfolgte. Der EuGH entschied, dass Aufsichtsbehörden, die als unabhängige Überwachungsinstanzen bezüglich der Datenverarbeitung durch den Verantwortlichen handeln, trotz Vorliegen einer Angemessenheitsentscheidung die Übermittlung personenbezogener Daten in ein Drittland verhindern können, sofern ausreichende Beweise dafür vorliegen, dass der angemessene Schutz im Drittland nicht länger gewährleistet ist.⁵⁰⁹

⁵⁰⁹ Rechtssache C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015, Randnrn. 26–36 und 40–41.

Jede Aufsichtsbehörde ist in ihrem Hoheitsgebiet für die Ausübung von Untersuchungs- und Abhilfebefugnissen zuständig. Da jedoch Verantwortliche und Auftragsverarbeiter häufig grenzüberschreitend tätig sind und die Datenverarbeitung Auswirkungen auf betroffene Personen hat, die in mehreren Mitgliedstaaten ansässig sind, stellt sich die Frage nach der Aufteilung der Zuständigkeiten zwischen den verschiedenen Aufsichtsbehörden. Der EuGH konnte dieses Thema in der Rechtssache *Weltimmo* untersuchen.

Beispiel: In der Rechtssache *Weltimmo*⁵¹⁰ prüfte der EuGH die Zuständigkeit nationaler Aufsichtsbehörden für Unternehmen, die nicht in ihrem Hoheitsgebiet niedergelassen sind. Bei *Weltimmo* handelte es sich um eine in der Slowakei eingetragene Gesellschaft, die eine Website zur Vermittlung von in Ungarn gelegenen Immobilien betrieb. Inserenten reichten bei der ungarischen Aufsichtsbehörde eine Beschwerde aufgrund der Verletzung des ungarischen Datenschutzrechts ein und die Aufsichtsbehörde belegte *Weltimmo* mit einem Bußgeld. Die Gesellschaft focht die Geldstrafe vor den nationalen Gerichten an und die Rechtssache wurde an den EuGH verwiesen, der feststellen sollte, ob die EU-Datenschutzrichtlinie der Aufsichtsbehörde eines Mitgliedstaats die Anwendung ihres nationalen Datenschutzrechts auf eine in einem anderen Mitgliedstaat eingetragene Gesellschaft erlaubte.

Der EuGH legte Artikel 4 Absatz 1 der Datenschutzrichtlinie dahin aus, dass er die Anwendung des Datenschutzrechts eines anderen Mitgliedstaats als dem, in dem der Verantwortliche eingetragen ist, erlaubt, „soweit dieser mittels einer festen Einrichtung im Hoheitsgebiet dieses Mitgliedstaats eine effektive und tatsächliche Tätigkeit ausübt, in deren Rahmen diese Verarbeitung ausgeführt wird, selbst wenn die Tätigkeit nur geringfügig ist“. Gestützt auf die ihm vorgelegten Informationen stellte der EuGH fest, dass *Weltimmo* eine tatsächliche und effektive Tätigkeit in Ungarn ausübte, da die Gesellschaft über einen Vertreter in Ungarn verfügte, der im slowakischen Handelsregister unter einer Adresse in Ungarn aufgeführt war, sowie über ein ungarisches Bankkonto und ein ungarisches Postfach, und in Ungarn Websites in ungarischer Sprache betrieb. Diese Informationen ließen auf die Existenz einer Niederlassung in Ungarn schließen und würden die Tätigkeit von *Weltimmo* dem ungarischen Datenschutzrecht und der Zuständigkeit

⁵¹⁰ EuGH, C-230/14, *Weltimmo s.r.o. / Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. Oktober 2015.

der ungarischen Aufsichtsbehörde unterstellen. Der EuGH überließ es jedoch dem nationalen Gericht, die Informationen zu prüfen und zu entscheiden, ob Weltimmo in der Tat über eine Niederlassung in Ungarn verfügte.

Sollte das vorliegende Gericht feststellen, dass Weltimmo über eine Niederlassung in Ungarn verfügte, hätten die ungarischen Aufsichtsbehörden die Befugnis zur Verhängung eines Bußgelds. Sollte das nationale Gericht jedoch das Gegenteil entscheiden, d. h., dass Weltimmo über keine Niederlassung in Ungarn verfügte, würde es sich beim anwendbaren Recht folglich um das Recht des Mitgliedstaats/der Mitgliedstaaten handeln, in dem/denen die Gesellschaft eingetragen war. Da die Befugnisse der Aufsichtsbehörden in Übereinstimmung mit der territorialen Souveränität des Mitgliedstaats auszuüben sind, könnte die ungarische Aufsichtsbehörde in diesem Fall keine Sanktionen verhängen. Da die Datenschutzrichtlinie für Aufsichtsbehörden eine Verpflichtung zur Zusammenarbeit vorsah, könnte die ungarische Aufsichtsbehörde jedoch ihr slowakisches Pendant darum ersuchen, die Angelegenheit zu untersuchen, einen Verstoß gegen slowakisches Recht festzustellen und die unter slowakischem Recht vorgesehenen Sanktionen zu verhängen.

Mit der Annahme der DSGVO gibt es nun detaillierte Vorschriften in Bezug auf die Zuständigkeit der Aufsichtsbehörden in grenzüberschreitenden Fällen. Die Verordnung führt den „One-Stop-Shop-Mechanismus“ ein und enthält Bestimmungen, die eine Zusammenarbeit zwischen den verschiedenen Aufsichtsbehörden anordnen. Um eine wirksame Zusammenarbeit in grenzüberschreitenden Fällen zu gewährleisten, verlangt die DSGVO die Festlegung einer federführenden Aufsichtsbehörde, wie etwa der Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters.⁵¹¹ Die federführende Aufsichtsbehörde ist für grenzüberschreitende Fälle zuständig, sie ist der einzige Ansprechpartner des Verantwortlichen oder des Auftragsverarbeiters und sie koordiniert die Zusammenarbeit mit anderen Aufsichtsbehörden, um einen Konsens zu erzielen. Die Zusammenarbeit umfasst den Informationsaustausch, die gegenseitige Amtshilfe bei der Durchführung von Kontrollen und Untersuchungen und das Fassen verbindlicher Beschlüsse.⁵¹²

511 DSGVO, Artikel 56 Absatz 1.

512 a.a.O., Artikel 60.

Im Recht des Europarates sind die Zuständigkeiten und Befugnisse der Aufsichtsbehörden in Artikel 15 des Modernisierten Übereinkommens Nr. 108 dargelegt. Diese Befugnisse entsprechen den Befugnissen, die den Aufsichtsbehörden im EU-Recht erteilt wurden, und umfassen unter anderem Untersuchungs- und Abhilfebefugnisse, Beschlussfassungen, Bußgeldbefugnisse bei Verstößen gegen die Bestimmungen des Übereinkommens, sowie Befugnisse Gerichtsverfahren anzustrengen. Unabhängige Aufsichtsbehörden sind auch dafür zuständig, seitens betroffener Personen eingereichte Anträge und Beschwerden zu bearbeiten, die Öffentlichkeit für das Datenschutzrecht zu sensibilisieren und die nationalen Entscheidungsträger im Hinblick auf Legislativ- oder Verwaltungsmaßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten zu beraten.

5.3. Zusammenarbeit

Die DSGVO schafft einen allgemeinen Rahmen für die Zusammenarbeit zwischen den Aufsichtsbehörden und liefert genauere Vorschriften für die Zusammenarbeit von Aufsichtsbehörden bei grenzüberschreitenden Datenverarbeitungen.

Nach Maßgabe der DSGVO gewähren die Aufsichtsbehörden einander Amtshilfe und tauschen maßgebliche Informationen aus, um die Verordnung einheitlich ergreifen und anzuwenden.⁵¹³ Dies beinhaltet, dass die ersuchte Aufsichtsbehörde Konsultationen, Nachprüfungen und Untersuchungen vornimmt. Die Aufsichtsbehörden können gemeinsame Maßnahmen einschließlich gemeinsamer Untersuchungen und gemeinsamer Durchsetzungsmaßnahmen durchführen, an denen Bedienstete aller Aufsichtsbehörden teilnehmen.⁵¹⁴

Innerhalb der EU arbeiten Verantwortliche und Auftragsverarbeiter in zunehmendem Maße länderübergreifend. Dies erfordert eine enge Zusammenarbeit zwischen den zuständigen Aufsichtsbehörden der Mitgliedstaaten, um zu gewährleisten, dass die Verarbeitung personenbezogener Daten den Anforderungen der DSGVO entspricht. Sofern ein Verantwortlicher oder ein Auftragsverarbeiter Niederlassungen in mehreren Mitgliedstaaten hat, oder eine einzige Niederlassung, die Verarbeitungstätigkeiten jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat

⁵¹³ a.a.O., Artikel 61 Absatz 1 bis 3 und Artikel 62 Absatz 1.

⁵¹⁴ a.a.O., Artikel 62 Absatz 1.

haben, so ist die Aufsichtsbehörde der Hauptniederlassung (oder der einzigen Niederlassung) nach Maßgabe des in der Verordnung dargelegten One-Stop-Shop-Verfahrens die federführende Aufsichtsbehörde für die grenzüberschreitenden Tätigkeiten des Verantwortlichen oder des Auftragsverarbeiters. Federführende Aufsichtsbehörden können Maßnahmen gegen den Verantwortlichen oder den Auftragsverarbeiter durchsetzen. Das One-Stop-Shop-Verfahren will Datenschutzrecht harmonisieren und dessen einheitliche Anwendung länderübergreifend verbessern. Es hat auch Vorteile für Unternehmen, da diese sich nur mit der federführenden anstatt mit mehreren Aufsichtsbehörden auseinandersetzen müssen. Dies erhöht die Rechtssicherheit für Unternehmen und sollte in der Praxis auch bedeuten, dass Beschlüsse schneller gefasst werden und Unternehmen es nicht mit verschiedenen Aufsichtsbehörden zu tun haben, die widersprüchliche Auflagen anordnen.

Um die federführende Aufsichtsbehörde festzustellen, muss die Hauptniederlassung bestimmt werden. Der Begriff „Hauptniederlassung“ ist in der DSGVO definiert. Darüber hinaus hat die Artikel-29-Datenschutzgruppe Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters herausgegeben, die die Kriterien für die Ermittlung der Hauptniederlassung enthalten.⁵¹⁵

Zur europaweiten Sicherstellung eines hohen Datenschutzniveaus handelt die federführende Aufsichtsbehörde nicht allein. Sie arbeitet mit den anderen betroffenen Aufsichtsbehörden zusammen, um Beschlüsse in Bezug auf die Verarbeitung personenbezogener Daten seitens Verantwortlicher und Auftragsverarbeiter zu fassen und bemüht sich dabei, einen Konsens zu erzielen und Kohärenz zu gewährleisten. Die Zusammenarbeit zwischen den entsprechenden Aufsichtsbehörden umfasst den Austausch von Informationen, die Gewährung gegenseitiger Amtshilfe sowie die Durchführung gemeinsamer Untersuchungen und gemeinsamer Überwachungstätigkeiten.⁵¹⁶ Im Zuge gegenseitiger Amtshilfe müssen die Aufsichtsbehörden die Auskunftersuchen anderer Aufsichtsbehörden sorgfältig bearbeiten und aufsichtsbezogene Maßnahmen ausüben, wie beispielsweise Ersuchen um vorherige Genehmigungen und eine vorherige Konsultation mit dem Verantwortlichen in Bezug auf dessen Verarbeitungstätigkeiten, sowie Vornahme von Nachprüfungen oder

⁵¹⁵ Artikel-29-Datenschutzgruppe (2016), *Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters*, WP 244, Brüssel, 13. Dezember 2016, überarbeitet am 5. April 2017.

⁵¹⁶ DSGVO, Artikel 60 Absatz 1–3.

Untersuchungen. Aufsichtsbehörden in anderen Mitgliedstaaten ist auf deren Ersuchen unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens Amtshilfe zu gewähren.⁵¹⁷

Wenn der Verantwortliche Niederlassungen in mehreren Mitgliedstaaten hat, können die Aufsichtsbehörden gemeinsame Maßnahmen einschließlich Untersuchungen und Durchsetzungsmaßnahmen durchführen, an denen Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten teilnehmen.⁵¹⁸

Die Zusammenarbeit zwischen den verschiedenen Aufsichtsbehörden stellt auch im Recht des Europarates eine wichtige Forderung dar. Das Modernisierte Übereinkommen Nr. 108 sieht vor, dass Aufsichtsbehörden in dem zur Durchführung ihrer Aufgaben erforderlichen Umfang zusammenarbeiten müssen.⁵¹⁹ Dies sollte beispielsweise durch die gegenseitige Bereitstellung maßgeblicher und zweckdienlicher Informationen, die Koordinierung von Untersuchungen und die Durchführung gemeinsamer Maßnahmen erfolgen.⁵²⁰

5.4. Der Europäische Datenschutzausschuss

Die Bedeutung unabhängiger Aufsichtsbehörden und die ihnen durch das europäische Datenschutzrecht eingeräumten Befugnisse wurden im vorliegenden Kapitel bereits beschrieben. Der Europäische Datenschutzausschuss hat ebenfalls eine zentrale Bedeutung und gewährleistet die wirksame und einheitliche Anwendung der Datenschutzvorschriften in der EU.

Die DSGVO stattet den EDSA als EU-Organ mit eigener Rechtspersönlichkeit aus.⁵²¹ Er ist Nachfolger der Artikel-29-Datenschutzgruppe,⁵²² die durch die Datenschutzrichtlinie eingerichtet wurde, um die Kommission zu allen

517 *a.a.O.*, Artikel 61 Absatz 1 und 2.

518 *a.a.O.*, Artikel 62 Absatz 1.

519 Modernisiertes Übereinkommen Nr. 108, Artikel 16 und 17.

520 *a.a.O.*, Artikel 17.

521 DSGVO, Artikel 68.

522 Nach Maßgabe der Richtlinie 95/46/EG sollte die Artikel-29-Datenschutzgruppe die Kommission zu allen EU-Maßnahmen beraten, die die Rechte der Personen in Bezug auf die Verarbeitung personenbezogener Daten und die Privatsphäre betreffen, die einheitliche Anwendung der Richtlinie fördern und gegenüber der Kommission zu Angelegenheiten im Zusammenhang mit dem Datenschutz sachkundig Stellung nehmen. Die Artikel-29-Datenschutzgruppe bestand aus Vertretern der Aufsichtsbehörden der EU-Mitgliedstaaten, Vertretern der Kommission und dem EDSB.

EU-Maßnahmen zu beraten, die die Rechte der Personen in Bezug auf die Verarbeitung personenbezogener Daten und die Privatsphäre betreffen, die einheitliche Anwendung der Richtlinie zu fördern und gegenüber der Kommission zu Angelegenheiten im Zusammenhang mit dem Datenschutz sachkundig Stellung zu nehmen. Die Artikel-29-Datenschutzgruppe bestand aus Vertretern der Aufsichtsbehörden der EU-Mitgliedstaaten, Vertretern der Kommission und dem EDSB.

Ähnlich wie die Datenschutzgruppe besteht der EDSA aus den Leitern der Aufsichtsbehörden jedes Mitgliedstaats und des EDSB oder ihren Vertretern.⁵²³ Der EDSB hat die gleichen Stimmrechte, mit Ausnahme von Fällen im Zusammenhang mit der Streitbeilegung, in denen er nur bei Beschlüssen stimmberechtigt ist, die Grundsätze und Vorschriften betreffen, die für die EU-Organe gelten und inhaltlich den Grundsätzen und Vorschriften der DSGVO entsprechen. Die Kommission ist berechtigt, ohne Stimmrechte an den Tätigkeiten und Sitzungen des EDSA teilzunehmen.⁵²⁴ Der Ausschuss wählt aus dem Kreis seiner Mitglieder mit einfacher Mehrheit einen Vorsitzenden (der mit der Vertretung des Ausschusses betraut wird) und zwei stellvertretende Vorsitzende für eine Amtszeit von fünf Jahren. Darüber hinaus steht dem EDSA auch ein Sekretariat zur Verfügung, das vom EDSB bereitgestellt wird und dem Ausschuss analytische, administrative und logistische Unterstützung leistet.⁵²⁵

Die Aufgaben des EDSA sind in den Artikeln 64, 65 und 70 DSGVO dargelegt und umfassen umfangreiche Pflichten, die in drei Haupttätigkeiten unterteilt werden können:

- **Kohärenz:** Der EDSA kann in drei Fällen verbindliche Beschlüsse fassen: wenn eine Aufsichtsbehörde in Fällen des One-Stop-Shop einen maßgeblichen und begründeten Einspruch eingelegt hat, wenn es widersprüchliche Standpunkte dazu gibt, welche Aufsichtsbehörde die „federführende“ Aufsichtsbehörde ist, und schließlich, wenn die zuständige Aufsichtsbehörde keine Stellungnahme des EDSA einholt oder dessen Stellungnahme nicht folgt.⁵²⁶ Die Hauptaufgabe des EDSA besteht in der

⁵²³ DSGVO, Artikel 68 Absatz 3.

⁵²⁴ a.a.O., Artikel 68 Absatz 4 und 5.

⁵²⁵ a.a.O., Artikel 73 und 75.

⁵²⁶ a.a.O., Artikel 65.

Gewährleistung der einheitlichen Anwendung der DSGVO in der EU und wie in [Abschnitt 5.5](#) beschrieben, spielt er eine führende Rolle im Kohärenzverfahren.

- **Beratung:** Zu den Aufgaben des EDSA zählen die Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, wie Änderungen der DSGVO, Überarbeitungen von die Datenverarbeitung betreffenden EU-Datenschutzvorschriften, die im Widerspruch zu EU-Datenschutzrecht stehen sowie zum Erlass von Angemessenheitsbeschlüssen durch die Kommission, die die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation ermöglichen.
- **Hinweise:** Der Ausschuss gibt auch Richtlinien, Empfehlungen und Best-Practice-Hinweise, um die einheitliche Anwendung der Verordnung sicherzustellen und fördert die Zusammenarbeit und den Austausch von Fachwissen unter den Aufsichtsbehörden. Darüber hinaus ermutigt er Verbände von Verantwortlichen oder Auftragsverarbeitern zur Ausarbeitung von Verhaltensregeln und zur Einrichtung von datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegeln.

Die Beschlüsse des EDSA können vor dem EuGH angefochten werden.

5.5. Das Kohärenzverfahren der DSGVO

Die DSGVO normiert ein Kohärenzverfahren zur Gewährleistung der einheitlichen Anwendung der Verordnung in allen Mitgliedstaaten, in dessen Rahmen die Aufsichtsbehörden untereinander und gegebenenfalls mit der Kommission zusammenarbeiten. Das Kohärenzverfahren kommt in zwei Situationen zum Einsatz. Die erste betrifft Stellungnahmen des EDSA in Fällen, in denen eine zuständige Aufsichtsbehörde beabsichtigt, Maßnahmen zu erlassen, wie die Annahme einer Liste der Verarbeitungsvorgänge die einer Datenschutz-Folgenabschätzung (DSFA) bedürfen, oder Standarddatenschutzklauseln festzulegen. Die zweite betrifft verbindliche Beschlüsse des EDSA für Aufsichtsbehörden in One-Stop-Shop Fällen, wenn eine Aufsichtsbehörde die Stellungnahme des EDSA nicht einholt oder dieser nicht folgt.

6

Rechte betroffener Personen und ihre Durchsetzung

EU	Behandelte Themen	Europarat
Recht auf Information		
DSGVO, Artikel 12 EuGH, C-473/12, <i>Institut professionnel des agents immobiliers (IPI)</i> / Englebert, 2013 EuGH, C-201/14, <i>Smaranda Bara und andere / Casa Națională de Asigurări de Sănătate und andere</i> , 2015	Transparenz der Information	Modernisiertes Übereinkommen Nr. 108, Artikel 8
DSGVO, Artikel 13 Absatz 1 und 2 und Artikel 14 Absatz 1 und 2	Inhalt der Information	Modernisiertes Übereinkommen Nr. 108, Artikel 8 Absatz 1
DSGVO, Artikel 13 Absatz 1 und Artikel 14 Absatz 3	Zeitpunkt der Information	Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe b
DSGVO, Artikel 12 Absatz 1, 5 und 7	Mittel zur Bereitstellung der Information	Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe b
DSGVO, Artikel 13 Absatz 2 Buchstabe d und Artikel 14 Absatz 2 Buchstabe e, Artikel 77, 78 und 79	Recht auf Beschwerde	Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe f

EU	Behandelte Themen	Europarat
Recht auf Auskunft		
DSGVO, Artikel 15 Absatz 1 EuGH, C-553/07, <i>College van burgemeester en wethouders van Rotterdam / M. E. E. Rijkeboer</i>, 2009 EuGH, Verbundene Rechtssachen C-141/12 und C-372/12, <i>YS / Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel / M und S</i>, 2014 EuGH, C-434/16, <i>Peter Nowak / Data Protection Commissioner</i>, 2017	Recht auf Auskunft über die eigenen Daten	Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe b EGMR, <i>Leander / Schweden</i>, Nr. 9248/81, 1987
Recht auf Berichtigung		
DSGVO, Artikel 16	Berichtigung falscher personenbezogener Daten	Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe e EGMR, <i>Cemalettin Canli / Türkei</i>, Nr. 22427/04, 2008 EGMR, <i>Ciubotaru / Republik Moldau</i>, Nr. 27138/04, 2010
Recht auf Löschung		
DSGVO, Artikel 17 Absatz 1	Löschung personenbezogener Daten	Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe e EGMR, <i>Segerstedt-Wiberg und andere / Schweden</i>, Nr. 62332/00, 2006
EuGH, C-131/12, <i>Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GK]</i>, 2014 EuGH, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni</i>, 2017	Recht auf Vergessenwerden	

EU	Behandelte Themen	Europarat
Recht auf Einschränkung der Verarbeitung		
DSGVO, Artikel 18 Absatz 1	Recht auf Beschränkung der Verwendung personenbezogener Daten	
DSGVO, Artikel 19	Meldepflicht	
Recht auf Datenübertragbarkeit		
DSGVO, Artikel 20	Recht auf Datenübertragbarkeit	
Widerspruchsrecht		
DSGVO, Artikel 21 Absatz 1 EuGH, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni</i> , 2017	Recht auf Widerspruch durch die betroffene Person aufgrund ihrer besonderen Situation	Profiling-Empfehlung, Artikel 5.3 Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe d
DSGVO, Artikel 21 Absatz 2	Recht auf Widerspruch gegen eine Nutzung von Daten zu Direktmarketing	Empfehlung zum Direktmarketing, Artikel 4 Absatz 1
DSGVO, Artikel 21 Absatz 5	Widerspruchsrecht mittels automatisierter Verfahren	
Rechte in Bezug auf die automatisierte Entscheidungsfindung und Profiling		
DSGVO, Artikel 22	Rechte in Bezug auf die automatisierte Entscheidungsfindung und Profiling	Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe a
DSGVO, Artikel 21	Widerspruchsrecht gegen automatisierte Entscheidungsfindung	
DSGVO, Artikel 13 Absatz 2 Buchstabe f	Informationsanspruch auf eine aussagekräftige Erklärung über die angewandte Logik sowie Tragweite und Auswirkungen	Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe c

EU	Behandelte Themen	Europarat
Rechtsbehelfe, Haftung, Sanktionen und Schadensersatz		
Die Charta, Artikel 47 EuGH, C-362/14, <i>Maximillian Schrems / Data Protection Commissioner</i> [GK], 2015 DSGVO; Artikel 77–84	Bei Verletzungen des nationalen Datenschutzrechts	EGMR, Artikel 13 (nur für Mitgliedstaaten des Europarats) Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe f, Artikel 12, 15, 16–21 EGMR, <i>K.U. / Finnland</i> , Nr. 2872/02, 2008 EGMR, <i>Biriuk / Litauen</i> , Nr. 23373/03, 2008
<i>Datenschutzverordnung für die EU-Organe</i> , Artikel 34 und 49 EuGH, C-28/08 P, <i>Europäische Kommission / The Bavarian Lager Co. Ltd</i> [GK], 2010	Bei Verletzungen des EU-Rechts durch Organe und Einrichtungen der EU	

Die Wirksamkeit gesetzlicher Vorschriften im Allgemeinen und der Rechte der betroffenen Personen im Besonderen hängen in nicht unerheblichem Umfang von der Existenz geeigneter Mechanismen zu ihrer Durchsetzung ab. Im digitalen Zeitalter ist die Datenverarbeitung allgegenwärtig und für die Einzelnen zunehmend schwerer zu verstehen. Um das Ungleichgewicht der Kräfte zwischen betroffenen Personen und Verantwortlichen abzuschwächen, wurden den betroffenen Personen bestimmte Rechte zuerkannt, um mehr Kontrolle über die Verarbeitung ihrer personenbezogenen Daten ausüben zu können. Das Recht auf Auskunft über die eigenen Daten und das Recht auf deren Berichtigung sind in Artikel 8 Absatz 2 der Charta der Grundrechte der Europäischen Union verankert, einem Dokument, das zum Primärrecht der EU zählt und in der Rechtsordnung der EU von grundlegender Bedeutung ist. Das Sekundärrecht der EU und insbesondere die Datenschutz-Grundverordnung haben einen einheitlichen Rechtsrahmen geschaffen, der den betroffenen Personen durch die Zuerkennung von Rechten gegenüber den für die Datenverarbeitung Verantwortlichen mehr Macht verleiht. Zusätzlich zu den Rechten auf Auskunft und Berichtigung nennt die DSGVO eine Reihe anderer Rechte, wie das Recht auf Löschung („Recht auf Vergessenwerden“), das Widerspruchsrecht oder das Recht auf Einschränkung der Verarbeitung, sowie Rechte in Bezug auf die automatisierte Entscheidungsfindung und Profiling. Auch im Modernisierten

Übereinkommen Nr. 108 sind ähnliche Garantien enthalten, die den betroffenen Personen die wirksame Kontrolle über ihre Daten ermöglichen. Artikel 9 nennt die Rechte, die die Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten ausüben können sollten. Die Vertragsparteien müssen gewährleisten, dass diese Rechte in ihrer Rechtsordnung jeder betroffenen Person zur Verfügung stehen und rechtswirksam ausgeübt werden können.

Neben der Bereitstellung von Rechten für die betroffenen Personen ist es ebenso wichtig, Mechanismen einzurichten, die diesen ermöglichen, Verletzungen ihrer Rechte anzufechten, Verantwortliche haftbar zu machen und Schadensersatzansprüche geltend zu machen. Das in der EMRK und in der Charta garantierte Recht auf einen wirksamen Rechtsbehelf erfordert, dass jeder Person Rechtsbehelfe zur Verfügung stehen.

6.1. Rechte der betroffenen Personen

Kernpunkte

- Jede betroffene Person hat grundsätzlich das Recht, über die Verarbeitung ihrer personenbezogenen Daten seitens aller Verantwortlichen informiert zu werden.
- Betroffene Personen haben das Recht:
 - Auskunft über ihre Daten und bestimmte Informationen über deren Verarbeitung zu erhalten;
 - ihre Daten vom Verantwortlichen berichtigen zu lassen, wenn die Daten unrichtig sind;
 - ihre Daten vom Verantwortlichen gegebenenfalls löschen zu lassen, wenn der Verantwortliche ihre Daten rechtswidrig verarbeitet;
 - die Verarbeitung vorübergehend einzuschränken;
 - ihre Daten unter bestimmten Voraussetzungen an einen anderen Verantwortlichen übermitteln zu lassen.
- Darüber hinaus haben betroffene Personen aus den nachstehenden Gründen das Recht, Widerspruch gegen die Verarbeitung einzulegen:
 - Gründe in Bezug auf ihre besondere Situation;
 - die Verwendung ihrer Daten für Zwecke der Direktwerbung.

- Betroffene Personen haben das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt. Betroffene Personen haben überdies das Recht:
 - auf ein menschliches Eingreifen seitens des Verantwortlichen;
 - auf Darlegung des eigenen Standpunkts und auf Anfechtung einer auf einer automatisierten Verarbeitung beruhenden Entscheidung.

6.1.1. Recht auf Information

Sowohl nach Maßgabe des **Rechts des Europarates** als auch nach Maßgabe des **EU-Rechts** sind Verantwortliche von Verarbeitungsvorgängen dazu verpflichtet, die betroffene Person zum Zeitpunkt der Erhebung personenbezogener Daten über deren beabsichtigte Verarbeitung zu unterrichten. Diese Verpflichtung hängt jedoch nicht von einem Antrag der betroffenen Person ab. Vielmehr muss der Verantwortliche diese Verpflichtung proaktiv erfüllen, unabhängig davon, ob die betroffene Person an der Unterrichtung interessiert ist oder nicht.

Das Recht des Europarates gibt in Artikel 8 des Modernisierten Übereinkommens Nr. 108 den Vertragsstaaten vor, sicherzustellen, dass die Verantwortlichen die betroffenen Personen über ihre Identität und ihren Aufenthaltsort, die Rechtsgrundlage und den Zweck der Verarbeitung, die Kategorien der verarbeiteten personenbezogenen Daten, (gegebenenfalls) die Empfänger der personenbezogenen Daten und über ihre Rechte gemäß Artikel 9 unterrichten, zu denen das Recht auf Auskunft, Berichtigung und Einlegung von Rechtsbehelfen zählt. Jedwede zusätzliche Information, die zur Gewährleistung einer nach Treu und Glauben und transparent erfolgenden Verarbeitung notwendig erscheint, sollen den betroffenen Personen ebenfalls mitgeteilt werden. Der Erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 verdeutlicht, dass die den betroffenen Personen vorgelegten Informationen „leicht zugänglich, lesbar, verständlich und an den Empfängerhorizont der betroffenen Personen angepasst sein müssen“.⁵²⁷

Im EU-Recht erfordert der Grundsatz der Transparenz, dass jede Verarbeitung personenbezogener Daten für die Personen grundsätzlich transparent sein sollte. Die Personen haben das Recht darauf, zu wissen, wie und welche

⁵²⁷ Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 68.

personenbezogenen Daten erhoben, verwendet oder auf sonstige Weise verarbeitet werden, und über die Risiken, Garantien und Rechte im Zusammenhang mit der Verarbeitung informiert zu werden.⁵²⁸ Artikel 12 DSGVO enthält daher die umfangreiche Verpflichtung für die Verantwortlichen transparente Information bereitzustellen und/oder den betroffenen Personen mitzuteilen, wie sie ihre Rechte ausüben können.⁵²⁹ Die Informationen müssen präzise, transparent, verständlich und leicht zugänglich sowie in klarer und einfacher Sprache abgefasst sein. Sie müssen schriftlich bereitgestellt werden, einschließlich gegebenenfalls in elektronischer Form, und können auf Antrag der betroffenen Person auch mündlich erteilt werden, sofern deren Identität ohne Zweifel nachgewiesen wurde. Die Informationen werden unverzüglich und unentgeltlich bereitgestellt.⁵³⁰

Artikel 13 und Artikel 14 DSGVO regeln das Recht der betroffenen Personen auf Information, sowohl in Situationen, in denen die personenbezogenen Daten direkt bei ihr erhoben wurden, als auch in Situationen, in denen diese nicht bei ihr erhoben wurden.

Der Umfang des Rechts auf Information und dessen Schranken nach EU-Recht klärte die Rechtsprechung des EuGH.

Beispiel: In der Rechtssache *Institut professionnel des agents immobiliers (IPI) gegen Englebert*⁵³¹ wurde der EuGH um die Auslegung von Artikel 13 Absatz 1 der Richtlinie 95/46/EG gebeten. Durch diesen Artikel erhielten die Mitgliedstaaten die Möglichkeit, zu entscheiden, ob sie Rechtsvorschriften erlassen, die den Umfang des Rechts auf Information der betroffenen Person bei Bedarf beschränken, um unter anderem die Rechte und Freiheiten anderer Personen zu schützen und Straftaten oder Verstöße gegen die berufsständischen Regeln bei reglementierten Berufen zu verhüten und zu ermitteln. IPI ist ein belgischer Berufsverband von Immobilienmaklern, der die Aufgabe hat, die Einhaltung der ordnungsgemäßen Ausübung des Berufs des Immobilienmaklers zu gewährleisten. Das IPI beantragte bei einem nationalen Gericht, festzustellen, dass die Beklagten Verstöße gegen

⁵²⁸ DSGVO, Erwägungsgrund 39.

⁵²⁹ a.a.O., Artikel 13 und 14; Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe b.

⁵³⁰ DSGVO, Artikel 12 Absatz 5; Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe b.

⁵³¹ EuGH, C-473/12, *Institut professionnel des agents immobiliers (IPI) / Geoffrey Englebert und andere*, 7. November 2013.

die berufsständischen Regeln begangen hatten, und ihnen die Einstellung verschiedener Geschäftstätigkeiten im Immobilienbereich aufzugeben. Die Klage war auf Beweise gestützt, die von Privatdetektiven, die das IPI in Anspruch genommen hatte, zusammengetragen worden waren.

Das nationale Gericht äußerte Zweifel in Bezug auf den Wert der von den Detektiven zusammengetragenen Beweise, angesichts der Möglichkeit, dass sie ohne Einhaltung der Datenschutzanforderungen der belgischen Gesetzgebung erlangt worden seien, und insbesondere der Pflicht zur Information der betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten vor Erhebung dieser Daten. Der EuGH stellte fest, dass Artikel 13 Absatz 1 besagte, dass die Mitgliedstaaten in ihrem nationalen Recht Ausnahmen von der Pflicht, die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten zu informieren, vorsehen „können“, nicht aber dazu verpflichtet sind. Da Artikel 13 Absatz 1 die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln als Gründe für die Beschränkung der Rechte der Einzelnen anführt, könne sich die Tätigkeit eines Berufsverbands wie des IPI und der in seinem Namen handelnden Privatdetektive auf diese Bestimmung berufen. Sofern ein Mitgliedstaat eine solche Ausnahme jedoch nicht vorgesehen hat, sind die betroffenen Personen zu informieren.

Beispiel: In der Rechtssache *Smaranda Bara und andere gegen Casa Națională de Asigurări de Sănătate und andere*⁵³² klärte der EuGH, ob das EU-Recht es ausschließt, dass eine nationale Verwaltungsbehörde personenbezogene Daten an eine andere Verwaltungsbehörde zur anschließenden Verarbeitung übermittelt, ohne dass die betroffenen Personen von der Übermittlung und der Verarbeitung unterrichtet wurden. In dieser Rechtssache hatte die Nationale Agentur der Steuerverwaltung die Beschwerdeführer nicht vorab darüber unterrichtet, dass sie ihre Daten an die Nationale Krankenversicherungsanstalt übermittelt hatte.

Der EuGH befand, dass die gemäß EU-Recht bestehende Pflicht einer Unterrichtung der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen umso wichtiger ist, als es die Voraussetzung dafür

⁵³² EuGH, C-201/14, *Smaranda Bara und andere / Casa Națională de Asigurări de Sănătate und andere*, 1 Oktober 2015.

schaft, dass sie ihr [...] Auskunfts- und Berichtigungsrecht in Bezug auf die verarbeiteten Daten und ihr Recht, der Verarbeitung der Daten zu widersprechen, ausüben können. Der Grundsatz der Verarbeitung nach Treu und Glauben erfordert die Unterrichtung der betroffenen Personen von der Übermittlung ihrer Daten an eine andere Verwaltungsbehörde zu deren Weiterverarbeitung. Nach Maßgabe von Artikel 13 Absatz 1 der Richtlinie 95/46/EG können Mitgliedstaaten das Recht auf Information beschränken, sofern dies für ein wichtiges wirtschaftliches oder finanzielles Interesse des Staates einschließlich Steuerangelegenheiten notwendig ist. Solche Beschränkungen sind jedoch durch Rechtsvorschriften vorzunehmen. Da weder die übermittlungsfähigen Informationen noch die Modalitäten ihrer Übermittlung durch Rechtsvorschriften festgelegt wurden, sondern vielmehr lediglich in einem zwischen den beiden Behörden geschlossenen Protokoll, waren die Voraussetzungen für die Ausnahme unter EU-Recht nicht erfüllt. Die Beschwerdeführer hätten vorab über die Übermittlung ihrer Daten an die Nationalen Krankenversicherungsanstalten und die anschließende Verarbeitung dieser Daten unterrichtet werden müssen.

Inhalt der Information

Gemäß Artikel 8 Absatz 1 des Modernisierten Übereinkommens Nr. 108 ist der Verantwortliche dazu verpflichtet, der betroffenen Person alle Informationen mitzuteilen, die eine nach Treu und Glauben und transparent erfolgende Verarbeitung personenbezogener Daten gewährleisten, darunter:

- die Identität und den Aufenthaltsort oder die Niederlassung des Verantwortlichen;
- die Rechtsgrundlage und den Zweck der Verarbeitung;
- die Kategorien der verarbeiteten personenbezogenen Daten;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- die Art und Weise, wie die betroffenen Personen ihre Rechte ausüben können.

Die DSGVO besagt: Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:⁵³³

- den Namen und die Kontaktdaten des Verantwortlichen, einschließlich gegebenenfalls der Kontaktdaten des DSB;
- die Zwecke und die Rechtsgrundlage für die Verarbeitung, d. h. ein Vertrag oder eine rechtliche Verpflichtung;
- das berechtigte Interesse des Verantwortlichen, sofern es die Grundlage für die Verarbeitung darstellt;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- ob die Daten an ein Drittland oder an eine internationale Organisation übermittelt werden und ob dies auf einem Angemessenheitsbeschluss beruht oder auf geeigneten Garantien stützt;
- die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls die Festsetzung dieser Dauer nicht möglich ist, die Kriterien für die Festlegung der Dauer der Datenspeicherung;
- die Rechte der betroffenen Personen in Bezug auf die Verarbeitung, wie das Recht auf Auskunft, Berichtigung, Löschung und auf Einschränkung der Verarbeitung oder das Widerspruchsrecht gegen die Verarbeitung;
- ob die Bereitstellung personenbezogener Daten gesetzlich oder durch einen Vertrag vorgeschrieben ist, ob die betroffene Person verpflichtet ist, ihre personenbezogenen Daten bereitzustellen, sowie die Folgen im Falle der Nichtbereitstellung personenbezogener Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling;

⁵³³ DSGVO, Artikel 13 Absatz 1.

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- das Bestehen eines Rechts auf Widerruf der Einwilligung.

In Fällen einer automatisierten Entscheidungsfindung, einschließlich Profiling, müssen die betroffenen Personen aussagekräftige Informationen über die beim Profiling angewandte Logik, dessen Aussagekraft und die angestrebten Konsequenzen, die sie aufgrund der Verarbeitung zu erwarten haben, erhalten.

In Fällen, in denen die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben wurden, teilt der Verantwortliche der Person die Quelle der personenbezogenen Daten mit. In jedem Fall unterrichtet der Verantwortliche die betroffenen Personen unter anderem über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling.⁵³⁴ Beabsichtigt ein Verantwortlicher schließlich, die personenbezogenen Daten für einen anderen als den ursprünglich angegebenen Zweck zu verarbeiten, erfordern die Grundsätze der Zweckbindung und der Transparenz, dass der Verantwortliche der betroffenen Person Informationen über diesen neuen Zweck zur Verfügung stellt. Diese Informationen sind seitens der Verantwortlichen vor jedweder Weiterverarbeitung bereitzustellen. Anders ausgedrückt: In Fällen, in denen die betroffene Person ihre Einwilligung zur Verarbeitung der personenbezogenen Daten erteilt hat, muss der Verantwortliche die erneute Einwilligung der betroffenen Person einholen, sofern sich der Zweck der Datenverarbeitung ändert oder weitere Zwecke hinzugefügt werden.

Zeitpunkt der Information

Die DSGVO unterscheidet zwischen zwei Szenarien und zwei Zeitpunkten, zu denen der Verantwortliche der betroffenen Person Informationen zur Verfügung stellen muss:

- Wenn die personenbezogenen Daten direkt bei der betroffenen Person erhoben werden, muss der Verantwortliche die betroffene Person zum Zeitpunkt der Erhebung dieser Daten über alle sie betreffenden Informationen und ihre Rechte im Rahmen der DSGVO benachrichtigen.⁵³⁵ Beabsichtigt

⁵³⁴ DSGVO, Artikel 13 Absatz 2 und Artikel 14 Absatz 2 Buchstabe f.

⁵³⁵ a.a.O., Artikel 13 Absatz 1 und 2, Einleitung, in der die DSGVO darauf verweist, dass diese Pflicht „zum Zeitpunkt der Erhebung dieser Daten“ Anwendung findet.

der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten, stellt er alle maßgeblichen Informationen zur Verfügung noch bevor diese Verarbeitung stattfindet.

- Wenn die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben wurden, ist der Verantwortliche „innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats“ oder vor der Offenlegung der Daten an einen Dritten zu der an die betroffene Person erfolgenden Bereitstellung der Informationen verpflichtet.⁵³⁶

Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 sieht vor, dass im Falle der Unmöglichkeit der Unterrichtung der betroffenen Personen bei Beginn der Verarbeitung, diese Unterrichtung zu einem späteren Zeitpunkt erfolgen kann, wie beispielsweise wenn der Verantwortliche aus irgendeinem Grund Kontakt zur betroffenen Person hat.⁵³⁷

Unterschiedliche Wege für die Information

Sowohl im Recht des Europarats als auch im EU-Recht müssen die seitens des Verantwortlichen den betroffenen Personen übermittelten Informationen präzise, transparent, verständlich und leicht zugänglich sein. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer, auch elektronischer Form, in klarer, einfacher und leicht verständlicher Sprache. Bei der Bereitstellung der Informationen kann der Verantwortliche auf standardisierte Bildsymbole zurückgreifen, um die Informationen in leicht wahrnehmbarer und verständlicher Form zu übermitteln.⁵³⁸ Ein Bildsymbol, das ein Schloss darstellt, kann beispielsweise verwendet werden, um zu signalisieren, dass die Daten sicher erhoben wurden und/oder verschlüsselt sind. Die betroffenen Personen können die mündliche Erteilung der Information verlangen. Die Informationen müssen unentgeltlich sein, es sei denn, die Anträge der betroffenen Person sind offenkundig unbegründet oder exzessiv (d. h. sie werden häufig

536 a.a.O., Artikel 13 Absatz 3 und Artikel 14 Absatz 3; siehe auch den Verweis auf angemessene Zeitabstände und ohne unzumutbare Verzögerung im Modernisierten Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe b.

537 Erläuternder Bericht zum Modernisierten Übereinkommen Nr. 108, Absatz 68.

538 Die Europäische Kommission wird die Informationen, die durch Bildsymbole darzustellen sind, und die Verfahren für die Bereitstellung standardisierter Bildsymbole durch delegierte Rechtsakte weiter ausbauen; siehe DSGVO, Artikel 12 Absatz 8.

wiederholt).⁵³⁹ Der leichte Zugang zu den bereitgestellten Informationen ist von entscheidender Bedeutung für die Möglichkeit der betroffenen Person, ihre Rechte im Rahmen des EU-Datenschutzrechts auszuüben.

Der Grundsatz der Verarbeitung nach Treu und Glauben erfordert, dass die Informationen für die betroffenen Personen leicht verständlich sind. Die verwendete Sprache muss für die Empfänger geeignet sein. Das Niveau und die Art der verwendeten Sprache müssten sich danach richten, ob es sich bei den vorgesehenen Empfängern beispielsweise um Erwachsene oder um Kinder, um die breite Öffentlichkeit oder um einen Wissenschaftler handelt. Die Frage, wie dieser Aspekt der verständlichen Informationen abgewogen werden kann, wurde in der Stellungnahme der Artikel-29-Datenschutzgruppe zu einheitlicheren Bestimmungen über Informationspflichten geprüft. Sie wirbt für die Idee der so genannten Mehrebenen-Erklärungen,⁵⁴⁰ bei denen die betroffene Person entscheiden kann, welchen Ausführlichkeitsgrad sie bevorzugt. Diese Art der Informationsdarstellung befreit den Verantwortlichen jedoch nicht von seiner Verpflichtung unter Artikel 1 und Artikel 14 DSGVO. Der Verantwortliche muss der betroffenen Person nach wie vor alle Informationen bereitstellen.

Eine der wirksamsten Arten der Informationsbereitstellung ist die Einstellung von geeigneten Informationsklauseln wie Website-Datenschutzbestimmungen auf der Website des Verantwortlichen. Gleichwohl nutzt ein wesentlicher Teil der Bevölkerung kein Internet, was die Informationspolitik eines Unternehmens oder einer Behörde berücksichtigen sollte.

Eine Datenschutzerklärung in Bezug auf die Verarbeitung personenbezogener Daten auf einer Website könnte wie folgt aussehen:

Wer sind wir?

Der „Verantwortliche“ für die Datenverarbeitung ist Bed and Breakfast C&U mit Sitz in [Anschrift: xxx], Tel.: xxx; Fax: xxx; E-Mail-Adresse info@c&u.com; Kontaktdaten des Datenschutzbeauftragten: [xxx].

539 DSGVO, Artikel 12 Absatz 1, 5 und 7 und Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe b.

540 Artikel-29-Datenschutzgruppe (2004), *Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten*, WP 100, Brüssel, 25. November 2004.

Die Informationserklärung über personenbezogene Daten ist Teil der unsere Hoteldienste regelnden Allgemeinen Geschäftsbedingungen.

Welche Daten erheben wir bei Ihnen?

Wir erheben ihre nachstehenden personenbezogenen Daten: Name, Postanschrift, Telefonnummer, E-Mail-Adresse, Informationen über Ihren Aufenthaltsort, Kredit- und ec-Kartenummer und IP-Adressen oder Domainnamen der Computer, die Sie für die Verbindung mit unserer Website benutzt haben.

Warum erheben wir Ihre Daten?

Wir verarbeiten Ihre Daten auf Grundlage Ihrer Einwilligung und für die Zwecke der Durchführung von Buchungen, für den Abschluss und die Erfüllung der Verträge im Zusammenhang mit den von uns angebotenen Dienstleistungen und zur Einhaltung der gesetzlich auferlegten Erfordernisse. Dies ist wie beispielsweise das Kommunalabgabengesetz, das uns zur Erhebung personenbezogener Daten verpflichtet, um eine Kurtaxe für ihren Aufenthalt entrichten zu können.

Wie verarbeiten wir Ihre Daten?

Ihre personenbezogenen Daten werden über einen Zeitraum von drei Monaten gespeichert. Ihre Daten unterliegen keinen automatisierten Entscheidungsverfahren.

Unser Bed and Breakfast C&U setzt strenge Sicherheitsverfahren ein, um zu gewährleisten, dass Ihre personenbezogenen Daten nicht beschädigt, zerstört oder ohne Ihre Erlaubnis Dritten gegenüber offengelegt werden, sowie zur Verhinderung von unbefugtem Zugang. Die Computer, auf denen die Daten gespeichert sind, werden in einer sicheren Umgebung mit beschränktem Zugang aufbewahrt. Wir verwenden sichere Firewalls und andere Maßnahmen zur Beschränkung des elektronischen Zugangs. Sollte es erforderlich sein, die Daten an eine andere Stellen zu übermitteln, so verlangen wir von dieser, dass sie über ähnliche Maßnahmen zum Schutz Ihrer personenbezogenen Daten verfügt.

Sämtliche von uns erhobenen oder gespeicherten Daten sind auf unsere Büros beschränkt. Nur Personen, die diese Daten zur Erfüllung ihrer Aufgaben im Rahmen des vorliegenden Vertrags benötigen, wird Zugang zu den personenbezogenen Daten gewährt. Wir werden Sie ausdrücklich fragen, wenn wir Informationen zu Ihrer Identifizierung benötigen. Bevor wir Ihnen Daten mitteilen, müssen Sie sich möglicherweise unseren Sicherheitskontrollen unterziehen. Die Aktualisierung Ihrer uns bereitgestellten personenbezogenen Daten ist jederzeit durch direkte Kontaktaufnahme mit uns möglich.

Welche Rechte haben Sie?

Sie haben das Recht auf Auskunft über Ihre Daten, das Recht auf den Erhalt einer Kopie Ihrer Daten, das Recht auf Löschung oder Berichtigung und das Recht auf Datenübertragung an einen anderen Verantwortlichen.

Ihre Anträge können Sie uns per E-Mail an info@c&u.com übermitteln. Wir müssen Ihre Anträge innerhalb eines Monats beantworten. Sollte Ihr Antrag zu komplex sein oder sollten zu viele andere Anträge bei uns eingehen, setzen wir Sie darüber in Kenntnis, dass dieser Zeitraum um weitere zwei Monate verlängert werden kann.

Auskunft über Ihre personenbezogenen Daten

Sie haben das Recht auf Auskunft über Ihre Daten, auf Anfrage erhalten Sie Kenntnis über die der Datenverarbeitung zugrunde liegende Logik, das Recht auf Löschung oder Berichtigung Ihrer Daten und das Recht, keiner rein automatisierten Entscheidung ohne Berücksichtigung Ihres Standpunkts zu unterliegen. Ihre Anträge können Sie uns per E-Mail an info@c&u.com übermitteln. Sie haben auch das Recht, der Verarbeitung zu widersprechen, Ihre Einwilligung zu widerrufen und eine Beschwerde bei der nationalen Aufsichtsbehörde einzulegen, sofern Sie der Ansicht sind, dass die Datenverarbeitung unter Verstoß gegen das Gesetz erfolgt, und Schadensersatz für den infolge der unrechtmäßigen Verarbeitung erlittenen Schaden geltend zu machen.

Das Recht auf Beschwerde

Die DSGVO verpflichtet den Verantwortlichen zur Unterrichtung der betroffenen Personen über im nationalen Recht und im EU-Recht bestehende gerichtliche und außergerichtliche Rechtsmittel, wenn gegen die Vorschriften zum Schutz personenbezogener Daten verstoßen wird. Der Verantwortliche muss die betroffenen Personen über ihr Beschwerderecht bei einer Aufsichtsbehörde und falls erforderlich bei einem nationalen Gericht unterrichten. Auch das Recht des Europarates beinhaltet das Recht der betroffenen Personen, darüber informiert zu werden, wie sie ihre Rechte ausüben können, einschließlich über das in Artikel 9 Absatz 1 Buchstabe f niedergelegte Recht auf ein Rechtsmittel.⁵⁴¹

Ausnahmen von der Informationspflicht

Die DSGVO sieht Ausnahmen von der Informationspflicht vor. Gemäß Artikel 13 Absatz 4 und Artikel 14 Absatz 5 DSGVO findet die Pflicht zur Information der betroffenen Personen keine Anwendung, wenn die betroffene Person bereits über die maßgeblichen Informationen verfügt.⁵⁴² Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, findet die Informationspflicht überdies keine Anwendung, wenn die Erteilung dieser Informationen sich als unmöglich oder unverhältnismäßig erweist, und insbesondere wenn die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erfolgt.⁵⁴³

Darüber hinaus genießen die Mitgliedstaaten unter der DSGVO einen Ermessensspielraum zur Beschränkung der den Personen im Rahmen der Verordnung eingeräumten Rechte und Pflichten, sofern diese Beschränkung in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die beispielsweise die nationale und öffentliche Sicherheit, die Landesverteidigung, den Schutz von gerichtlichen Ermittlungen und Gerichtsverfahren oder den Schutz von wirtschaftlichen und finanziellen Interessen sowie privaten Interessen sicherstellt, die in der Abwägung höher gewichtig sind als Datenschutzinteressen.⁵⁴⁴

541 DSGVO, Artikel 13 Absatz 2 Buchstabe d und Artikel 14 Absatz 2 Buchstabe e; Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe f.

542 a.a.O., Artikel 13 Absatz 4 und Artikel 14 Absatz 5 Buchstabe a.

543 a.a.O., Artikel 14 Absatz 5, Buchstabe b - e.

544 DSGVO, Artikel 23 Absatz 1.

Alle Ausnahmen und Beschränkungen müssen in einer demokratischen Gesellschaft notwendig sein und in einem angemessenen Verhältnis zum verfolgten Ziel stehen. In sehr seltenen Ausnahmefällen wie beispielsweise aufgrund ärztlicher Empfehlung kann der Schutz der betroffenen Person selbst eine Beschränkung der Transparenz erfordern; dies betrifft insbesondere das grundsätzliche Auskunftsrecht jeder betroffenen Person.⁵⁴⁵ Als Mindestschutzniveau muss das nationale Recht jedoch den Wesensgehalt der nach Maßgabe des EU-Rechts geschützten Grundrechte und Freiheiten wahren.⁵⁴⁶ Dies erfordert, dass das nationale Recht spezifische Vorschriften enthält, die den Zweck der Verarbeitung, die Kategorien der einbezogenen personenbezogenen Daten, die Garantien und andere Verfahrensvorschriften klarstellen.⁵⁴⁷

Werden Daten zu wissenschaftlichen oder historischen Forschungszwecken, zu statistischen Zwecken oder für im öffentlichen Interesse liegende Archivzwecke erfasst, können im Unionsrecht oder im Recht der Mitgliedstaaten Ausnahmen von der Informationspflicht vorgesehen werden, sofern diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen.⁵⁴⁸

Ähnliche Anwendungsgrenzen existieren im Recht des Europarates. Hier können Rechte, die betroffenen Personen nach Artikel 9 des Modernisierten Übereinkommens 108 zustehen, unter strengen Voraussetzungen gemäß Artikel 11 des Modernisierten Übereinkommen 108 eingeschränkt werden. Zudem ist laut Artikel 8 Absatz 2 des Modernisierten Übereinkommens 108 die Verpflichtung der Verantwortlichen zur transparenten Datenverarbeitung nicht gegeben, sofern die betroffene Person bereits die Information besitzt.

Das Recht auf Auskunft über die eigenen Daten

Im Recht des Europarates ist das Recht auf Auskunft über die eigenen Daten ausdrücklich in Artikel 9 des Modernisierten Übereinkommens Nr. 108 anerkannt. Dieser Artikel sieht vor, dass jede Person auf Anfrage das Recht hat, Informationen über die Verarbeitung ihrer personenbezogenen Daten zu erhalten, die ihr in einer verständlichen Form mitgeteilt werden müssen. Das Auskunftsrecht wurde nicht nur in den Bestimmungen des Modernisierten

⁵⁴⁵ DSGVO, Artikel 15.

⁵⁴⁶ DSGVO, Artikel 23 Absatz 1.

⁵⁴⁷ a.a.O., Artikel 23 Absatz 2.

⁵⁴⁸ a.a.O., Artikel 89 Absatz 2 und 3.

Übereinkommens Nr. 108 anerkannt, sondern auch in der Rechtsprechung des EGMR. Der EGMR befand wiederholt, dass Personen ein Recht auf Auskunft über ihre personenbezogenen Daten haben und dieses Recht aus der Achtung des Privatlebens resultiert.⁵⁴⁹ Gleichwohl kann das Recht auf Auskunft über die seitens öffentlicher oder privater Einrichtungen gespeicherten personenbezogenen Daten unter gewissen Umständen eingeschränkt sein.⁵⁵⁰

Im EU-Recht wird das Recht auf Auskunft über die eigenen Daten in Artikel 15 DSGVO ausdrücklich anerkannt und in Artikel 8 Absatz 2 der Charta der Grundrechte der Europäischen Union auch als Bestandteil des Grundrechts auf Schutz personenbezogener Daten niedergelegt.⁵⁵¹ Das Recht des Einzelnen auf Auskunft über seine personenbezogenen Daten ist ein zentraler Bestandteil des europäischen Datenschutzrechts.⁵⁵²

Die DSGVO sieht vor, dass jede betroffene Person das Recht auf Auskunft über ihre personenbezogenen Daten und bestimmte Informationen über die Verarbeitung hat, die der Verantwortliche bereitzustellen hat.⁵⁵³ Insbesondere hat jede betroffene Person das Recht, (vom Verantwortlichen) eine Bestätigung darüber zu erlangen, ob sie betreffende personenbezogene Daten verarbeitet werden, sowie zumindest die nachstehenden Informationen:

- die Verarbeitungszwecke;
- die Kategorien der Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die Daten offengelegt werden;
- die geplante Dauer, für die die Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

549 EGMR, *Gaskin / Vereinigtes Königreich*, Nr. 10454/83, 7. Juli 1989; EGMR, *Odièvre / Frankreich* [GK], Nr. 42326/98, 13. Februar 2003; EGMR, *K.H. und andere / Slowakei*, Nr. 32881/04, 28. April 2009; EGMR, *Godelli / Italien*, Nr. 33783/09, 25. September 2012.

550 EGMR, *Leander / Schweden*, Nr. 9248/81, 26. März 1987.

551 Siehe auch EuGH, Verbundene Rechtssachen C-141/12 und C-372/12, *YS / Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel / M und S*, 17. Juli 2014; EuGH, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) / Europäische Behörde für Lebensmittelsicherheit (EFSA), Europäische Kommission*, 16. Juli 2015.

552 EuGH, Verbundene Rechtssachen C-141/12 und C-372/12, *YS / Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel / M und S*, 17. Juli 2014.

553 DSGVO, Artikel 15 Absatz 1.

- das Bestehen von Rechten auf Berichtigung oder Löschung der personenbezogenen Daten oder auf Einschränkung der Verarbeitung personenbezogener Daten;
- das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde;
- wenn die Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der zu verarbeitenden Daten;
- im Falle automatisierter Entscheidungen die mit der automatisierten Verarbeitung der Daten verbundene Logik.

Der Verantwortliche hat der betroffenen Person eine Kopie der zu verarbeitenden personenbezogenen Daten zur Verfügung zu stellen. Jedwede an die betroffene Person erfolgende Informationsübermittlung muss in verständlicher Form erfolgen, was bedeutet, dass der Verantwortliche sicherstellen muss, dass die betroffene Person die bereitgestellten Informationen verstehen kann. So reicht es beispielsweise normalerweise nicht aus, in eine Auskunftsanfrage technische Abkürzungen, verschlüsselte Begriffe oder Abkürzungen einzufügen, es sei denn, die Bedeutung dieser Begriffe wird erklärt. Im Falle der Durchführung einer automatisierten Entscheidungsfindung einschließlich Profiling, ist die mit der automatisierten Entscheidungsfindung verbundene allgemeine Logik zu erklären, einschließlich der Kriterien, die bei der Bewertung der betroffenen Person berücksichtigt wurden. Im **Recht des Europarates** gibt es ähnliche Anforderungen.⁵⁵⁴

Beispiel: Hat die betroffene Person Einsicht in ihre personenbezogenen Daten, hilft ihr dies bei der Ermittlung, ob die Daten sachlich richtig sind oder nicht. Daher ist es von wesentlicher Bedeutung, dass die betroffene Person in verständlicher Form sowohl über die tatsächlich verarbeiteten personenbezogenen Daten als auch über die Kategorien unterrichtet wird, unter denen diese personenbezogenen Daten verarbeitet werden, wie Name, IP-Adresse, Standortkoordinaten, Kreditkartennummer, usw.

Wenn die Daten nicht bei der betroffenen Person erhoben werden, müssen Informationen über die Quelle der Daten auf ein Auskunftersuchen hin

⁵⁵⁴ Siehe Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe c.

gegeben werden, sofern diese Informationen vorliegen. Diese Bestimmung ist vor dem Hintergrund der Grundsätze der Verarbeitung nach Treu und Glauben, der Transparenz und der Rechenschaftspflicht zu sehen. Ein Verantwortlicher darf Informationen über die Quelle der Daten nicht vernichten, um sie nicht weitergeben zu müssen, es sei denn, die Löschung hätte auch ohne Erhalt des Auskunftersuchens stattgefunden. Ebenso muss er nach wie vor seinen allgemeinen Verpflichtungen in Bezug auf die „Rechenschaftspflicht“ nachkommen.

Wie in der Rechtsprechung des EuGH dargelegt, darf das Recht auf Auskunft über personenbezogene Daten nicht ungebührlich durch Zeitlimits eingeschränkt werden. Den betroffenen Personen muss auch eine angemessene Möglichkeit geboten werden, etwas über vergangene Datenverarbeitungen in Erfahrung zu bringen.

Beispiel: In der Rechtssache *Rijkeboer*⁵⁵⁵ sollte der EuGH darüber entscheiden, ob das Recht einer natürlichen Person auf Auskunft über die Empfänger oder Kategorien von Empfängern personenbezogener Daten und den Inhalt der Daten auf ein Jahr vor ihrem Auskunftersuchen beschränkt werden durfte.

Um feststellen zu können, ob die EU-Gesetze eine solche zeitliche Begrenzung zulassen, beschloss der Gerichtshof, Artikel 12 im Licht der mit der Richtlinie verfolgten Ziele auszulegen. Zunächst befand der EuGH, dass dieses Auskunftsrecht erforderlich ist, um der betroffenen Person die Wahrnehmung des Rechts auf Berichtigung, Löschung oder Sperrung ihrer Daten durch den Verantwortlichen oder die Mitteilung dieser Berichtigung, Löschung oder Sperrung an Dritte, an die diese Daten übermittelt worden sind, zu ermöglichen. Ein wirksames Auskunftsrecht ist außerdem notwendig, um der betroffenen Person ihr Recht auf Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten oder ihr Recht auf Beschwerde und Geltendmachung von Schadensersatz zu ermöglichen.⁵⁵⁶

Um die praktische Wirksamkeit der den betroffenen Personen eingeräumten Rechte zu gewährleisten, muss nach Auffassung des EuGH „das Recht zwingend für die Vergangenheit gelten. Denn andernfalls wäre die betroffene

⁵⁵⁵ EuGH, C-553/07, *College van burgemeester en wethouders van Rotterdam / M. E. E. Rijkeboer*, 7. Mai 2009.

⁵⁵⁶ DSGVO, Artikel 15 Absatz 1 Buchstabe c und f, Artikel 16, Artikel 17 Absatz 2 und Artikel 21, und Kapitel VIII.

Person weder in der Lage, wirksam ihr Recht auf Berichtigung, Löschung oder Sperrung von Daten wahrzunehmen, die ihrer Ansicht nach unbefugt verarbeitet wurden oder falsch sind, noch, einen gerichtlichen Rechtsbehelf einzulegen und Schadenersatz zu erlangen“.

6.1.2. Recht auf Berichtigung

Sowohl **im EU-Recht** als auch **im Recht des Europarates** haben die betroffenen Personen das Recht auf Berichtigung ihrer personenbezogenen Daten. Die Richtigkeit personenbezogener Daten ist von wesentlicher Bedeutung, um den betroffenen Personen ein hohes Datenschutzniveau zu gewährleisten.⁵⁵⁷

Beispiel: In der Rechtssache *Ciubotaru gegen Republik Moldau*⁵⁵⁸ konnte der Beschwerdeführer die Angabe seiner ethnischen Herkunft in amtlichen Dokumenten nicht von „moldawisch“ in „rumänisch“ ändern, weil er angeblich seinen Antrag nicht ausreichend begründet hatte. Nach Auffassung des EGMR ist es durchaus vertretbar, dass Staaten bei der Erfassung der ethnischen Identität einer Person objektive Beweise verlangen. Seien solche Behauptungen rein subjektiv und nicht belegt, könnten die Behörden den Antrag ablehnen. Der Beschwerdeführer hatte sich jedoch bei seinem Antrag auf mehr als die subjektive Wahrnehmung seiner eigenen ethnischen Zugehörigkeit gestützt; er konnte vielmehr objektiv überprüfbare Bindungen zur rumänischen ethnischen Gruppe wie Sprache, Name, Empathie und andere belegen. Nach innerstaatlichem Recht musste der Beschwerdeführer gleichwohl den Beweis dafür vorlegen, dass seine Eltern der rumänischen Ethnie angehört hatten. In Anbetracht der historischen Gegebenheiten der Republik Moldau hätte eine solche Anforderung ein unüberwindliches Hindernis für die Eintragung einer anderen als der von den sowjetischen Behörden für seine Eltern eingetragenen ethnischen Identität bedeutet. Der Staat hatte verhindert, dass der Antrag des Beschwerdeführers im Lichte objektiv überprüfbarer Beweise geprüft wurde und kam damit seiner positiven Verpflichtung nicht nach, die wirksame Achtung des Privatlebens des Beschwerdeführers sicherzustellen. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

557 a.a.O., Artikel 16 und Erwägungsgrund 65; Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe e.

558 EGMR, *Ciubotaru / Republik Moldau*, Nr. 27138/04, 27. April 2010, Randnrn. 51 und 59.

Mitunter möchte die betroffene Person nur einfach eine Berichtigung beispielsweise der Schreibweise eines Namens oder die Eintragung einer neuen Anschrift oder Telefonnummer beantragen. Nach Maßgabe des **EU-Rechts** und des **Rechts des Europarates** sind unrichtige personenbezogene Daten unverzüglich und ohne unzumutbare Verzögerung zu berichtigen.⁵⁵⁹ Geht es in solchen Anträgen allerdings um rechtlich wichtige Aspekte wie die Rechtspersönlichkeit der betroffenen Person oder den korrekten Wohnort für die Zustellung von amtlichen Dokumenten, reicht ein Antrag auf Berichtigung möglicherweise nicht aus und der Verantwortliche kann befugt sein, einen Nachweis der angeblichen fehlenden Richtigkeit der Daten zu verlangen. Solche Forderungen dürfen für die betroffene Person keine unverhältnismäßige Beweislast bedeuten und damit betroffene Personen daran hindern, die Berichtigung ihrer Daten zu erlangen. Der EGMR befand auf eine Verletzung von Artikel 8 EMRK in mehreren Fällen, in denen es dem Beschwerdeführer versagt war, die Richtigkeit der in Geheimregistern gespeicherten Daten in Frage zu stellen.⁵⁶⁰

Beispiel: In der Rechtssache *Cemalettin Canli gegen Türkei*⁵⁶¹ stellte der EGMR eine Verletzung von Artikel 8 EMRK durch unrichtige Angaben der Polizei in Strafverfahren fest.

Der Beschwerdeführer wurde zweimal in Strafverfahren wegen mutmaßlicher Mitgliedschaft in einer kriminellen Vereinigung angeklagt, war aber nicht verurteilt worden. Als der Beschwerdeführer ein weiteres Mal verhaftet und einer anderen Straftat angeklagt wurde, legte die Polizei dem Strafgericht einen Bericht mit dem Titel „*Informationsblatt zu weiteren Straftaten*“ vor, in dem der Beschwerdeführer als Mitglied zweier krimineller Vereinigungen dargestellt wurde. Vergeblich beantragte der Beschwerdeführer eine Änderung des Berichts und der polizeilichen Unterlagen. Nach Auffassung des EGMR fielen die Informationen im Polizeibericht in den Anwendungsbereich von Artikel 8 EMRK, da systematisch erhobene öffentlich verfügbare Informationen, die in Akten bei Behörden gespeichert werden, durchaus zum „Privatleben“ gerechnet werden können. Des Weiteren sei die Abfassung des Polizeiberichts unrichtig gewesen und seine Vorlage bei Gericht habe nicht im Einklang mit dem Gesetz gestanden. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 vorlag.

559 DSGVO, Artikel 16, Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1.

560 EGMR, *Rotaru / Rumänien* [GK], Nr. 28341/95, 4. Mai 2000.

561 EGMR, *Cemalettin Canli / Türkei*, Nr. 22427/04, 18. November 2008, Randnrn. 33 und 42–43; EGMR, *Dalea / Frankreich*, Nr. 964/07, 2. Februar 2010.

Um in Zivil- oder Verwaltungsverfahren entscheiden zu können, ob die Daten richtig sind oder nicht, kann die betroffene Person beantragen, einen Vermerk zu ihrem Datensatz zu nehmen, der besagt, dass die Richtigkeit angefochten wird und eine offizielle Entscheidung aussteht.⁵⁶² In diesem Zeitraum darf der Verantwortliche insbesondere gegenüber Dritten die Daten nicht als richtig oder endgültig darstellen.

6.1.3. Recht auf Löschung („Recht auf Vergessenwerden“)

Den betroffenen Personen ein Recht auf Löschung ihrer personenbezogenen Daten einzuräumen, ist für die Wirksamkeit der Datenschutzgrundsätze und insbesondere des Grundsatzes der Datenminimierung (personenbezogene Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein) von besonderer Bedeutung. Daher ist das Recht auf Löschung sowohl im Recht des Europarates als auch im EU-Recht anzutreffen.⁵⁶³

Beispiel: In der Rechtssache *Segerstedt-Wiberg und andere gegen Schweden*⁵⁶⁴ waren die Beschwerdeführer Mitglieder bestimmter liberaler und kommunistischer politischer Parteien. Sie hegten den Verdacht, dass Daten über sie in Akten der Sicherheitspolizei eingegeben worden waren und beantragten deren Löschung. Der EGMR zeigte sich zufrieden damit, dass die in Frage stehende Datenspeicherung eine Rechtsgrundlage hatte und einem rechtmäßigen Ziel diene. Bezüglich einiger der Beschwerdeführer befand der EGMR jedoch, die fortgesetzte Speicherung der Daten sei ein unverhältnismäßiger Eingriff in ihr Privatleben. Im Fall eines Beschwerdeführers beispielsweise würden die Behörden nach wie vor speichern, er habe sich 1969 angeblich für gewalttätigen Widerstand gegen Polizeikontrollen bei Demonstrationen eingesetzt. Nach Auffassung des EGMR konnte diese Information, insbesondere aufgrund ihres historischen Charakters, kaum von Bedeutung für die nationalen Sicherheitsinteressen gewesen sein. Bei vier der fünf Beschwerdeführer befand der EGMR, dass eine Verletzung von Artikel 8 EMRK vorlag, da die fortgesetzte Speicherung

⁵⁶² DSGVO, Artikel 18 und Erwägungsgrund 67.

⁵⁶³ a.a.O., Artikel 17.

⁵⁶⁴ EGMR, *Segerstedt-Wiberg und andere / Schweden*, Nr. 62332/00, 6. Juni 2006, Randnrn. 89 und 90; siehe beispielsweise auch EGMR, *M.K. / Frankreich*, Nr. 19522/09, 18. April 2013.

ihrer Daten in Anbetracht der langen Zeitspanne seit den angeblichen Handlungen des Beschwerdeführers nicht sachdienlich sei.

Beispiel: In der Rechtssache *Brunet gegen Frankreich*⁵⁶⁵ beklagten sich die Beschwerdeführer über die Speicherung ihrer personenbezogenen Daten in einer Polizeidatenbank, die Informationen über Verurteilte, Angeklagte und Opfer enthielt. Obgleich das Strafverfahren gegen den Beschwerdeführer eingestellt worden war, erschienen seine Angaben in der Datenbank. Der EGMR stellte eine Verletzung von Artikel 8 EMRK fest. Der Gerichtshof schlussfolgerte, dass für den Beschwerdeführer in der Praxis keine Möglichkeit bestand, seine personenbezogenen Daten aus der Datenbank löschen zu lassen. Der EGMR prüfte auch die Art der in der Datenbank enthaltenen Informationen und erachtete diese als Eingriff in die Privatsphäre des Beschwerdeführers, da sie Einzelheiten zu seiner Identität und Persönlichkeit enthielten. Darüber hinaus befand der Gerichtshof, dass die 20-jährige Speicherfrist für die in der Datenbank enthaltenen personenbezogenen Daten übermäßig lange sei, insbesondere aufgrund der Tatsache, dass der Beschwerdeführer zu keiner Zeit von einem Gericht verurteilt worden war.

Das Modernisierte Übereinkommen Nr. 108 erkennt ausdrücklich an, dass jede Person das Recht auf Löschung unrichtiger, falscher oder unrechtmäßig verarbeiteter Daten hat.⁵⁶⁶

Im EU-Recht gilt Artikel 17 DSGVO für die Anträge der betroffenen Personen auf Löschung von Daten. Das Recht auf die unverzügliche Löschung seiner personenbezogenen Daten findet Anwendung, wenn:

- die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind;
- die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung stützte, widerruft und es keine anderweitige Rechtsgrundlage für die Verarbeitung gibt;
- die betroffene Person Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen;

⁵⁶⁵ EGMR, *Brunet / Frankreich*, Nr. 21010/10, 18. September 2014.

⁵⁶⁶ Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe e.

- die personenbezogenen Daten unrechtmäßig verarbeitet wurden;
- die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist, dem der Verantwortliche unterliegt;
- die personenbezogenen Daten in Bezug auf Kindern angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 DSGVO erhoben wurden.⁵⁶⁷

Die Beweislast für die Zulässigkeit der Datenverarbeitung liegt bei den Verantwortlichen, da sie für die Rechtmäßigkeit der Verarbeitung verantwortlich sind.⁵⁶⁸ Nach Maßgabe des Grundsatzes der Rechenschaftspflicht muss der Verantwortliche jederzeit nachweisen können, dass seine Datenverarbeitung auf einer tragfähigen Rechtsgrundlage beruht, da die Verarbeitung andernfalls eingestellt werden muss.⁵⁶⁹ Die DSGVO definiert Ausnahmen vom Recht auf Vergessenwerden, soweit die Verarbeitung unter anderem aus den nachstehenden Gründen erforderlich ist:

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke;
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.⁵⁷⁰

Der EuGH hat die Bedeutung des Rechts auf Löschung zur Gewährleistung eines hohen Datenschutzniveaus bekräftigt.

⁵⁶⁷ DSGVO, Artikel 17 Absatz 1.

⁵⁶⁸ a.a.O.

⁵⁶⁹ a.a.O., Artikel 5 Absatz 2.

⁵⁷⁰ a.a.O., Artikel 17 Absatz 3.

Beispiel: In der Rechtssache *Google Spain*⁵⁷¹ prüfte der EuGH, ob Google zur Löschung veralteter Informationen über die finanziellen Schwierigkeiten des Beschwerdeführers aus seiner Suchergebnisliste verpflichtet war. Unter anderem bestritt Google seine Verantwortung mit dem Argument, dass es lediglich einen Hyperlink zur Webseite des Herausgebers bereitstellt, der die Informationen hostet, und bei dem es sich im vorliegenden Fall um eine Zeitung handelt, die über die Insolvenzprobleme berichtete.⁵⁷² Google argumentierte, dass das Ersuchen um Löschung veralteter Informationen von einer Webseite an den Host der Webseite und nicht an Google zu richten sei, der lediglich einen Link zur Originalseite bereitstellt. Der EuGH befand, dass Google beim Durchsuchen des World Wide Web nach Informationen und Webseiten und beim Indexieren von Inhalten zur Bereitstellung von Suchergebnissen zu einem Verantwortlichen wird, auf den die Vorschriften über die Verantwortlichkeit und Pflichten des EU-Rechts Anwendung finden.

Der EuGH legte dar, dass Internetsuchmaschinen und Suchergebnisse, die personenbezogene Daten liefern, ein detailliertes Profil einer Person erstellen können.⁵⁷³ Suchmaschinen machen die in einer solchen Suchergebnisliste enthaltenen Informationen allgegenwärtig. In Anbetracht seiner potenziellen Ernsthaftigkeit kann dieser Eingriff nicht nur durch das wirtschaftliche Interesse gerechtfertigt werden, das der Betreiber einer solchen Suchmaschine an dieser Verarbeitung hat. Insbesondere ist zwischen dem berechtigten Interesse der Internetnutzer am Zugang zu Informationen und den Grundrechten der betroffenen Person gemäß Artikel 7 und 8 der Charta der Grundrechte der EU ein faires Gleichgewicht zu finden. In einer zunehmend digitalisierten Gesellschaft ist das Erfordernis, dass personenbezogene Daten sachlich richtig sind und nicht über das (zur Information der Öffentlichkeit) erforderliche Maß hinausgehen, von grundlegender Bedeutung, um den Einzelnen ein hohes Datenschutzniveau

571 EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014, Rdnrn. 55–58.

572 Google bestritt auch die Anwendung der EU-Datenschutzvorschriften, da Google Inc. in den Vereinigten Staaten niedergelassen ist und die Verarbeitung der im vorliegenden Fall strittigen personenbezogenen Daten ebenfalls in den Vereinigten Staaten erfolgte. Ein zweites Argument für die Unanwendbarkeit des EU-Datenschutzrechts betraf die Behauptung, dass Suchmaschinen in Bezug auf die in ihren Suchergebnissen angezeigten Daten nicht als „Verantwortliche“ betrachtet werden könnten, da sie diese Daten weder kennen, noch Kontrolle über sie ausüben. Der EuGH wies beide Argumente zurück und befand, dass die Richtlinie 95/46/EG in diesem Fall Anwendung finde, und setzte die Untersuchung des Umfangs der durch sie garantierten Rechte fort, und insbesondere des Rechts auf Löschung der personenbezogenen Daten.

573 a.a.O., Rdnrn. 36, 38, 80–81 und 97.

zu gewährleisten. Der „für die Verarbeitung Verantwortliche muss in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür sorgen, dass die Verarbeitung den Anforderungen“ des EU-Rechts „genügt“, damit die eingerichteten gesetzlichen Garantien ihre volle Wirkung entfalten.⁵⁷⁴ Dies bedeutet, dass das Recht auf Löschung seiner personenbezogenen Daten im Falle einer veralteten oder nicht länger erforderlichen Verarbeitung auch Verantwortliche umfasst, die die Informationen vervielfältigen.⁵⁷⁵

Im Rahmen der Prüfung, ob Google zur Entfernung der mit dem Beschwerdeführer im Zusammenhang stehenden Links verpflichtet war, befand der EuGH, dass natürliche Personen unter bestimmten Voraussetzungen das Recht auf die Löschung ihrer personenbezogenen Daten haben. Dieses Recht kann geltend gemacht werden, wenn Informationen in Bezug auf eine natürliche Person sachlich unrichtig/ ungenau, unzureichend, für die Zwecke der Datenverarbeitung irrelevant oder übermäßig sind. Der EuGH erkannte an, dass es sich dabei nicht um ein absolutes Recht handelt; es muss gegen andere Rechte und Interessen abgewogen werden, und hierbei insbesondere gegen das Interesse der breiten Öffentlichkeit auf Zugang zu bestimmten Informationen. Jede beantragte Löschung erfordert eine individuelle Abwägung, zwischen den Grundrechten auf Schutz personenbezogener Daten und auf Achtung des Privatlebens der betroffenen Person einerseits und den berechtigten Interessen aller Internetnutzer einschließlich der Herausgeber andererseits. Der EuGH stellte eine Orientierungshilfe in Bezug auf die im Zuge dieses Abwägens zu berücksichtigenden Faktoren bereit. Bei der Art der betroffenen Information handelt es sich um einen besonders wichtigen Faktor. Sofern sich die Information auf das Privatleben der natürlichen Person bezieht und kein öffentliches Interesse an der Verfügbarkeit der Information besteht, überwiegen der Datenschutz und das Recht auf Achtung der Privatsphäre gegenüber dem Recht der breiten Öffentlichkeit auf Zugang zu der Information. Stellt sich hingegen heraus, dass es sich bei der betroffenen

574 a.a.O., Randnrn. 81–83.

575 EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014, Randnr. 88. Siehe auch Artikel-29-Datenschutzgruppe (2014), *Leitlinien für die Umsetzung des Urteils des Gerichtshofs der Europäischen Union in der Rechtssache C-131/12 „Google Spain und Inc / Agencia Española de Protección de Datos (AEPD) und Mario Costeja González“*, WP 225, Brüssel, 26. November 2014 und Empfehlung CM/Rec(2012)3 des Ministerkomitees an die Mitgliedstaaten zum Schutz der Menschenrechte im Hinblick auf Suchmaschinen, 4. April 2012.

Person um eine Persönlichkeit des öffentlichen Lebens handelt, oder die Information derart ist, dass sie die Gewährung des Zugangs der breiten Öffentlichkeit zu dieser Information rechtfertigt, ist der Eingriff in die Grundrechte der betroffenen Person auf Datenschutz und auf Achtung der Privatsphäre gerechtfertigt.

Im Anschluss an das Urteil nahm die Artikel-29-Datenschutzgruppe Leitlinien zur Umsetzung der Entscheidung des EuGH an.⁵⁷⁶ Diese Leitlinien enthalten eine Liste der seitens der Aufsichtsbehörden beim Umgang mit Beschwerden in Bezug auf Löschungsanträge natürlicher Personen anzuwendenden gemeinsamen Kriterien, erläutern die Folgen dieses Rechts auf Löschung und leiten die Aufsichtsbehörden beim Abwägen der Rechte an. Diese Leitlinien wiederholen, dass die Beurteilung von Fall zu Fall erfolgen muss. Da das Recht auf Vergessenwerden kein absolutes Recht ist, kann sich das Ergebnis eines Ersuchens in Abhängigkeit vom jeweiligen Fall unterscheiden. Dies veranschaulicht auch die nach der Rechtssache Google erfolgte Rechtsprechung des EuGH.

Beispiel: In der Rechtssache *Camera di Commercio di Lecce gegen Manni*⁵⁷⁷ musste der EuGH prüfen, ob eine Person nach Auflösung ihres Unternehmens das Recht auf Löschung ihrer in einem Unternehmensregister veröffentlichten personenbezogenen Daten hatte. Herr Manni hatte die Handelskammer von Lecce um die Entfernung seiner personenbezogenen Daten aus diesem Register ersucht, da er herausgefunden hatte, dass potenzielle Kunden auf das Register zurückgreifen und sehen würden, dass er früher der alleinige Geschäftsführer eines Unternehmens war, das über ein Jahrzehnt zuvor für insolvent erklärt worden war. Der Beschwerdeführer war der Ansicht, dass diese Informationen potenzielle Kunden abschrecken würden.

Im Zuge der Abwägung von Herrn Mannis Recht auf Schutz seiner personenbezogenen Daten und dem Interesse der breiten Öffentlichkeit auf Zugang zu den Informationen prüfte der EuGH zunächst den Zweck des Unternehmensregisters. Er wies auf die Tatsache hin, dass die Offenlegung gesetzlich und insbesondere von einer EU-Richtlinie vorgesehen war, die

576 Artikel-29-Datenschutzgruppe (2014), Leitlinien für die Umsetzung des Urteils des Gerichtshofs der Europäischen Union in der Rechtssache C-131/12 „*Google Spain und Inc / Agencia Española de Protección de Datos (AEPD) und Mario Costeja González*“, WP 225, Brüssel, 26. November 2014.

577 EuGH, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni*, 9. März 2017.

den Zugang Dritter zu Unternehmensinformationen erleichtern soll. Dritte sollten folglich Zugang zu den wesentlichen Urkunden einer Gesellschaft sowie einige sie betreffende Angaben haben und diese prüfen können, „insbesondere die Personalien derjenigen, welche die Gesellschaft verpflichten können“. Der Zweck der Offenlegung bestand auch in der Gewährleistung der Rechtssicherheit im Hinblick auf eine Intensivierung des Geschäftsverkehrs zwischen den Mitgliedstaaten durch die Sicherstellung, dass Dritte Zugang zu sämtlichen maßgeblichen Informationen über Gesellschaften in der gesamten EU haben.

Der EuGH stellte überdies fest, dass selbst nach dem Ablauf einer gewissen Zeitspanne und selbst nach der Auflösung einer Gesellschaft die Rechte und rechtlichen Verpflichtungen der Gesellschaft oftmals weiterbestehen. Streitigkeiten in Bezug auf eine Gesellschaftsauflösung können langwierig sein und selbst viele Jahre nach der Auflösung können noch Fragen in Bezug auf die Gesellschaft, ihre Geschäftsführer und Liquidatoren auftauchen. Der EuGH befand, dass es in Anbetracht der Vielzahl der möglichen Szenarien und der Unterschiede der in den einzelnen Mitgliedstaaten vorgesehenen Verjährungsfristen „derzeit nicht möglich [erscheint], eine einheitliche Frist festzulegen, die mit der Auflösung einer Gesellschaft zu laufen beginnt und nach deren Ablauf die Eintragung der Daten im Register und ihre Offenlegung nicht mehr notwendig wären“. Aufgrund des rechtmäßigen Ziels der Offenlegung und der Schwierigkeiten der Festsetzung eines Zeitraums, nach dessen Ablauf die personenbezogenen Daten ohne Verletzung der Interessen Dritter aus dem Unternehmensregister gelöscht werden könnten, befand der EuGH, dass die Datenschutzvorschriften der EU für Personen, die sich in der Situation von Herrn Manni befinden, kein Recht auf Löschung personenbezogener Daten garantieren.

Hat der Verantwortliche personenbezogene Daten öffentlich gemacht und ist er zu deren Löschung verpflichtet, so ist er dazu verpflichtet, „angemessene“ Maßnahmen zu treffen, um andere Verantwortliche, die dieselben Daten verarbeiten, über den Antrag der betroffenen Person auf Löschung zu informieren. Die Maßnahmen des Verantwortlichen müssen die verfügbare Technologie und die Implementierungskosten berücksichtigen.⁵⁷⁸

⁵⁷⁸ DSGVO, Artikel 17 Absatz 2 und Erwägungsgrund 66.

6.1.4. Recht auf Einschränkung der Verarbeitung

Artikel 18 DSGVO ermächtigt die betroffenen Personen vorübergehend den Verantwortlichen bezüglich der Verarbeitung ihrer personenbezogenen Daten einzuschränken. Die betroffenen Personen können von dem Verantwortlichen die Einschränkung der Verarbeitung verlangen, wenn

- die Richtigkeit der personenbezogenen Daten bestritten wird;
- die Verarbeitung unrechtmäßig ist und die betroffene Person statt der Löschung der personenbezogenen Daten die Einschränkung ihrer Nutzung verlangt;
- die Daten zur Geltendmachung oder Verteidigung von Rechtsansprüchen benötigt werden;
- eine Entscheidung anhängig ist, ob die berechtigten Interessen des Verantwortlichen gegenüber den Interessen der betroffenen Person überwiegen.⁵⁷⁹

Die Methoden, mit denen ein Verantwortlicher die Verarbeitung personenbezogener Daten einschränken kann, könnten beispielsweise darin bestehen, dass ausgewählte Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass personenbezogene Daten vorübergehend entfernt werden.⁵⁸⁰ Der Verantwortliche unterrichtet die betroffene Person, bevor die Einschränkung aufgehoben wird.⁵⁸¹

Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Der Verantwortliche muss jede Berichtigung oder Löschung personenbezogener Daten oder jede Beschränkung ihrer Verarbeitung jedem Empfänger mitteilen, dem er die personenbezogenen Daten offengelegt hat, soweit dies nicht

⁵⁷⁹ a.a.O., Artikel 18 Absatz 1.

⁵⁸⁰ a.a.O., Erwägungsgrund 67.

⁵⁸¹ a.a.O., Artikel 18 Absatz 3.

unmöglich oder unverhältnismäßig ist.⁵⁸² Wenn die betroffene Person Informationen über diese Empfänger verlangt, stellt der Verantwortliche ihr diese Informationen bereit.⁵⁸³

6.1.5. Recht auf Datenübertragbarkeit

Die DSGVO gibt den betroffenen Personen das Recht auf Datenübertragbarkeit. Dieses besteht in Situationen, in denen die personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, mithilfe automatisierter Verfahren auf Grundlage ihrer Einwilligung verarbeitet werden oder die Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrags erforderlich ist und mithilfe automatisierter Verfahren erfolgt. Dies bedeutet, dass es kein Recht auf Datenübertragbarkeit gibt, wenn die Verarbeitung der personenbezogenen Daten auf einer anderen Rechtsgrundlage als einer Einwilligung oder eines Vertrags erfolgt.⁵⁸⁴

Greift das Recht auf Datenübertragbarkeit, haben die betroffenen Personen das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.⁵⁸⁵ Um dies zu erleichtern, sollte der Verantwortliche interoperable Formate entwickeln, die den von der Datenverarbeitung betroffenen Personen die Datenübertragbarkeit ermöglichen.⁵⁸⁶ Die DSGVO präzisiert, dass diese Formate zur Erleichterung der Interoperabilität strukturiert, gängig und maschinenlesbar sein müssen.⁵⁸⁷ Im weiteren Sinne kann Interoperabilität als die Fähigkeit von Informationssystemen definiert werden, Daten auszutauschen und die gemeinsame Nutzung von Informationen zu ermöglichen.⁵⁸⁸ Während der Zweck der verwendeten Formate in der Erzielung von Interoperabilität besteht, gibt die DSGVO keine besonderen Empfehlungen in Bezug auf

582 DSGVO Artikel 19.

583 DSGVO, Artikel 19.

584 a.a.O., Erwägungsgrund 68 und Artikel 20 Absatz 1.

585 a.a.O., Artikel 20 Absatz 2.

586 a.a.O., Erwägungsgrund 68 und Artikel 20 Absatz 1.

587 a.a.O., Erwägungsgrund 68.

588 Europäische Kommission, Mitteilung über solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit, COM(2016) 205 final, 2. April 2016.

das bereitzustellende spezifische Format vor: Formate können je nach Sektor unterschiedlich sein.⁵⁸⁹

Den Leitlinien der Artikel-29-Datenschutzgruppe zufolge, „fördert“ das Recht auf Datenübertragbarkeit „die Wahl- und Kontrollmöglichkeiten der Nutzer und die Selbstbestimmung der Verbraucher“ und zielt darauf ab, den betroffenen Personen Kontrolle über ihre personenbezogenen Daten zu verleihen.⁵⁹⁰ Die Leitlinien verdeutlichen die wesentlichen Elemente der Datenübertragbarkeit, darunter:

- das Recht der betroffenen Personen, die sie betreffenden und vom Verantwortlichen verarbeiteten personenbezogenen Daten in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten;
- das Recht zur Übermittlung personenbezogener Daten von einem Verantwortlichen an einen anderen Verantwortlichen „ohne Behinderung“, soweit dies technisch machbar ist;
- das System der Kontrolle – wenn ein Verantwortlicher eine Anfrage zur Datenübertragbarkeit beantwortet, handelt er auf Anweisung der betroffenen Person, was bedeutet, dass er nicht für die Einhaltung des Datenschutzrechts seitens des Empfängers haftet, da die betroffene Person entscheidet, an wen die Daten übermittelt werden;
- die Ausübung des Rechts auf Datenübertragbarkeit (oder eines anderen in der DSGVO verankerten Rechts) erfolgt unbeschadet anderer Rechte.

6.1.6. Widerspruchsrecht

Betroffene Personen können der Verarbeitung ihrer personenbezogener Daten aufgrund ihrer besonderen Situation und im Falle der Verarbeitung von Daten für Zwecke der Direktwerbung widersprechen. Das Widerspruchsrecht kann mittels automatisierter Verfahren ausgeübt werden.

589 Artikel-29-Datenschutzgruppe (2016), *Leitlinien zum Recht auf Datenübertragbarkeit*, WP 242, 13. Dezember 2016 und überarbeitet am 5. April 2017, S. 13.

590 a.a.O.

Recht auf Widerspruch aufgrund der besonderen Situationen der betroffenen Personen

Die betroffenen Personen haben kein allgemeines Recht auf Widerspruch gegen die Verarbeitung ihrer Daten.⁵⁹¹ Artikel 21 Absatz 1 DSGVO ermächtigt die betroffene Person, aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch einzulegen, sofern die Rechtsgrundlage für die Verarbeitung in der seitens des Verantwortlichen erfolgenden Wahrnehmung einer Aufgabe beruht, die im öffentlichen Interesse liegt, oder die Verarbeitung auf den berechtigten Interessen des Verantwortlichen beruht.⁵⁹² Das Widerspruchsrecht findet auf Profiling-Tätigkeiten Anwendung. Ein ähnliches Recht wurde auch im Modernisierten Übereinkommen Nr. 108 anerkannt.⁵⁹³

Das Recht auf Widerspruch aufgrund der besonderen Situation der betroffenen Person zielt darauf ab, eine angemessene Abwägung zwischen den Datenschutzrechten der betroffenen Person und den legitimen Rechten anderer an der Verarbeitung ihrer Daten vorzunehmen. Der EuGH verdeutlichte jedoch, dass die Rechte der betroffenen Person „im Allgemeinen“ gegenüber den wirtschaftlichen Interessen eines Verantwortlichen überwiegen, dies jedoch von „der Art der betreffenden Information, von deren Sensibilität für das Privatleben der betroffenen Person und vom Interesse der Öffentlichkeit am Zugang zu der Information“ abhängt.⁵⁹⁴ Nach Maßgabe der DSGVO liegt die Beweislast bei den Verantwortlichen, die zwingende Gründe für die Fortsetzung der Verarbeitung vorbringen müssen.⁵⁹⁵ Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 verdeutlicht auf ähnliche Weise, dass die berechtigten Gründe für die Datenverarbeitung (die das Widerspruchsrecht der betroffenen Personen überwiegen können) in jedem Einzelfall nachzuweisen sind.⁵⁹⁶

591 Siehe auch EGMR, *M.S. / Schweden*, Nr. 20837/92, 27. August 1997 (wo medizinische Daten ohne Einwilligung und ohne Möglichkeit des Widerspruchs weitergegeben wurden); EGMR, *Leander / Schweden*, Nr. 9248/81, 26. März 1987; EGMR, *Mosley / Vereinigtes Königreich*, Nr. 48009/08, 10. Mai 2011.

592 DSGVO, Erwägungsgrund 69; Artikel 6 Absatz 1 Buchstabe e und f.

593 Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe d; Profiling-Empfehlung, Artikel 5 Absatz 3.

594 EuGH, C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014, Randnr. 81.

595 Siehe auch Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe d, der besagt, dass die betroffene Person der Verarbeitung der sie betreffenden personenbezogenen Daten widersprechen kann, „es sei denn, der Verantwortliche weist berechtigte Gründe für die Verarbeitung nach, die ihre Interessen oder Rechte und Grundfreiheiten überwiegen“.

596 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 78.

Beispiel: In der Rechtssache *Manni*⁵⁹⁷ befand der EuGH, dass Herr Manni aufgrund des rechtmäßigen Zwecks der Offenlegung personenbezogener Daten in einem Unternehmensregister, insbesondere des Schutzes der Interessen Dritter und der Gewährleistung von Rechtssicherheit, grundsätzlich kein Recht auf Löschung seiner personenbezogenen Daten aus dem Unternehmensregister hatte. Er erkannte das Bestehen eines Rechts auf Widerspruch gegen die Verarbeitung an, indem er feststellte, „dass [...] nicht auszuschließen ist, dass es besondere Situationen gibt, in denen es aus überwiegenden, schutzwürdigen, sich aus dem konkreten Fall der betroffenen Person ergebenden Gründen ausnahmsweise gerechtfertigt ist, den Zugang zu den im Register eingetragenen personenbezogenen Daten, die sie betreffen, nach Ablauf einer hinreichend langen Frist [...] auf Dritte zu beschränken, die ein besonderes Interesse an der Einsichtnahme in diese Daten nachweisen“.

Der EuGH hielt die nationalen Gerichte dafür verantwortlich, jeden Einzelfall unter Berücksichtigung aller maßgeblichen Umstände der Person und unter Berücksichtigung dessen zu beurteilen, ob eventuell überwiegende, schutzwürdige Gründe vorliegen, die es gegebenenfalls ausnahmsweise rechtfertigen könnten, den beschränkten Zugang Dritter zu den personenbezogenen Daten in Gesellschaftsregistern zu rechtfertigen. Er stellte jedoch klar, dass im Fall von Herrn Manni die bloße Tatsache, dass die Offenlegung seiner personenbezogenen Daten im Register seine Kundschaft angeblich beeinflusste, nicht als solch überwiegender und schutzwürdiger Grund betrachtet werden könne. Die potenziellen Kunden von Herrn Manni haben ein berechtigtes Interesse am Zugang zu den Informationen in Bezug auf die Insolvenz seines früheren Unternehmens.

Ein erfolgreicher Widerspruch hat zur Folge, dass der Verantwortliche die fraglichen Daten nicht länger verarbeiten darf. Die Verarbeitungen der Daten der betroffenen Person, die vor dem Widerspruch vorgenommen wurden, bleiben jedoch rechtmäßig.

⁵⁹⁷ EuGH, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni*, 9. März 2017, Randnrn. 47 und 60.

Recht auf Widerspruch gegen die Verarbeitung von Daten für Zwecke der Direktwerbung

Artikel 21 Absatz 2 DSGVO sieht ein eigenes Recht auf Widerspruch gegen die Verwendung personenbezogener Daten für Zwecke der Direktwerbung vor und ergänzt damit Artikel 13 der ePrivacy-Richtlinie. Ein solches Recht findet sich auch im Modernisierten Übereinkommen Nr. 108 sowie in der Empfehlung des Europarates zum Direktmarketing.⁵⁹⁸ Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 verdeutlicht, dass Widersprüche gegen die Datenverarbeitung für Zwecke der Direktwerbung zur bedingungslosen Löschung oder Entfernung der fraglichen personenbezogenen Daten führen müssen.⁵⁹⁹

Die betroffene Person hat das Recht, jederzeit unentgeltlich Widerspruch gegen die Verwendung der sie betreffenden personenbezogenen Daten für Zwecke der Direktwerbung einzulegen. Die betroffenen Personen müssen über dieses Recht in einer verständlichen und von anderen Informationen getrennten Form unterrichtet werden.

Widerspruchsrecht mittels automatisierter Verfahren

Werden personenbezogene Daten für Dienste der Informationsgesellschaft verwendet und verarbeitet, kann die betroffene Person ihr Recht auf Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten mittels automatisierter Verfahren ausüben.

Dienste der Informationsgesellschaft sind definiert als jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.⁶⁰⁰

Verantwortliche, die Dienste der Informationsgesellschaft anbieten, müssen über geeignete technische Einrichtungen und Verfahren verfügen, um die wirksame Ausübung des Widerspruchsrechts mittels automatisierter Verfahren sicherzustellen.⁶⁰¹ Dies kann z.B. das Blockieren von Cookies auf Webseiten oder das Deaktivieren des Internet-Browser-Trackings beinhalten.

598 Europarat, Ministerkomitee (1985), Empfehlung Rec(85)20 an die Mitgliedstaaten betreffend den Schutz personenbezogener Daten, die für Zwecke des Direktmarketing verwendet werden, 25. Oktober 1985, Artikel 4 Absatz 1.

599 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 79.

600 Richtlinie 98/34/EG in der durch die Richtlinie 98/48/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften geänderten Fassung, Artikel 1 Absatz 2.

601 DSGVO, Artikel 21 Absatz 5.

Recht auf Widerspruch gegen eine Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken

Im EU-Recht sollte die wissenschaftliche Forschung weit ausgelegt werden und beispielsweise die technologische Entwicklung und Beweisführung, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen.⁶⁰² Zur historischen Forschung zählt auch Forschung im Bereich der Ahnenforschung, wobei darauf hinzuweisen ist, dass die Verordnung nicht für verstorbene Personen gelten sollte.⁶⁰³ Unter dem Begriff „statistische Zwecke“ ist jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung personenbezogener Daten zu verstehen.⁶⁰⁴ Auch hier ist die besondere Situation einer betroffenen Person die Rechtsgrundlage für das Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten zu Forschungszwecken.⁶⁰⁵ Die einzige Ausnahme ist das Erfordernis der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe. Das Recht auf Löschung findet jedoch keine Anwendung, wenn die Verarbeitung (mit oder ohne Vorliegen von Gründen des öffentlichen Interesses) zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erforderlich ist.⁶⁰⁶

Artikel 89 DSGVO wägt die Erfordernisse der wissenschaftlichen, statistischen oder historischen Forschung und die Rechte der betroffenen Personen mit speziellen Garantien und Ausnahmen ab. Folglich können im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen vom Widerspruchsrecht vorgesehen werden, als dieses Recht voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich macht oder ernsthaft beeinträchtigt und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

Im **Recht des Europarates** regelt Artikel 11 Absatz 2 des Modernisierten Übereinkommens Nr. 108, dass Einschränkungen der Rechte der betroffenen Personen, einschließlich des Widerspruchsrechts, für die Datenverarbeitung zu im

602 a.a.O., Erwägungsgrund 159.

603 a.a.O., Erwägungsgrund 160.

604 a.a.O., Erwägungsgrund 162.

605 a.a.O., Artikel 21 Absatz 6.

606 a.a.O., Artikel 17 Absatz 3 Buchstabe d.

öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gesetzlich vorgesehen sein können, sofern kein erkennbares Risiko für die Verletzungen der Rechte und Grundfreiheiten der betroffenen Personen besteht.

Der erläuternde Bericht (Absatz 41) erkennt jedoch auch an, dass die betroffenen Personen Gelegenheit erhalten sollten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen und zu widersprechen, sofern sie die Verarbeitung ohne rechtmäßigen Grund als zu starken Eingriff in ihre Rechte und Freiheiten empfinden.

Anders ausgedrückt würde eine solche Verarbeitung folglich a priori als vereinbar betrachtet werden, vorausgesetzt, es bestehen andere Garantien und die Verarbeitungsvorgänge schließen grundsätzlich jede Verwendung der erhaltenen Informationen für Entscheidungen oder Maßnahmen in Bezug auf eine bestimmte Person aus.

6.1.7. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Automatisierte Entscheidungen sind Entscheidungen, die unter Verwendung personenbezogener Daten nur mit Hilfe von mechanischen Anwendungen, ohne jegliches menschliche Eingreifen, getroffen werden. **Im EU-Recht** dürfen die betroffenen Personen keinen automatisierten Entscheidungen unterworfen werden, die rechtliche Wirkung entfalten oder ähnlich erhebliche Auswirkungen haben. Sollten sich solche Entscheidungen erheblich auf das Leben der Personen auswirken, da sie sich beispielsweise auf die Kreditwürdigkeit, das E-Recruiting, die Arbeitsleistung oder die Analyse des Verhaltens oder der Zuverlässigkeit beziehen, ist zur Vermeidung negativer Folgen ein besonderer Schutz erforderlich. Zu automatisierten Entscheidungen gehört auch das Profiling, das in jeglicher Form der automatisierten Bewertung der „persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person“.⁶⁰⁷

⁶⁰⁷ a.a.O., Erwägungsgrund 71, Artikel 4 Absatz 4 und Artikel 22.

Beispiel: Zur raschen Bewertung der Kreditwürdigkeit eines künftigen Kunden erheben Kreditauskunfteien Daten beispielsweise darüber, wie der Kunde seine Guthaben- und Dienstkonten führt, über die Einzelheiten der früheren Anschriften des Kunden sowie über Informationen aus öffentlichen Quellen wie Wählerverzeichnissen, öffentlichen Aufzeichnungen (einschließlich Gerichtsurteilen) oder Konkurs- und Insolvenzdaten. Diese personenbezogenen Daten werden im Anschluss daran in einen Scoring-Algorithmus eingegeben, der einen Gesamtwert für die Kreditwürdigkeit des potenziellen Kunden berechnet.

Nach Ansicht der Artikel-29-Datenschutzgruppe entspricht das Recht, keinen Entscheidungen unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und die rechtliche Wirkung für die betroffene Person entfalten oder sie erheblich beeinträchtigen können, einem allgemeinen Verbot und erfordert nicht, dass die betroffene Person proaktiv einen Widerspruch gegen eine solche Entscheidung anstrebt.⁶⁰⁸

Nach Maßgabe der DSGVO können automatisierte Entscheidungen, die rechtliche Wirkung entfalten oder die betroffenen Personen erheblich beeinträchtigen, gleichwohl zulässig sein, sofern sie für den Abschluss oder die Erfüllung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person erforderlich sind oder die betroffene Person ihre ausdrückliche Einwilligung gegeben hat. Automatisierte Entscheidungen sind ebenfalls zulässig, wenn sie aufgrund von Rechtsvorschriften zulässig sind und sie angemessene Maßnahmen zur Wahrung der Rechte, Freiheiten und berechtigten Interessen der betroffenen Person enthalten.⁶⁰⁹

Die DSGVO sieht auch vor, dass es zu den Pflichten des Verantwortlichen in Bezug auf die Informationspflicht bei der Erhebung personenbezogener Daten zählt, dass die betroffenen Personen vom Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling, zu unterrichten sind.⁶¹⁰ Das Auskunftsrecht über die seitens des Verantwortlichen verarbeiteten

608 Artikel-29-Datenschutzgruppe, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3. Oktober 2017, S. 15.

609 DSGVO, Artikel 22 Absatz 2.

610 a.a.O., Artikel 12.

personenbezogenen Daten bleibt unberührt.⁶¹¹ Die Unterrichtung sollte sich dabei nicht nur auf die Tatsache beschränken, dass Profiling erfolgen wird, sondern auch aussagekräftige Informationen über die beim Profiling angewandte Logik und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffenen Personen beinhalten.⁶¹² Eine Krankenversicherung, die automatisierte Entscheidungen in Bezug auf Anträge einsetzt, sollte den betroffenen Personen beispielsweise allgemeine Informationen über die Funktionsweise des Algorithmus bereitstellen und über die Faktoren, die der Algorithmus zur Berechnung ihrer Versicherungsbeiträge verwendet. Ebenso können die betroffenen Personen bei der Ausübung ihres „Auskunftsrechts“ vom Verantwortlichen Informationen über das Bestehen einer automatisierten Entscheidungsfindung und aussagekräftige Informationen über die angewandte Logik verlangen.⁶¹³

Die den betroffenen Personen bereitgestellten Informationen sollen Transparenz verschaffen und den betroffenen Personen ermöglichen, gegebenenfalls ihre in informierter Weise erfolgende Einwilligung zu geben oder das Eingreifen einer Person zu erwirken. Der Verantwortliche ist dazu verpflichtet, angemessene Maßnahmen zu treffen, um die Rechte, Freiheiten und berechtigten Interessen der betroffenen Person zu wahren. Dazu gehört mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung einer auf automatisierter Verarbeitung ihrer personenbezogenen Daten beruhenden Entscheidung.⁶¹⁴

Die Artikel-29-Datenschutzgruppe hat eine weitere Anleitung für die Anwendung automatisierter Entscheidungen im Rahmen der DSGVO bereitgestellt.⁶¹⁵

Im Recht des Europarates haben Personen das Recht, keiner Entscheidung unterworfen zu werden, die erhebliche Auswirkungen auf sie hat und ausschließlich auf einer automatisierten Verarbeitung ohne Berücksichtigung

611 a.a.O., Artikel 15.

612 a.a.O., Artikel 13 Absatz 2 Buchstabe f.

613 a.a.O., Artikel 15 Absatz 1 Buchstabe h.

614 a.a.O., Artikel 22 Absatz 3.

615 Artikel 29-Datenschutzgruppe (2017), *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3. Oktober 2017.

ihrer Standpunkte beruht.⁶¹⁶ Das Erfordernis zur Berücksichtigung der Standpunkte der betroffenen Personen bei Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen, bedeutet, dass diese ein Recht auf Anfechtung solcher Entscheidungen haben und dazu in der Lage sein sollten, jede Unrichtigkeit der vom Verantwortlichen verwendeten personenbezogenen Daten anzufechten und zu hinterfragen, ob die auf sie angewandten Profile zutreffend sind.⁶¹⁷ Eine Person kann dieses Recht jedoch nicht ausüben, wenn die automatisierte Entscheidung aufgrund von Rechtsvorschriften, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte, Freiheiten und berechtigten Interessen der betroffenen Person enthalten. Darüber hinaus haben die betroffenen Personen das Recht, auf Antrag über die der durchgeführten Datenverarbeitung zugrundeliegenden Wertungen informiert zu werden.⁶¹⁸ Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 enthält das Beispiel des „Credit Scoring“. Die Personen sollten nicht nur das Recht auf Informationen über die positive oder negative „Scoring“-Entscheidung selbst haben, sondern auch über die der Verarbeitung ihrer personenbezogenen Daten zugrundeliegende *Logik*, die zu einer solchen Entscheidung geführt hat. „Die Kenntnis dieser Faktoren trägt zur wirksamen Ausübung weiterer wesentlicher Garantien wie dem Widerspruchsrecht und dem Beschwerderecht bei einer zuständigen Behörde bei“.⁶¹⁹

Die wenngleich nicht rechtsverbindliche Profiling-Empfehlung präzisiert die Voraussetzungen für die Erhebung und Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling.⁶²⁰ Sie enthält Bestimmungen in Bezug auf das Erfordernis, dass die im Rahmen des Profiling vorgenommene Verarbeitung fair, rechtmäßig, verhältnismäßig und für festgelegte und legitime Zwecke bestimmt sein sollte. Sie enthält auch Bestimmungen zu den Informationen, die die Verantwortlichen den betroffenen Personen bereitstellen sollten. Die Empfehlung beinhaltet auch den Grundsatz der Datenqualität, der die Verantwortlichen dazu verpflichtet, angemessene Maßnahmen zu ergreifen, um Faktoren, die zu Datenungenauigkeit führen, zu berichtigen,

616 Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe a.

617 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 75.

618 Modernisiertes Übereinkommen Nr. 108, Artikel 9 Absatz 1 Buchstabe c.

619 Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 77.

620 Europarat, *Empfehlung CM/Rec(2010)13* des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling, Artikel 3.

um Fehllrisiken, die das Profiling zur Folge haben könnte, zu begrenzen und um die Qualität der verwendeten Daten und Algorithmen in regelmäßigen Abständen zu bewerten.

6.2. Rechtsbehelfe, Haftung, Sanktionen und Schadensersatz

Kernpunkte

- Gemäß dem Modernisierten Übereinkommen Nr. 108 sind im einzelstaatlichen Recht der Vertragsparteien angemessene Rechtsbehelfe und Sanktionen bei Verletzungen des Rechts auf Datenschutz festzulegen.
- In der EU sieht die DSGVO für die betroffenen Personen Rechtsbehelfe im Falle der Verletzung ihrer Rechte vor, sowie Sanktionen gegen die Verantwortlichen und Auftragsverarbeiter, die die Bestimmungen der Verordnung nicht einhalten. Darüber hinaus sieht sie auch ein Recht auf Schadensersatz und die Haftung vor.
- Die betroffenen Personen haben das Recht auf Beschwerde bei einer Aufsichtsbehörde aufgrund des mutmaßlichen Verstoßes gegen die Verordnung, sowie das Recht auf wirksamen gerichtlichen Rechtsbehelf und auf den Erhalt von Schadensersatz.
- Bei der Ausübung ihres Rechts auf wirksamen Rechtsbehelf können sich die Personen von im Bereich des Datenschutzes tätigen Organisationen ohne Gewinnerzielungsabsicht vertreten lassen.
- Der Verantwortliche oder der Auftragsverarbeiter haftet für jeden durch den Verstoß entstandenen materiellen oder immateriellen Schaden.
- Die Aufsichtsbehörden sind bei Verstößen gegen die Verordnung zur Verhängung von Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes befugt, je nachdem, welcher der Beträge höher ist.
- Betroffene Personen können Verletzungen des Datenschutzrechts als letztes Mittel und unter bestimmten Voraussetzungen vor den EGMR bringen.
- Jede natürliche oder juristische Person hat das Recht, unter den in den Verträgen genannten Voraussetzungen beim EuGH Beschwerde gegen jeglichen Beschluss des Datenschutzausschusses einzulegen.

Die Annahme von Rechtsinstrumenten reicht nicht aus, um den Schutz personenbezogener Daten innerhalb Europas zu gewährleisten. Um den europäischen Datenschutzvorschriften Geltung zu verschaffen, ist es erforderlich, Mechanismen einzurichten, die den Personen ermöglichen, Verletzungen ihrer Rechte entgegenzuwirken und Schadensersatz für jeden erlittenen Schaden zu verlangen. Auch wichtig ist es, dass Aufsichtsbehörden die Befugnis zur Verhängung von wirksamen, abschreckenden und zum fraglichen Verstoß verhältnismäßigen Sanktionen haben.

Die im Datenschutzrecht verankerten Rechte können von der Person ausgeübt werden, deren Rechte in Gefahr sind; dabei handelt es sich um jemanden, der eine von der Datenverarbeitung betroffene Person ist. Andere Personen, die die im nationalen Recht erforderlichen Anforderungen erfüllen, können die betroffenen Personen jedoch ebenfalls bei der Ausübung ihrer Rechte vertreten.

In zahlreichen Jurisdiktionen müssen Kinder und Menschen mit geistiger Behinderung durch ihre Erziehungsberechtigten/Vormund vertreten werden.⁶²¹ Nach dem EU-Datenschutzrecht ist eine Vereinigung, deren rechtmäßiger Zweck es ist, den Schutz personenbezogener Daten zu fördern, berechtigt, die betroffenen Personen vor einer Aufsichtsbehörde oder einem Gericht zu vertreten.⁶²²

6.2.1. Recht eine Beschwerde bei einer Aufsichtsbehörde einzureichen

Sowohl **im Recht des Europarates** als auch **im EU-Recht** haben Personen das Recht, bei der zuständigen Aufsichtsbehörde Anträge und Beschwerden einzureichen, sofern sie der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht in Übereinstimmung mit dem Gesetz erfolgt.

Das Modernisierte Übereinkommen Nr. 108 erkennt das Recht der betroffenen Personen an, bei der Ausübung der ihnen im Rahmen des Übereinkommens zustehenden Rechte ungeachtet ihrer Staatsangehörigkeit oder ihres

621 FRA (2015), [Handbuch zu den europarechtlichen Grundlagen im Bereich der Rechte des Kindes](#), Luxemburg, Amt für Veröffentlichungen; FRA (2013), [Die Rechts- und Handlungsfähigkeit von Menschen mit geistiger Behinderung und Menschen mit psychischen Gesundheitsproblemen](#), Luxemburg, Amt für Veröffentlichungen der Europäischen Union.

622 DSGVO, Artikel 80.

Aufenthaltsorts die Unterstützung einer Aufsichtsbehörde in Anspruch zu nehmen.⁶²³ Ein Antrag auf Unterstützung kann nur in Ausnahmefällen abgewiesen werden und die betroffenen Personen sollten die mit der Unterstützung verbundenen Kosten und Gebühren nicht tragen müssen.⁶²⁴

Auch das EU-Recht enthält ähnliche Bestimmungen. Die DSGVO verpflichtet die Aufsichtsbehörden, das Einreichen von Beschwerden durch Maßnahmen zu erleichtern, wie etwa die Bereitstellung eines elektronischen Beschwerdeformulars.⁶²⁵ Die betroffene Person kann die Beschwerde bei der Aufsichtsbehörde im Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes einreichen.⁶²⁶ Beschwerden sind zu untersuchen und die Aufsichtsbehörde unterrichtet die betroffene Person über den Stand und die Ergebnisse der Beschwerde.⁶²⁷

Potenzielle Verstöße seitens der Organe oder Einrichtungen der EU können dem Europäischen Datenschutzbeauftragten zur Kenntnis gebracht werden.⁶²⁸ Ergeht innerhalb von sechs Monaten keine Antwort des EDSB, so gilt die Beschwerde als abgelehnt. Im Rahmen der Verordnung (EG) Nr. 45/2001, die den Organen und Einrichtungen der EU die Verpflichtung zur Einhaltung der Datenschutzvorschriften auferlegt, können Berufungen gegen die Entscheidungen des EDSB vor den EuGH gebracht werden.

Gegen Entscheidungen einer nationalen Aufsichtsbehörde muss gerichtlich vorgegangen werden können. Dies gilt sowohl für die betroffenen Personen als auch für Verantwortliche und Auftragsverarbeiter, die an einem Verfahren vor einer Aufsichtsbehörde beteiligt waren.

623 Modernisiertes Übereinkommen Nr. 108, Artikel 18.

624 *a.a.O.*, Artikel 20 und 21.

625 DSGVO, Artikel 57 Absatz 2.

626 *a.a.O.*, Artikel 77 Absatz 1.

627 *a.a.O.*, Artikel 77 Absatz 2.

628 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001.

Beispiel: Im September 2017 belegte die spanische Datenschutzbehörde Facebook aufgrund der Verletzung mehrerer Datenschutzverordnungen mit einer Geldstrafe. Die Aufsichtsbehörde ahndete das soziale Netzwerk aufgrund der Erhebung, Speicherung und Verarbeitung personenbezogener Daten, darunter auch besonderer Kategorien von personenbezogenen Daten, zu Werbezwecken und ohne Einholung der Einwilligung der betroffenen Person. Das Urteil gründete auf einer Untersuchung, die auf Eigeninitiative der Aufsichtsbehörde durchgeführt wurde.

6.2.2. Recht auf wirksamen gerichtlichen Rechtsbehelf

Zusätzlich zu dem Recht auf Beschwerde bei einer Aufsichtsbehörde müssen die Personen das Recht haben, einen wirksamen gerichtlichen Rechtsbehelf einzulegen und ein Gericht mit ihrem Fall zu befassen. Das Recht auf einen Rechtsbehelf ist in der europäischen Rechtstradition fest verankert und sowohl in Artikel 47 der Charta der Grundrechte der EU als auch in Artikel 13 EMRK als Grundrecht anerkannt.⁶²⁹

Im EU-Recht geht die Bedeutung der Bereitstellung wirksamer Rechtsbehelfe für die betroffenen Personen im Falle einer Verletzung ihrer Rechte sowohl aus den Bestimmungen der DSGVO, die ein Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Aufsichtsbehörden, Verantwortliche und Auftragsverarbeiter begründet, als auch aus der Rechtsprechung des EuGH eindeutig hervor.

Beispiel: In der Rechtssache *Schrems*⁶³⁰ erklärte der EuGH die Safe-Harbor-Angemessenheitsentscheidung für ungültig. Diese Entscheidung erlaubte die internationale Datenübermittlung von der EU an Organisationen in den Vereinigten Staaten, die über eine Selbstzertifizierung unter dem Safe-Harbor-System verfügten. Nach Ansicht des EuGH wies das Safe-Harbor-System mehrere Mängel auf, die die Grundrechte der EU-Bürger auf den Schutz der Privatsphäre, den Schutz personenbezogener Daten und das Recht auf wirksamen gerichtlichen Rechtsbehelf gefährdeten.

629 Siehe zum Beispiel EGMR, *Karabeyoğlu / Türkei*, Nr. 30083/10, 7. Juni 2016; EGMR, *Mustafa Sezgin Tanrikulu / Türkei*, Nr. 27473/06, 18. Juli 2017.

630 EuGH, Rechtssache C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015.

In Bezug auf die Verletzung der Rechte auf Privatsphäre und Datenschutz hob der EuGH hervor, dass die Gesetzgebung der Vereinigten Staaten bestimmten Behörden den Zugang zu den seitens der Mitgliedstaaten an die Vereinigten Staaten übermittelten personenbezogenen Daten und zu deren Verarbeitung in einer Weise erlaube, die mit den ursprünglichen Übermittlungszwecken unvereinbar sei und über das Maß hinausgehe, das für den Schutz der nationalen Sicherheit unbedingt nötig und angemessen sei. In Bezug auf das Recht auf wirksamen Rechtsbehelf stellte der Gerichtshof fest, dass es für die betroffenen Personen keine administrativen oder gerichtlichen Rechtsbehelfe gab, die es ihnen erlaubten, Zugang zu den sie betreffenden Daten zu erhalten und gegebenenfalls deren Berichtigung oder Löschung zu erwirken. Der EuGH schlussfolgerte, dass eine Regelung, die keine Möglichkeit vorsieht, mittels eines Rechtsbehelfs Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, „den Wesensgehalt des in Artikel 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz [verletzt]“. Er hob hervor, dass das Vorhandensein eines gerichtlichen Rechtsbehelfs zur Gewährleistung der Einhaltung der Rechtsvorschriften dem Wesen eines Rechtsstaats inhärent ist.

Einzelpersonen, Verantwortliche oder Auftragsverarbeiter, die einen rechtlich bindenden Beschluss einer Aufsichtsbehörde anfechten möchten, können das Verfahren vor ein Gericht bringen.⁶³¹ Der Begriff „Beschluss“ sollte dabei weit ausgelegt werden und die Untersuchungs-, Sanktions- und Genehmigungsbefugnisse der Aufsichtsbehörden umfassen, sowie Beschlüsse in Bezug auf die Ablehnung oder Abweisung von Beschwerden. Rechtlich nicht bindende Maßnahmen, wie von der Aufsichtsbehörde abgegebene Stellungnahmen oder Empfehlungen, können jedoch nicht Gegenstand einer Klage vor Gericht sein.⁶³² Für die gerichtliche Klage sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.⁶³³

In Fällen, in denen ein Verantwortlicher oder ein Auftragsverarbeiter die Rechte einer betroffenen Person verletzt, haben die betroffenen Personen das Recht auf einen wirksamen gerichtlichen Rechtsbehelf.⁶³⁴ Bei gegen einen Verantwortlichen oder Auftragsverarbeiter eingeleiteten Verfahren

631 DSGVO, Artikel 78.

632 a.a.O., Erwägungsgrund 143.

633 a.a.O., Artikel 78 Absatz 3.

634 a.a.O., Artikel 79.

ist es besonders wichtig, dass die Personen die Wahlmöglichkeit haben, vor welches Gericht sie die Klage bringen. Die Beschwerde können sie wahlweise bei einem Gericht des Mitgliedstaats einreichen, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat, oder bei den Gerichten des Mitgliedstaats, in dem die betroffenen Personen ihren Aufenthaltsort haben.⁶³⁵ Die zweite Möglichkeit erleichtert den Personen die Ausübung ihrer Rechte in erheblichem Maße, da Sie die Klage in dem Mitgliedstaat erheben können, in dem sie ansässig sind und dessen Rechtsordnung ihnen vertraut ist. Die Beschränkung des Gerichtsstands für Verfahren gegen Verantwortliche und Auftragsverarbeiter auf den Mitgliedstaat, in dem Letztere eine Niederlassung haben, könnte betroffene Personen, die in einem anderen Mitgliedstaat ansässig sind, von der Erhebung einer gerichtlichen Klage abschrecken, da es Reisekosten und zusätzliche Kosten zur Folge hätte und das Verfahren in einer fremden Sprache und in einer fremden Rechtsordnung stattfinden könnte. Die einzige Ausnahme betrifft Fälle, in denen es sich beim Verantwortlichen oder Auftragsverarbeiter um eine Behörde handelt und die Verarbeitung in Ausübung ihrer hoheitlichen Befugnisse erfolgt. In diesem Fall sind ausschließlich die Gerichte im Staat der entsprechenden Behörde für eine Klage zuständig.⁶³⁶

Während Rechtssachen in Bezug auf Datenschutzvorschriften in den meisten Fällen in den Gerichten der Mitgliedstaaten entschieden werden, können einige Rechtssachen auch vor den EuGH gebracht werden. Die erste Möglichkeit betrifft den Fall, in dem eine betroffene Person, ein Verantwortlicher, ein Auftragsverarbeiter oder eine Aufsichtsbehörde eine Klage auf Nichtigerklärung eines Beschlusses des EDSA erheben möchte. Eine solche Klage unterliegt jedoch Artikel 263 AEUV, was bedeutet, dass diese Personen oder Stellen für die Zulässigkeit der Klage nachweisen müssen, dass der Beschluss des Ausschusses sie unmittelbar und individuell betrifft.

Das zweite Szenario betrifft Fälle der unrechtmäßigen Verarbeitung personenbezogener Daten seitens Organen und Einrichtungen der EU. In Fällen, in denen EU-Organen das Datenschutzrecht verletzen, können die betroffenen Personen unmittelbar Klage beim Gericht der EU erheben (das Teil des EuGH ist). Das Gericht ist in erster Instanz für Beschwerden in Bezug auf Verletzungen des EU-Rechts seitens EU-Organen zuständig. Folglich können Beschwerden gegen

635 a.a.O., Artikel 79 Absatz 2.

636 a.a.O.

den EDSB, bei dem es sich um ein EU-Organ handelt, ebenfalls vor das Gericht gebracht werden.⁶³⁷

Beispiel: In der Rechtssache *Bavarian Lager*⁶³⁸ verlangte das Unternehmen von der Europäischen Kommission Einsicht in das vollständige Protokoll einer von der Kommission einberufenen Sitzung, in der es angeblich um für das Unternehmen relevante rechtliche Fragen gegangen sei. Die Kommission lehnte das Ersuchen des Unternehmens auf Einsichtnahme ab und führte hierbei übergeordnete Datenschutzinteressen an.⁶³⁹ Gegen diese Entscheidung hatte Bavarian Lager gemäß Artikel 32 der Datenschutzverordnung für die EU-Organe vor dem Gericht erster Instanz (dem Vorläufer des Gerichts) geklagt. In seiner Entscheidung (Rechtssache T-194/04 *The Bavarian Lager Co. Ltd gegen Kommission der Europäischen Gemeinschaften*) hob das Gericht erster Instanz die Entscheidung der Kommission auf, das Ersuchen auf Einsichtnahme zurückzuweisen. Die Europäische Kommission legte gegen diese Entscheidung Rechtsbehelf beim EuGH ein.

Der EuGH (Große Kammer) hob in seinem Urteil das Urteil des Gerichts erster Instanz auf und bestätigte die Zurückweisung des Ersuchens auf Einsichtnahme in das vollständige Protokoll der Sitzung durch die Europäische Kommission zum Schutz der personenbezogenen Daten der Sitzungsteilnehmer. Der EuGH war der Ansicht, dass die Kommission zu Recht die Offenlegung dieser Informationen verweigert hatte, da die Teilnehmer kein Einverständnis zur Offenlegung ihrer personenbezogenen Daten gegeben hatten. Darüber hinaus hatte Bavarian Lager die Notwendigkeit der Einsichtnahme in diese Informationen nicht nachgewiesen.

Im Zuge von innerstaatlichen Verfahren können betroffene Personen, Aufsichtsbehörden, Verantwortliche oder Auftragsverarbeiter schließlich das einzelstaatliche Gericht auffordern, beim EuGH eine Klarstellung der Auslegung und Gültigkeit von Handlungen der Organe, Einrichtungen, Ämter und Agenturen der EU zu beantragen Solche Klarstellungen werden als

637 Verordnung (EG) Nr. 45/2001, Artikel 32 Absatz 3.

638 EuGH, C-28/08 P, *Europäische Kommission / The Bavarian Lager Co. Ltd* [GK], 2010.

639 Für eine Analyse des Arguments siehe: EDSB (2011), *Zugang der Öffentlichkeit zu Dokumenten mit personenbezogenen Daten nach dem Urteil in der Rechtssache Bavarian Lager*, Brüssel, EDSB.

Vorabentscheidungen bezeichnet. Dies ist kein unmittelbarer Rechtsbehelf für den Kläger, doch können einzelstaatliche Gerichte auf diesem Wege sicherstellen, dass sie die korrekte Auslegung des EU-Rechts anwenden. Über diesen Mechanismus der Vorabentscheidungen konnten wegweisende Rechtssachen wie die Rechtssachen *Digital Rights Ireland* und *Kärntner Landesregierung und andere*⁶⁴⁰ und *Schrems*⁶⁴¹, die die Entwicklung des EU-Datenschutzrechts stark beeinflussten, vor den EuGH gelangen.

Beispiel: Bei der Rechtssache *Digital Rights Ireland* und *Kärntner Landesregierung und andere*⁶⁴² handelte es sich um eine verbundene Rechtssache, die vom irischen High Court und vom österreichischen Verfassungsgerichtshof vorgelegt wurde und die Übereinstimmung der Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten) mit dem EU-Datenschutzrecht betraf. Der österreichische Verfassungsgerichtshof legte dem EuGH Fragen bezüglich der Gültigkeit von Artikel 3 bis 9 der Richtlinie 2006/24/EG im Lichte von Artikel 7, 9 und 11 der Charta der Grundrechte vor. Dazu zählte, ob bestimmte Bestimmungen des österreichischen Bundestelekommunikationsgesetzes zur Umsetzung der Richtlinie über die Vorratsspeicherung von Daten mit Aspekten der früheren Datenschutzrichtlinie und der Datenschutzverordnung für die EU-Organe vereinbar sind oder nicht.

In der Rechtssache *Kärntner Landesregierung und andere* führte Herr Seitlinger, einer der Kläger im Verfahren vor dem Verfassungsgerichtshof, an, er verwende Telefon, Internet und E-Mail sowohl für seine Arbeit als auch privat. Folglich gingen die Informationen, die er versende und empfangt, über öffentliche Telekommunikationsnetzwerke. Gemäß dem österreichischen Telekommunikationsgesetz aus dem Jahr 2003 sei sein Telekommunikationsanbieter gesetzlich verpflichtet, Daten über seine Nutzung des Netzes zu erheben und zu speichern. Herr Seitlinger meinte, diese Erhebung und Speicherung seiner personenbezogenen Daten sei für die technischen Zwecke des Versands und des Empfangs

640 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere* und *Kärntner Landesregierung und andere* [GK], 8. April 2014.

641 Rechtssache C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015.

642 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere* und *Kärntner Landesregierung und andere* [GK], 8. April 2014.

von Informationen über das Netzwerk nicht erforderlich. Tatsächlich sei die Erhebung und Speicherung dieser Daten auch nicht für Gebührenabrechnungszwecke erforderlich. Herr Seitlinger habe in diese Verarbeitung seiner personenbezogenen Daten nicht eingewilligt, deren Erhebung und Speicherung einzig und allein wegen des österreichischen Telekommunikationsgesetzes aus dem Jahr 2003 erfolgte.

Herr Seitlinger reichte deshalb Beschwerde vor dem österreichischen Verfassungsgerichtshof ein, in der er behauptete, die gesetzlichen Verpflichtungen seines Telekommunikationsanbieters würden seine Grundrechte unter Artikel 8 der Charta der Grundrechte der EU verletzen. Da die österreichischen Rechtsvorschriften EU-Recht umsetzten (die damalige Richtlinie über die Vorratsspeicherung von Daten), verwies der österreichische Verfassungsgerichtshof die Angelegenheit an den EuGH, der über die Vereinbarkeit der Richtlinie mit den in der Charta der Grundrechte der EU verankerten Rechten auf Privatsphäre und Datenschutz entscheiden sollte.

Die Große Kammer des EuGH fällte das Urteil in der Rechtssache, das zur Nichtigerklärung der EU-Richtlinie über die Vorratsspeicherung von Daten führte. Der EuGH befand, dass die Richtlinie einen besonders schwerwiegenden Eingriff in die Grundrechte auf Privatsphäre und Datenschutz beinhalte, der nicht auf das absolut Notwendige beschränkt sei. Die Richtlinie verfolge zwar ein rechtmäßiges Ziel, da sie den nationalen Behörden zusätzliche Möglichkeiten zur Ermittlung und Verfolgung schwerer Straftaten biete und daher ein nützliches Mittel für strafrechtliche Ermittlungen darstelle. Gleichwohl stellte der EuGH fest, dass die Beschränkungen der Grundrechte auf das absolut Notwendige zu beschränken seien und von klaren und präzisen Regeln zu ihrer Tragweite sowie von Garantien für die betroffenen Personen begleitet sein sollten.

Nach Ansicht des EuGH erfülle die Richtlinie diese Notwendigkeitsprüfung nicht. Zunächst sehe sie keine klaren und präzisen Regeln zur Begrenzung der Tragweite des Eingriffs vor. Anstatt einen Zusammenhang zwischen den auf Vorrat gespeicherten Daten und schweren Straftaten zu verlangen, fand die Richtlinie auf sämtliche Metadaten aller Benutzer aller elektronischen Kommunikationsmittel Anwendung. Infolgedessen stelle sie einen Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung dar, der als unverhältnismäßig zu betrachten sein könne. Sie enthalte weder

Voraussetzungen um die zugangsberechtigten Personen einzugrenzen, noch unterliege dieser Zugang verfahrensrechtlichen Voraussetzungen wie dem Erhalt einer vorherigen Genehmigung seitens einer Verwaltungsbehörde oder eines Gerichts. Schließlich lege die Richtlinie keine klaren Garantien für den Schutz der auf Vorrat gespeicherten Daten dar. Daher könne sie keinen wirksamen Schutz der Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung der Daten gewährleisten.⁶⁴³

Grundsätzlich muss der Gerichtshof die ihm vorgelegten Fragen beantworten und darf eine Vorabentscheidung nicht mit dem Argument ablehnen, diese Antwort wäre für das Hauptverfahren weder erheblich noch käme sie rechtzeitig. Er kann eine Frage jedoch zurückweisen, wenn sie nicht in seinen Zuständigkeitsbereich fällt.⁶⁴⁴ Der EuGH erlässt eine Entscheidung nur zu den Bestandteilen des an ihn gerichteten Vorabentscheidungsersuchens, während das einzelstaatliche Gericht seine Zuständigkeit für die Entscheidung im Hauptverfahren behält.⁶⁴⁵

Im **Recht des Europarates** müssen die Vertragsparteien angemessene gerichtliche und außergerichtliche Rechtsbehelfe für Verletzungen der Bestimmungen des Modernisierten Übereinkommens Nr. 108 einrichten.⁶⁴⁶ Gegen eine Vertragspartei der EMRK vorgebrachte Anschuldigungen in Bezug auf Verletzungen von Datenschutzrechten gemäß Artikel 8 EMRK, können nach Erschöpfung aller im innerstaatlichen Recht verfügbaren Rechtsbehelfe vor den EGMR gebracht werden. Wird vor dem EGMR eine Verletzung von Artikel 8 EMRK vorgebracht, müssen weitere Zulässigkeitsvoraussetzungen erfüllt sein (Artikel 34 und 35 EMRK).⁶⁴⁷

643 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere v. Kärntner Landesregierung und andere* [GK], 8. April 2014, Randnr. 66.

644 EuGH, C-244/80, *Pasquale Foglia / Mariella Novello* (Nr. 2), 16. Dezember 1981; EuGH, C-467/04, *Strafverfahren gegen Giuseppe Francesco Gasparini und andere*, 28. September 2006.

645 EuGH, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union / Viking Line ABP, OÜ Viking Line Eesti* [GK], 11. Dezember 2007, Randnr. 85.

646 Modernisiertes Übereinkommen Nr. 108, Artikel 12.

647 EMRK, *Artikel 34–37*.

Obwohl Anträge an den EGMR nur gegen Vertragsparteien gerichtet sein können, können sie auch indirekt Handlungen oder Unterlassungen Privater zum Gegenstand haben, sofern eine Vertragspartei ihren positiven Verpflichtungen nach der EMRK nicht nachgekommen ist und ihr innerstaatliches Recht nicht genügend Schutz vor Verletzungen von Datenschutzrechten bietet.

Beispiel: In der Rechtssache *K.U. gegen Finnland*⁶⁴⁸ führte der Beschwerdeführer, ein Minderjähriger, Beschwerde, dass auf einer Dating-Website im Internet über ihn eine Werbeanzeige sexueller Natur gepostet worden war. Aufgrund der im finnischen Recht vorgesehenen Geheimhaltungspflicht enthüllte der Diensteanbieter nicht die Identität der Person, die die Information gepostet hatte. Der Beschwerdeführer behauptete, das finnische Recht biete nicht genügend Schutz vor solchen Handlungen einer Privatperson, die belastende Daten über den Beschwerdeführer ins Internet gestellt habe. Der EGMR befand, Staaten seien nicht nur zwingend dazu verpflichtet, sich willkürlicher Eingriffe in das Privatleben von Personen zu enthalten, sondern hätten auch positive Verpflichtungen, zu denen „das Ergreifen von Maßnahmen“ gehöre, „mit denen sich die Achtung des Privatlebens auch im Verhältnis der Personen untereinander gewährleisten lasse“. Im Fall des Beschwerdeführers erforderte es sein praktischer und wirksamer Schutz, dass wirksame Maßnahmen zur Identifizierung und strafrechtlichen Verfolgung des Täters ergriffen wurden. Ein solcher Schutz sei vom Staat aber nicht bereitgestellt worden, und der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Beispiel: In der Rechtssache *Köpke gegen Deutschland*⁶⁴⁹ war die Beschwerdeführerin des Diebstahls an ihrem Arbeitsplatz verdächtigt und einer verdeckten Videoüberwachung unterzogen worden. Der EGMR befand, dass „nichts darauf hindeutet, dass die innerstaatlichen Behörden innerhalb ihres Ermessensspielraums keine Interessenabwägung zwischen dem Recht der Beschwerdeführerin auf Achtung ihres Privatlebens unter Artikel 8 und sowohl dem Interesse des Arbeitgebers an der Achtung seiner Eigentumsrechte und dem öffentlichen Interesse an einer geordneten Rechtspflege vorgenommen hätten“. Die Beschwerde wurde daher für unzulässig erklärt.

648 EGMR, *K.U. / Finnland*, Nr. 2872/02, 2. Dezember 2008.

649 EGMR, *Köpke / Deutschland* (Entscheidung), Nr. 420/07, 5. Oktober 2010.

Stellt der EGMR fest, dass eine Vertragspartei eines der durch die EMRK geschützten Rechte verletzt hat, ist die Vertragspartei zur Vollstreckung des EGMR-Urteils verpflichtet (Artikel 46 EMRK). Vollstreckungsmaßnahmen müssen zunächst die Verletzung beenden und dann, soweit möglich, ihre negativen Folgen für den Beschwerdeführer abstellen. Die Vollstreckung von Urteilen kann auch allgemeine Maßnahmen zur Verhütung von Verletzungen erfordern, die den vom Gerichtshof festgestellten ähnlich sind; dies kann durch Änderungen der Rechtsvorschriften, Rechtsprechung oder andere Maßnahmen geschehen.

Stellt der EGMR eine Verletzung der EMRK fest, sieht Artikel 41 EMRK vor, dass er der verletzten Partei auf Kosten des Vertragsstaats eine „gerechte Entschädigung“ zusprechen kann.

Recht zur Beauftragung einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht

Die DSGVO ermöglicht Personen, die eine Beschwerde bei einer Aufsichtsbehörde einlegen oder eine Klage vor Gericht erheben, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht mit ihrer Vertretung zu beauftragen.⁶⁵⁰ Die satzungsmäßigen Ziele dieser Organisationen ohne Gewinnerzielungsabsicht müssen im öffentlichen Interesse liegen und die Organisationen müssen im Bereich des Datenschutzes tätig sein. Sie können im Namen der betroffenen Person(en) Beschwerden einlegen oder das Recht auf einen gerichtlichen Rechtsbehelf ausüben. Die Verordnung räumt den Mitgliedstaaten die Möglichkeit ein, in Übereinstimmung mit dem nationalen Recht zu entscheiden, ob eine Einrichtung auch ohne Auftrag der betroffenen Person Beschwerden einlegen kann.

Dieses Vertretungsrecht ermöglicht den Personen, vom Sachverstand und von den organisatorischen und finanziellen Möglichkeiten solcher Organisationen ohne Gewinnerzielungsabsicht zu profitieren, die ihnen die Ausübung ihrer Rechte dadurch erheblich erleichtern. Die DSGVO erlaubt diesen Organisationen die Erhebung von Sammelklagen im Namen mehrerer betroffenen Personen. Dies kommt auch der Funktionsweise und der Leistungsfähigkeit des Rechtssystems zugute, da ähnliche Klagen gruppiert und zusammen untersucht werden.

⁶⁵⁰ DSGVO, Artikel 80.

6.2.3. Haftung und Recht auf Schadensersatz

Das Recht auf ein wirksames Rechtsmittel muss die betroffenen Personen dazu ermächtigen, Schadensersatz für jeglichen Schaden, der infolge der Verletzung geltender Datenschutzvorschriften entstanden ist, zu verlangen. Die Haftung der Verantwortlichen und Auftragsverarbeiter für unrechtmäßige Verarbeitung wird in der DSGVO ausdrücklich anerkannt.⁶⁵¹ Die DSGVO verleiht den betroffenen Personen das Recht, vom Verantwortlichen oder vom Auftragsverarbeiter Schadensersatz für materielle und immaterielle Schäden zu erhalten, und legt in ihren Erwägungsgründen dar, dass „[d]er Begriff des Schadens [...] im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden [sollte], die den Zielen der DSGVO in vollem Umfang entspricht“.⁶⁵² Sofern die Verantwortlichen ihren Verpflichtungen aus der DSGVO nicht nachkommen, haften sie und könnten Schadensersatzforderungen unterliegen. Auftragsverarbeiter personenbezogener Daten haften für den durch eine Verarbeitung verursachten Schaden nur dann, wenn sie ihren speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen sind oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Verantwortlichen oder gegen diese Anweisungen gehandelt haben. Hat ein Verantwortlicher oder Auftragsverarbeiter vollständigen Schadenersatz gezahlt, so sieht die DSGVO vor, dass er von den übrigen an derselben Verarbeitung beteiligten Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückfordern kann, der ihrem Verantwortungsgrad für den Schaden entspricht.⁶⁵³ Gleichzeitig werden Ausnahmen von der Haftung sehr streng gehandhabt und erfordern den Nachweis, dass der Verantwortliche oder der Auftragsverarbeiter in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Der Schadensersatz muss im Verhältnis zum erlittenen Schaden „vollständig und wirksam“ sein. Sofern der Schaden durch die Verarbeitung mehrerer Verantwortlicher oder Auftragsverarbeiter verursacht wurde, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden. Diese Vorschrift dient der Sicherstellung eines wirksamen Schadensersatzes für die betroffenen Personen und eines koordinierten Ansatzes in Bezug auf die Einhaltung der Vorschriften seitens der an Verarbeitungstätigkeiten beteiligten Verantwortlichen und Auftragsverarbeiter.

651 a.a.O., Artikel 82.

652 a.a.O., Erwägungsgrund 146.

653 a.a.O., Artikel 82 Absatz 2 und 5.

Beispiel: Die betroffenen Personen sind nicht dazu verpflichtet, alle für einen Schaden verantwortlichen Stellen zu verklagen und von allen Schadensersatz zu fordern, da dies kostspielige und langwierige Verfahren zur Folge hätte. Es genügt, einen der gemeinsam Verantwortlichen zu verklagen, der für den gesamten Schaden zur Haftung gezogen werden kann. In solchen Fällen ist der Verantwortliche oder Auftragsverarbeiter, der für den Schaden aufkommt, im Anschluss daran dazu berechtigt, von den übrigen an der Verarbeitung beteiligten und für die Verletzung verantwortlichen Stellen den ihrem Anteil an der Verantwortung für den Schaden entsprechenden Betrag einzuziehen. Diese Vorgehensweisen zwischen den verschiedenen gemeinsam Verantwortlichen und Auftragsverarbeitern finden erst statt, nachdem die betroffene Person ihren Schadensersatz erhalten hat und die betroffene Person ist daran nicht beteiligt.

Im Recht des Europarates verpflichtet Artikel 12 des Modernisierten Übereinkommens Nr. 108 die Vertragsparteien zur Einrichtung angemessener Rechtsbehelfe bei Verletzungen der nationalen Rechtsvorschriften zur Umsetzung der Erfordernisse des Übereinkommens. Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 gibt an, dass die Rechtsbehelfe die Möglichkeit der gerichtlichen Anfechtung eines Beschlusses oder einer Praktik vorsehen müssen, wobei auch außergerichtliche Rechtsbehelfe bereitzustellen sind.⁶⁵⁴ Die Modalitäten und unterschiedlichen Vorschriften im Zusammenhang mit dem Zugang zu diesen Rechtsbehelfen werden ebenso wie das zu befolgende Verfahren dem Ermessen jeder Vertragspartei überlassen. Die Vertragsparteien und die nationalen Gerichte sollten auch Bestimmungen in Bezug auf die finanzielle Entschädigung von durch die Verarbeitung verursachten materiellen und immateriellen Schäden vorsehen, sowie die Möglichkeit von Sammelklagen.⁶⁵⁵

6.2.4. Sanktionen

Im **Recht des Europarates** sieht Artikel 12 des Modernisierten Übereinkommens Nr. 108 vor, dass jede Vertragspartei geeignete Sanktionen und Rechtsmittel für Verletzungen der Vorschriften des innerstaatlichen Rechts festlegt, welche den im Übereinkommen Nr. 108 aufgestellten Grundsätzen für den Datenschutz Wirkung verleihen. Das Übereinkommen sieht von der

⁶⁵⁴ Erläuternder Bericht zum Modernisierten Übereinkommen 108, Absatz 100.

⁶⁵⁵ a.a.O.

Festsetzung oder Auferlegung eines bestimmten Katalogs von Sanktionen ab. Es weist hingegen klar darauf hin, dass die Festsetzung der Art der gerichtlichen oder außergerichtlichen Sanktionen, bei denen es sich um straf-, verwaltungs- oder zivilrechtliche Sanktionen handeln kann, im Ermessen jeder Vertragspartei liegt. Der erläuternde Bericht zum Modernisierten Übereinkommen Nr. 108 sieht vor, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sein müssen.⁶⁵⁶ Die Vertragsparteien müssen sich bei der Festsetzung der Art und Schwere der in ihrer innerstaatlichen Rechtsordnung verfügbaren Sanktionen an diesen Grundsatz halten.

Im **EU-Recht** ermächtigt Artikel 83 DSGVO die Aufsichtsbehörden der Mitgliedstaaten zur Verhängung von Geldbußen für Verstöße gegen die Verordnung. Die Höhe der Geldbußen und die seitens der nationalen Behörden bei der Festsetzung der Verhängung oder Nichtverhängung einer Geldbuße zu berücksichtigenden Umstände sowie die Gesamtobergrenzen einer Geldbuße sind ebenfalls in Artikel 83 dargelegt. Folglich ist das Sanktionssystem europaweit harmonisiert.

In Bezug auf die Geldbußen verfolgt die DSGVO einen gestuften Ansatz. Die Aufsichtsbehörden sind zur Verhängung von Geldbußen für Verstöße gegen die Verordnung befugt, deren Höhe sich auf bis zu 20 000 000 EUR oder im Fall eines Unternehmens auf bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes belaufen kann, je nachdem, welcher der Beträge höher ist. Zu den Verstößen, die eine Geldbuße dieser Höhe auslösen können, zählen Verstöße gegen die Grundsätze für die Verarbeitung und die Bedingungen für die Einwilligung, Verstöße gegen die Rechte der betroffenen Personen und die Bestimmungen der Verordnung in Bezug auf die Übermittlung personenbezogener Daten an Empfänger in Drittländern. Für andere Verstöße können die Aufsichtsbehörden Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes verhängen, je nachdem, welcher der Beträge höher ist.

Bei der Festsetzung der Art und Höhe der zu verhängenden Geldstrafe müssen die Aufsichtsbehörden eine Reihe von Faktoren berücksichtigen.⁶⁵⁷ So müssen sie beispielsweise die Art, Schwere und Dauer des Verstoßes, die Kategorien der betroffenen personenbezogenen Daten und ob der Verstoß vorsätzlich

⁶⁵⁶ a.a.O.

⁶⁵⁷ DSGVO, Artikel 83 Absatz 2.

oder fahrlässig erfolgte, ordnungsgemäß prüfen. Ebenso berücksichtigt werden sollte, ob ein Verantwortlicher oder Auftragsverarbeiter Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens getroffen hat. Ebenso sind der Umfang der Zusammenarbeit mit der Aufsichtsbehörde im Anschluss an den Verstoß und die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde (ob er beispielsweise seitens der für die Verarbeitung verantwortlichen Stelle oder seitens einer betroffenen Person mitgeteilt wurde, deren Rechte verletzt wurden) weitere wichtige Faktoren, die die Aufsichtsbehörden bei ihrer Entscheidung leiten.⁶⁵⁸

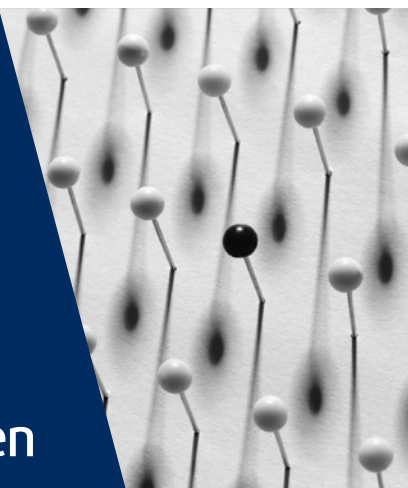
Neben der Möglichkeit zur Verhängung von Geldbußen steht den Aufsichtsbehörden ein breites Spektrum anderer Abhilfebefugnisse zur Verfügung. Die sogenannten „Abhilfebefugnisse“ der Aufsichtsbehörden sind in Artikel 58 DSGVO dargelegt. Sie reichen von Anweisungen, Warnungen und Verwarnungen der Verantwortlichen und der Auftragsverarbeiter bis hin zur Verhängung von vorübergehenden oder dauerhaften Verboten von Verarbeitungstätigkeiten.

Bei Verstößen gegen EU-Recht durch Organe und Einrichtungen der EU können aufgrund des besonderen Geltungsbereichs der Datenschutzverordnung für EU-Organe Sanktionen in Form von Disziplinarmaßnahmen vorgesehen werden. Artikel 49 der Verordnung besagt: „Jede vorsätzliche oder fahrlässige Nichteinhaltung der Verpflichtungen aus dieser Verordnung zieht für Beamte oder sonstige Bedienstete der Europäischen Gemeinschaften disziplinarische Maßnahmen nach sich [...]“.

658 Artikel-29-Datenschutzgruppe (2017), *Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679*, WP 253, 3. Oktober 2017.

7

Internationale Datenübermittlungen und freier Verkehr personenbezogener Daten



EU	Behandelte Themen	Europarat
Übermittlung personenbezogener Daten		
DSGVO, Artikel 44	Begriff	Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 1 und 2
Freier Verkehr personenbezogener Daten		
DSGVO, Artikel 1 Absatz 3 und Erwägungsgrund 170	Zwischen EU-Mitgliedstaaten	
	Zwischen Vertragsparteien des Übereinkommens Nr. 108	Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 1
Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen		
DSGVO, Artikel 45 C-362/14, Maximilian Schrems / Data Protection Commissioner [GK], 2015	Angemessenheitsbeschluss/ Drittländer oder internationale Organisationen mit angemessenem Schutzniveau	Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 2

EU	Behandelte Themen	Europarat
DSGVO, Artikel 46 Absatz 1 und Artikel 46 Absatz 2	Geeignete Garantien einschließlich durchsetzbarer Rechte und Rechtsbehelfe für die betroffenen Personen, die durch Standarddatenschutzklauseln, verbindliche interne Datenschutzvorschriften, Verhaltensregeln und Zertifizierungsverfahren bereitgestellt werden	Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 2, 3, 5 und 6
DSGVO, Artikel 46 Absatz 3	Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde: Vertragsklauseln und Bestimmungen in Verwaltungsvereinbarungen zwischen Behörden	
DSGVO, Artikel 46 Absatz 5	Bestehende Genehmigungen auf Grundlage der Richtlinie 95/46/EG	
DSGVO, Artikel 47	Verbindliche interne Datenschutzvorschriften	
DSGVO, Artikel 49	Ausnahmen für bestimmte Fälle	Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 4
Beispiele: EU-US PNR-Abkommen EU-US SWIFT-Abkommen	Internationale Abkommen	Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 3 Buchstabe a

Im EU-Recht gewährleistet die DSGVO den freien Datenverkehr innerhalb der Europäischen Union. Sie enthält jedoch auch genaue Anforderungen an die Übermittlung personenbezogener Daten an Drittländer außerhalb der EU und an internationale Organisationen. Die DSGVO erkennt die Bedeutung solcher Übermittlungen an, insbesondere angesichts des internationalen Handels und der internationalen Zusammenarbeit, ist sich aber auch der erhöhten Gefahr für personenbezogene Daten bewusst. Die DSGVO zielt folglich darauf ab, personenbezogenen Daten, die an Drittländer übermittelt werden, dasselbe Schutzniveau bereitzustellen, das diese in der EU genießen.⁶⁵⁹ Auch das Recht

⁶⁵⁹ DSGVO, Erwägungsgrund 101 und 116.

des Europarates kennt die Bedeutung davon, Regeln für grenzüberschreitende Datenübermittlungen einzuführen, die auf einem freien Datenverkehr zwischen Vertragsparteien und genauen Anforderungen für Übermittlungen an Nicht-Vertragsparteien gründen.

7.1. Wesen der Übermittlung personenbezogener Daten

Kernpunkte

- Im Recht der EU und im Recht des Europarates gibt es Vorschriften für die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen.
- Die Gewährleistung des Schutzes der Rechte der betroffenen Person bei der Übermittlung der Daten nach außerhalb der EU ermöglicht, dass der durch das EU-Recht gewährte Schutz den aus der EU stammenden personenbezogenen Daten folgt.

Im **Recht des Europarates** versteht man unter grenzüberschreitendem Datenverkehr die Übermittlung personenbezogener Daten an Empfänger, die einer ausländischen Hoheitsgewalt unterstehen.⁶⁶⁰ Grenzüberschreitender Datenverkehr an einen Empfänger, der keiner Rechtsordnung einer Vertragspartei untersteht, ist nur im Falle des Vorhandenseins eines angemessenen Schutzniveaus erlaubt.⁶⁶¹

Das **EU-Recht** regelt die Übermittlung „personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen [...]“.⁶⁶² Dieser Datenverkehr ist nur zulässig, wenn die in Kapitel V DSGVO dargelegten Vorschriften eingehalten werden.

Der grenzüberschreitende Verkehr personenbezogener Daten ist im Recht des Europarates und im EU-Recht an einen Empfänger erlaubt, der der Rechtsordnung

660 Zusatzprotokoll zum Modernisierten Übereinkommen Nr. 108, Artikel 2 Absatz 1.

661 Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 2.

662 DSGVO, Artikel 44.

eines Vertragsstaates bzw. eines Mitgliedstaates untersteht. In beiden Rechtssystemen ist auch die Übermittlung von Daten an ein Land erlaubt, das keine Vertragspartei oder kein Mitgliedstaat ist, vorausgesetzt, bestimmte Bedingungen sind erfüllt.

7.2. Freier Verkehr personenbezogener Daten zwischen Mitgliedstaaten oder zwischen Vertragsparteien

Kernpunkt

- Der europaweite Verkehr personenbezogener Daten sowie die Übermittlung personenbezogener Daten unter den Vertragsparteien des Modernisierten Übereinkommens Nr. 108 darf nicht eingeschränkt werden. Da es sich jedoch nicht bei allen Vertragsparteien des Modernisierten Übereinkommens Nr. 108 um Mitgliedstaaten der EU handelt, sind Übermittlungen von einem EU-Mitgliedstaat an ein Drittland, bei dem es sich gleichwohl um eine Vertragspartei des Übereinkommens Nr. 108 handelt, nicht möglich, sofern sie die in der DSGVO dargelegten Bedingungen nicht erfüllen.

Im **Recht des Europarates** muss es zwischen den Vertragsparteien des Modernisierten Übereinkommens Nr. 108 einen freien Verkehr personenbezogener Daten geben. Die Übermittlung kann jedoch verboten sein, wenn „ein reales und ernstes Risiko besteht, dass die Übermittlung an eine andere Partei zur Umgehung der Bestimmungen des Übereinkommens führt“, oder wenn eine Partei „durch harmonisierte Schutzvorschriften für Staaten gebunden sind, die einer regionalen internationalen Organisation angehören“.⁶⁶³

Im **EU-Recht** sind Einschränkungen oder Verbote des freien Verkehrs personenbezogener Daten zwischen den EU-Mitgliedstaaten aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten untersagt.⁶⁶⁴ Der Bereich für den freien Datenverkehr wurde durch das Abkommen

⁶⁶³ Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 1.

⁶⁶⁴ DSGVO, Artikel 1 Absatz 3.

über den Europäischen Wirtschaftsraum (EWR) noch erweitert,⁶⁶⁵ damit gehören auch Island, Liechtenstein und Norwegen zum Daten-Binnenmarkt.

Beispiel: Übermittelt ein Unternehmen eines internationalen Konzerns mit Sitz in mehreren Mitgliedstaaten, darunter Slowenien und Frankreich, personenbezogene Daten von Slowenien nach Frankreich, darf dieser Datenverkehr durch das einzelstaatliche Recht Sloweniens zum Schutz personenbezogener Daten nicht eingeschränkt oder untersagt werden.

Möchte dieses slowenische Konzernunternehmen jedoch dieselben personenbezogenen Daten an das Mutterunternehmen in Malaysia übermitteln, muss der slowenische Datenexporteur die Vorschriften aus Kapitel V DSGVO berücksichtigen. Diese Bestimmungen schützen personenbezogene Daten der betroffenen Personen, die der Rechtsordnung der EU unterstehen.

Im EU-Recht gilt Richtlinie (EU) 2016/680 für den Verkehr personenbezogener Daten an Mitgliedstaaten des EWR zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.⁶⁶⁶ Diese gewährleistet auch, dass der Austausch personenbezogener Daten seitens zuständiger Behörden innerhalb der Union nicht aus Datenschutzgründen eingeschränkt oder verboten ist. Im Recht des Europarates ist jede Verarbeitung personenbezogener Daten (einschließlich deren grenzüberschreitenden Verkehrs mit anderen Vertragsparteien des Übereinkommens Nr. 108) ohne Ausnahmen, die auf Zwecken oder Aufgaben beruhen, vom Geltungsbereich des Übereinkommens Nr. 108 erfasst, wenngleich die Vertragsparteien Ausnahmen vorsehen können. Alle EWR-Mitglieder sind auch Vertragsparteien des Übereinkommens Nr. 108.

665 Beschluss des Rates und der Kommission vom 13. Dezember 1993 über den Abschluss des Abkommens über den Europäischen Wirtschaftsraum zwischen den Europäischen Gemeinschaften und ihren Mitgliedstaaten sowie der Republik Österreich, der Republik Finnland, der Republik Island, dem Fürstentum Liechtenstein, dem Königreich Norwegen, dem Königreich Schweden und der Schweizerischen Eidgenossenschaft, ABl. L 1 vom 3.1.1994.

666 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 4.5.2016.

7.3. Übermittlung personenbezogener Daten an Drittländer/Nicht-Vertragsparteien und internationale Organisationen

Kernpunkte

- Sowohl der **Europarat** als auch die **EU** erlauben die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, vorausgesetzt, bestimmte Bedingungen für den Schutz personenbezogener Daten sind erfüllt.
- Nach dem **Recht des Europarates** kann ein angemessenes Schutzniveau durch die Rechtsvorschriften des Staates oder der internationalen Organisation oder durch das Vorhandensein angemessener Standards erzielt werden.
- Im **EU-Recht** können Übermittlungen stattfinden, wenn das Drittland ein angemessenes Schutzniveau gewährleistet oder wenn der Verantwortliche oder Auftragsverarbeiter über Maßnahmen wie Standarddatenschutzklauseln oder verbindliche interne Datenschutzvorschriften geeignete Garantien einschließlich durchsetzbarer Rechte der betroffenen Personen und Rechtsbehelfe bereitstellt.
- **Sowohl das Recht des Europarates als auch das EU-Recht** sehen Ausnahmeklauseln vor, die die Übermittlung personenbezogener Daten unter bestimmten Umständen selbst dann erlauben, wenn weder ein angemessenes Schutzniveau noch geeignete Garantien bestehen.

Wenngleich sowohl das Recht des Europarates als auch das EU-Recht den Datenverkehr in Drittländer oder an internationale Organisationen erlauben, setzen sie hierfür unterschiedliche Bedingungen fest. Jedes Bedingungs paket berücksichtigt die unterschiedliche Struktur und die unterschiedlichen Zwecke der jeweiligen Organisation.

Im **EU-Recht** gibt es grundsätzlich zwei Möglichkeiten, die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen zu erlauben. Die Übermittlung personenbezogener Daten kann auf der Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission erfolgen,⁶⁶⁷ oder bei Nichtvorliegen eines solchen Angemessenheitsbeschlusses im Falle der Bereitstellung geeigneter Garantien seitens des Verantwortlichen oder des Auftragsverarbeiters, zu denen durchsetzbare Rechte und Rechtsbehelfe für die betroffenen Personen

⁶⁶⁷ DSGVO, Artikel 45.

zählen.⁶⁶⁸ Sofern weder ein Angemessenheitsbeschluss noch geeignete Garantien vorliegen, stehen eine Reihe von Ausnahmen zur Verfügung.

Im **Recht des Europarates** ist die freie Datenübermittlung an Nicht-Vertragsparteien des Übereinkommens nur auf Grundlage der nachstehenden Voraussetzungen erlaubt:

- die Rechtsvorschriften dieses Staates oder dieser internationalen Organisation einschließlich der anwendbaren internationalen Verträge oder Vereinbarungen gewährleisten geeignete Garantien;
- es sind für den Einzelfall formulierte oder genehmigte standardisierte Garantien vorhanden, die in Form von rechtsverbindlichen und durchsetzbaren Instrumenten bereitgestellt werden, die seitens der an der Übermittlung und Weiterverarbeitung beteiligten Personen angenommen und umgesetzt wurden.⁶⁶⁹

Ähnlich wie im EU-Recht steht in Ermangelung eines angemessenen Datenschutzniveaus eine Reihe von Ausnahmen zur Verfügung.

7.3.1. Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

Im **EU-Recht** sieht Artikel 45 DSGVO den freien Verkehr personenbezogener Daten an Drittländer vor, die über ein angemessenes Datenschutzniveau verfügen. Der EuGH stellte klar, dass der Begriff „angemessenes Schutzniveau“ erfordert, dass das Drittland ein Schutzniveau der Grundrechte und Freiheiten gewährleistet, das dem in der EU gesetzlich garantierten Niveau „der Sache nach gleichwertig ist“⁶⁷⁰. Gleichzeitig können sich die Mittel, auf die das Drittland zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden, die in der EU herangezogen werden, da die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den EU-Vorschriften erfordert.⁶⁷¹

⁶⁶⁸ a.a.O., Artikel 46.

⁶⁶⁹ Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 3 Buchstaben a und b.

⁶⁷⁰ EuGH, C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015, Randnr. 96.

⁶⁷¹ a.a.O., Randnr. 74. Siehe auch Europäische Kommission (2017), Mitteilung der Kommission an das Europäische Parlament und den Rat „Austausch und Schutz personenbezogener Daten in einer globalisierten Welt“, COM(2017)7 final vom 10. Januar 2017, S. 6.

Die Europäische Kommission bewertet das Datenschutzniveau in Drittländern unter Berücksichtigung ihres nationalen Rechts und der geltenden internationalen Verpflichtungen. Die Teilnahme eines Landes an multilateralen oder regionalen Systemen, insbesondere in Bezug auf den Schutz von personenbezogenen Daten, ist ebenfalls zu berücksichtigen. Sofern die Europäische Kommission der Ansicht ist, dass das Drittland oder die internationale Organisation ein angemessenes Schutzniveau gewährleistet, kann sie einen Angemessenheitsbeschluss erlassen, der verbindliche Wirkung hat.⁶⁷² Gleichwohl hat der EuGH festgestellt, dass nationale Aufsichtsbehörden nach wie vor dafür zuständig sind, die Eingabe einer Person zu prüfen, die sich auf den Schutz ihrer personenbezogenen Daten bezieht, die in ein Drittland übermittelt wurden, von dem die Kommission der Ansicht war, dass es ein angemessenes Schutzniveau gewährleistet, wenn diese Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten.⁶⁷³

Die Europäische Kommission kann auch die Angemessenheit eines Gebiets innerhalb eines Drittlandes bewerten oder sich auf bestimmte Branchen beschränken, wie beispielsweise im Falle des privaten Wirtschaftsrechts in Kanada.⁶⁷⁴ Es gibt auch Angemessenheitsfeststellungen für Übermittlungen auf der Grundlage von Abkommen zwischen der EU und Drittländern. Diese Entscheidungen beziehen sich ausschließlich auf eine einzige Art von Datenübermittlungen wie die Übermittlung von Fluggastdatensätzen (PNR-Daten) durch Fluggesellschaften an ausländische Grenzkontrollbehörden bei Flügen aus der EU in bestimmte Länder in Übersee (siehe [Abschnitt 7.3.4](#)).

Angemessenheitsbeschlüsse unterliegen einer fortwährenden Kontrolle. Die Europäische Kommission überprüft diese Beschlüsse regelmäßig, um Entwicklungen zu verfolgen, die sich auf ihren Status auswirken könnten. Ist die Europäische Kommission der Ansicht, dass das Drittland oder die internationale Organisation die den Angemessenheitsbeschluss rechtfertigenden Bedingungen nicht länger erfüllt, kann sie den Beschluss ändern, aussetzen oder widerrufen. Die Kommission kann auch Beratungen mit dem betreffenden Drittland

672 Eine laufend aktualisierte Liste von Ländern, für die ein Angemessenheitsbeschluss vorliegt, findet sich auf der Website der Europäischen Kommission, Generaldirektion Justiz.

673 Rechtssache C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015, Randnrn. 63 und 65–66.

674 Europäische Kommission (2002), Entscheidung 2002/2/EG vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, ABl. L 2 vom 4.1.2002.

oder der betreffenden internationalen Organisation aufnehmen, um Abhilfe für das Problem zu schaffen, das zu ihrem Beschluss geführt hat.

Von der Europäischen Kommission auf Grundlage der Richtlinie 95/46/EG erlassene Angemessenheitsbeschlüsse bleiben so lange in Kraft, bis sie durch einen in Übereinstimmung mit den Vorschriften aus Artikel 45 DSGVO erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Bis heute hat die Europäische Kommission Andorra, Argentinien, Kanada (Handelsorganisationen, die unter den Anwendungsbereich des Personal Information Protection and Electronic Documents Act – PIPEDA fallen), die Färöer Inseln, Guernsey, die Insel Man, Israel, Jersey, Neuseeland, die Schweiz und Uruguay als Länder anerkannt, die angemessenen Schutz gewähren. In Bezug auf Datenübermittlungen in die Vereinigten Staaten nahm die Europäische Kommission im Jahr 2000 eine Angemessenheitsentscheidung an, die die Datenübermittlung an Unternehmen erlaubte, die den von ihnen gewährleisteten Schutz für aus der EU übermittelte personenbezogene Daten und die Einhaltung der sogenannten „Safe-Harbor-Grundsätze“ selbst bescheinigten.⁶⁷⁵ Der EuGH setzte diese Entscheidung 2015 außer Kraft und im Juli 2016 wurde ein neuer Angemessenheitsbeschluss angenommen, dem die Unternehmen seit 1. August 2016 beitreten können.

Beispiel: In der Rechtssache *Schrems*⁶⁷⁶ nutzte der österreichische Staatsangehörige Maximilian Schrems seit mehreren Jahren Facebook. Einige oder alle der von Herrn Schrems Facebook bereitgestellten Daten wurden von der irischen Tochtergesellschaft von Facebook an in den Vereinigten Staaten befindende Server übermittelt, wo sie verarbeitet wurden. Herr Schrems legte eine Beschwerde bei der irischen Datenschutzbehörde ein, in deren Rahmen er den Standpunkt vertrat, dass das Recht und die Praxis der Vereinigten Staaten angesichts der Enthüllungen des amerikanischen Whistleblowers Edward Snowden in Bezug auf die Überwachungstätigkeiten der amerikanischen Nachrichtendienste keinen hinreichenden Schutz für

⁶⁷⁵ Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000. Die Entscheidung wurde vom EuGH in der Rechtssache C-632/14, *Maximilian Schrems / Data Protection Commissioner* [GK] für ungültig erklärt.

⁶⁷⁶ C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015.

die in dieses Land übermittelten Daten boten. Die irische Behörde wies die Beschwerde mit der Begründung zurück, dass die Kommission in ihrer Entscheidung vom 26. Juli 2000 die Ansicht vertrat, dass die Vereinigten Staaten im Rahmen des „Safe-Harbor“-Systems ein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleisten. Die Rechtssache wurde vor den irischen High Court gebracht, der sie dem EuGH im Rahmen einer Vorabentscheidung vorlegte.

Der EuGH entschied, dass die Entscheidung der Kommission zur Angemessenheit des Safe-Harbor-Systems ungültig sei. Der EuGH stellte zunächst fest, dass die Entscheidung es ermöglichte, Grundsätze des Safe-Harbor-Datenschutzes auf Grundlage der Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen oder von Rechtsvorschriften der Vereinigten Staaten zu beschränken. Die Entscheidung ermöglichte demnach Eingriffe in die Grundrechte der Personen, deren personenbezogene Daten in die Vereinigten Staaten übermittelt wurden oder werden könnten.⁶⁷⁷ Er stellte überdies fest, dass die Entscheidung weder eine Feststellung dazu enthält, ob es in den Vereinigten Staaten Regeln gibt, die dazu dienen, derartige Eingriffe zu begrenzen, noch eine Feststellung zum Bestehen eines wirksamen gerichtlichen Schutzes gegen derartige Eingriffe.⁶⁷⁸ Der EuGH hob hervor, dass das innerhalb der EU garantierte Schutzniveau der Grundrechte und Freiheiten erfordere, dass Rechtsvorschriften, die einen Eingriff in Artikel 7 und 8 darstellen, klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme enthalten und Mindestanforderungen, Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten aufstellen müssen.⁶⁷⁹ In Anbetracht dessen, dass die Kommission in ihrer Entscheidung nicht festgestellt hatte, dass die Vereinigten Staaten aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen tatsächlich ein solches Schutzniveau gewährleisten, befand der EuGH, dass die Entscheidung die Anforderungen der entsprechenden Übermittlungsbestimmung in der Datenschutzrichtlinie nicht erfülle und demnach ungültig sei.⁶⁸⁰

⁶⁷⁷ a.a.O., Randnr. 87.

⁶⁷⁸ a.a.O., Randnrn. 88–89.

⁶⁷⁹ a.a.O., Randnrn. 91–92.

⁶⁸⁰ a.a.O., Randnrn. 96–97.

Das Schutzniveau der Vereinigten Staaten war demnach den seitens der EU gewährten Grundrechten und Freiheiten nicht „der Sache nach gleichwertig“.⁶⁸¹ Der EuGH führte aus, dass verschiedene Artikel der Charta der Grundrechte der EU verletzt worden seien. Erstens werde der Wesensgehalt von Artikel 7 verletzt, da die Gesetze der Vereinigten Staaten „es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen“. Zweitens werde der Wesensgehalt von Artikel 47 auch deshalb verletzt, weil die Gesetze keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken. Da die Safe-Harbor-Regelung die oben genannten Artikel verletze, seien die personenbezogenen Daten schließlich nicht länger rechtmäßig verarbeitet worden, was zu einer Verletzung von Artikel 8 führte.

Nachdem der EuGH die Safe-Harbor-Entscheidung für ungültig erklärte, vereinbarten die Kommission und die Vereinigten Staaten mit dem EU-US-Datenschutzschild einen neuen Rechtsrahmen. Am 12. Juli 2016 nahm die Kommission einen Beschluss an, in dem sie erklärte, dass die Vereinigten Staaten ein angemessenes Schutzniveau für seitens der Union im Rahmen des Datenschutzschilds an Organisationen in den Vereinigten Staaten übermittelte personenbezogene Daten gewährleisten.⁶⁸²

Ähnlich wie Safe-Harbor bezweckt auch das EU-US-Datenschutzschild den Schutz personenbezogener Daten, die zu Handelszwecken von der EU in die Vereinigten Staaten übermittelt werden.⁶⁸³ US-Unternehmen können sich freiwillig durch Selbstzertifizierung in die Datenschutzschild-Liste anmelden und verpflichten sich damit, den Datenschutzstandard einzuhalten. Die zuständigen

681 a.a.O., Randnrn. 73–74 und 96.

682 [Durchführungsbeschluss \(EU\) 2016/1250 der Kommission](#) vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. L 207 vom 1.8.2016. Die Artikel-29-Datenschutzgruppe begrüßte die durch den Datenschutzschildmechanismus im Vergleich zur Safe-Harbor-Entscheidung eingeführten Verbesserungen und lobte die Kommission und die Behörden der Vereinigten Staaten für die in der endgültigen Fassung der Dokumente zum Datenschutzschild erfolgte Berücksichtigung der in ihrer Stellungnahme WP238 über den Entwurf des Angemessenheitsbeschlusses des EU-US-Datenschutzschilds zum Ausdruck gebrachten Bedenken. Gleichwohl hob sie eine Reihe noch offener Fragen hervor. Für weitere Einzelheiten siehe Artikel-29-Datenschutzgruppe *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, angenommen am 13. April 2016, 16/EN WP 238.

683 Für weitere Informationen siehe das [EU-U.S. Privacy Shield Factsheet](#).

US-Behörden überwachen und prüfen die Einhaltung dieser Standards seitens der zertifizierten Unternehmen.

Insbesondere sieht das Datenschutzschild Nachstehendes vor:

- Datenschutzverpflichtungen für Unternehmen, die personenbezogene Daten aus der EU empfangen;
- Schutz und Rechtsschutz für die Personen, insbesondere die Einrichtung eines Ombudsmechanismus, der unabhängig von den US-Nachrichtendiensten ist und sich mit Beschwerden von Einzelnen befasst, die der Ansicht sind, dass ihre personenbezogenen Daten seitens der US-Behörden im Bereich der nationalen Sicherheit unrechtmäßig verwendet wurden;
- eine gemeinsame jährliche Überprüfung zur Überwachung der Umsetzung;⁶⁸⁴ die erste Überprüfung fand im September 2017 statt.⁶⁸⁵

Die US-Regierung hat schriftliche Zusagen und Zusicherungen gemacht, die den Beschluss zum Datenschutzschild begleiten. Diese sehen Einschränkungen und Schutzmechanismen für den Zugang der US-Regierung zu personenbezogenen Daten zu Zwecken der Strafverfolgung und der nationalen Sicherheit vor.

7.3.2. Datenübermittlung vorbehaltlich geeigneter Garantien

Sowohl das **EU-Recht** als auch das **Recht des Europarates** erkennen geeignete Garantien zwischen dem die Daten ausführenden Verantwortlichen und dem Empfänger im Drittland oder in der internationalen Organisation als mögliche Maßnahme zur Gewährleistung eines hinreichenden Datenschutzes durch den Empfänger an.

Im **EU-Recht** ist die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation erlaubt, sofern der Verantwortliche

684 Für weitere Informationen siehe die Website der Europäischen Kommission zum [EU-US-Datenschutzschild](#).

685 Europäische Kommission, *Bericht der Kommission an das Europäische Parlament und den Rat, Erster Bericht zur jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds*, COM(2017) 611 final, 18. Oktober 2017. Siehe auch, Artikel-29-Datenschutzgruppe, *EU – U.S. Privacy Shield – First annual Joint Review*, angenommen am 28 November 2017, 17/EN WP 255.

oder der Auftragsverarbeiter geeignete Garantien und durchsetzbare Rechte vorsehen und den betroffenen Personen wirksame Rechtsbehelfe zur Verfügung stehen.⁶⁸⁶ Das Verzeichnis der „geeigneten Garantien“ ist ausschließlich im EU-Datenschutzrecht enthalten. Geeignete Garantien können wie folgt eingerichtet werden:

- durch ein rechtlich bindendes und durchsetzbares Dokument zwischen den Behörden oder öffentlichen Stellen;
- durch verbindliche interne Datenschutzvorschriften;
- durch Standarddatenschutzklauseln, die von der Kommission oder von einer Aufsichtsbehörde erlassen werden;
- durch Verhaltensregeln;
- durch Zertifizierungsverfahren.⁶⁸⁷

Individualisierte Vertragsklauseln zwischen dem Verantwortlichen oder Auftragsverarbeiter in der EU und dem Datenempfänger in einem Drittland sind eine andere Maßnahme zur Bereitstellung geeigneter Sicherheiten. Solche Vertragsklauseln sind jedoch von der zuständigen Aufsichtsbehörde zu genehmigen, bevor sie für die Übermittlung personenbezogener Daten herangezogen werden können. Ebenso können sich Behörden Datenschutzbestimmungen bedienen, die in ihren Verwaltungsvereinbarungen enthalten sind, vorausgesetzt, diese wurden von der Aufsichtsbehörde genehmigt.⁶⁸⁸

Im **Recht des Europarates** sind die Datenübermittlungen an einen Staat oder an eine internationale Organisation, die keine Vertragspartei des Modernisierten Übereinkommens Nr. 108 ist, unter der Voraussetzung erlaubt, dass ein angemessenes Schutzniveau sichergestellt ist. Dies kann wie folgt erreicht werden:

- durch das Recht des Staates oder der internationalen Organisation, oder
- durch für den Einzelfall formulierte oder standardisierte Garantien, die Bestandteil eines rechtsverbindlichen Dokuments sind.⁶⁸⁹

686 DSGVO, Artikel 46.

687 DSGVO, Artikel 46 Absatz 1 Buchstabe c und d, Absatz 2 Buchstabe a, b, e und f und Artikel 47.

688 a.a.O., Artikel 46 Absatz 3.

689 Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 3 Buchstabe b.

Datenübermittlung aufgrund von Vertragsklauseln

Sowohl das **EU-Recht** als auch das **Recht des Europarates** erkennen Vertragsklauseln zwischen dem die Daten ausführenden Verantwortlichen und dem Empfänger im Drittland oder in der internationalen Organisation als mögliche Maßnahme zur Gewährleistung eines hinreichenden Datenschutzes für den Empfänger an.⁶⁹⁰

Auf **Ebene der EU** hat die Europäische Kommission mit Unterstützung der Artikel-29-Datenschutzgruppe Standardvertragsklauseln ausgearbeitet, die offiziell mit einem Beschluss der Kommission als Nachweis eines angemessenen Datenschutzes bestätigt wurden.⁶⁹¹ Da Beschlüsse der Kommission für die Mitgliedstaaten in allen ihren Teilen verbindlich sind, müssen die für die Überwachung des Datenverkehrs zuständigen einzelstaatlichen Behörden diese Standardvertragsklauseln in ihrer Kontrollpraxis grundsätzlich akzeptieren.⁶⁹² Werden sich der die Daten exportierende Verantwortliche und der Empfänger im Drittland also einig und unterzeichnen sie diese Klauseln, sollte dies für die Aufsichtsbehörde hinreichender Beweis dafür sein, dass angemessene Garantien bestehen. Dennoch befand der EuGH in der Rechtssache *Schrems*, dass die Europäische Kommission nicht dazu berechtigt sei, die Befugnisse der nationalen Aufsichtsbehörden zur Kontrolle der Übermittlung personenbezogener Daten an Drittländer einzuschränken, welche Gegenstand einer Angemessenheitsentscheidung der Kommission war.⁶⁹³ Folglich sind nationale Aufsichtsbehörden nicht daran gehindert, ihre Befugnisse auszuüben und unter anderem eine Übermittlung personenbezogener Daten auszusetzen oder zu verbieten, wenn durch die Übermittlung EU- oder nationale Datenschutzvorschriften verletzt werden, beispielsweise wenn der Datenimporteur die Standardvertragsklauseln missachtet.⁶⁹⁴

690 DSGVO, Artikel 46 Absatz 3; Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 3 Buchstabe b.

691 a.a.O., Artikel 46 Absatz 2 Buchstabe c Gegenwärtig existieren drei Klauselwerke, die gemäß Art. 46 Abs. 5 Satz 2 DSGVO fortgelten.

692 a.a.O., Artikel 46 Absatz 2 Buchstabe c; Vertrag über die Arbeitsweise der Europäischen Union Art. 288 (ex-Artikel 249 EGV).

693 Rechtssache C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015, Randnrn. 96-98 und 102-105.

694 Zur Berücksichtigung des Standpunkts des EuGH in der Rechtssache *Schrems*, änderte die Kommission ihren Beschluss über Standardvertragsklauseln. [Durchführungsbeschluss \(EU\) 2016/2297 der Kommission](#) vom 16. Dezember 2016 zur Änderung der Entscheidung 2001/497/EG und des Beschlusses 2010/87/EU über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer sowie an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. L 344 vom 17.12.2016.

Die Tatsache, dass es im EU-Rechtsrahmen Standarddatenschutzklauseln gibt, sollte die Verantwortlichen jedoch nicht davon abhalten, für den Einzelfall individuelle andere Vertragsklauseln zu formulieren, solange diese von der Aufsichtsbehörde genehmigt werden.⁶⁹⁵ Sie müssten jedoch das gleiche Datenschutzniveau erbringen wie die Standarddatenschutzklauseln. Bei der Genehmigung von für den Einzelfall formulierten Klauseln sind die Aufsichtsbehörden zur Anwendung des Kohärenzverfahrens verpflichtet, um einen europaweit einheitlichen Regelungsansatz zu gewährleisten.⁶⁹⁶ Das bedeutet, dass die zuständige Aufsichtsbehörde ihren Beschlussentwurf zu den Klauseln dem EDSA übermitteln muss. Der EDSA gibt eine Stellungnahme darüber ab, der die Aufsichtsbehörde beim Formulieren ihres Beschlusses weitestgehend Rechnung tragen muss. Sofern sie die Nichtbefolgung der Stellungnahme des EDSA beabsichtigt, wird das Streitbeilegungsverfahren ausgelöst und der Ausschuss erlässt einen verbindlichen Beschluss.⁶⁹⁷

Zu den wichtigsten Merkmalen einer Standarddatenschutzklausel gehören

- eine Drittbegünstigtenklausel, die betroffenen Personen die Möglichkeit zur Ausübung von Vertragsrechten gibt, auch wenn sie nicht Vertragspartei sind;
- die Zustimmung des Datenempfängers oder -einführers, sich im Fall einer Streitigkeit der Amtsbefugnis der nationalen Aufsichtsbehörde und/oder des Gerichts des die Daten ausführenden Verantwortlichen zu unterwerfen.

Derzeit stehen zwei Sätze von Standardvertragsklauseln für Übermittlungen von Verantwortlichen an Verantwortliche zur Verfügung, zwischen denen der die Daten exportierende Verantwortliche wählen kann.⁶⁹⁸ Für Übermittlungen von Verantwortlichen an Auftragsverarbeiter gibt es nur einen Satz

695 DSGVO, Artikel 46 Absatz 3 Buchstabe a.

696 a.a.O., Artikel 63 und Artikel 64 Absatz 1 Buchstabe a.

697 a.a.O., Artikel 64 und Artikel 65.

698 Satz I ist zu finden im Anhang zu Europäische Kommission (2001), Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, ABl. L 181 vom 4.7.2001; Satz II findet sich im Anhang zu Europäische Kommission (2004), Entscheidung 2004/915/EG der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, ABl. L 385 vom 29.12.2004.

Standardvertragsklauseln.⁶⁹⁹ Diese Standardvertragsklauseln sind gegenwärtig jedoch Gegenstand von Gerichtsverfahren.

Beispiel: Nachdem der EuGH die Safe-Harbor-Entscheidung für ungültig erklärte,⁷⁰⁰ konnte die Übermittlung personenbezogener Daten in die Vereinigten Staaten nicht länger aufgrund dieser Angemessenheitsentscheidung erfolgen. Während die Verhandlungen mit den US-Behörden am Laufen waren und der Erlass eines neuen Angemessenheitsbeschlusses anhängig war (der schließlich am 12. Juli 2016 angenommen wurde),⁷⁰¹ konnte die Datenübermittlung lediglich im Rahmen anderer Rechtsgrundlagen wie Standardvertragsklauseln oder verbindlicher interner Datenschutzvorschriften durchgeführt werden. Mehrere Unternehmen wie auch Facebook Irland (gegen das die Rechtssache, die zur Nichtigkeit der Safe-Harbor-Entscheidung führte, vorgebracht wurde), stiegen zur Fortsetzung ihrer Datenübermittlungen zwischen der EU und den Vereinigten Staaten auf Standardvertragsklauseln um.

Herr Schrems legte bei der irischen Aufsichtsbehörde eine Beschwerde ein und ersuchte sie um die Aussetzung der auf Grundlage von Standardvertragsklauseln erfolgten Datenübermittlung an die Vereinigten Staaten. Im Wesentlichen behauptete er, dass es im Hinblick auf die Übermittlung seiner personenbezogenen Daten von der irischen Tochtergesellschaft von Facebook an Facebook Inc. und an sich in den Vereinigten Staaten befindende Server keine Garantie für den Schutz dieser Daten gebe. Facebook Inc. sei an amerikanische Gesetze gebunden, die das Unternehmen zur Offenlegung personenbezogener Daten gegenüber amerikanischen Strafverfolgungsbehörden verpflichten könnten und für Europäer gebe es keinen Rechtsweg zur Anfechtung dieser Praktik.⁷⁰² Aus diesen Gründen hatte der EuGH die Safe-Harbor-Entscheidung für ungültig befunden. Während das Urteil des Gerichtshofs auf die Untersuchung

699 Europäische Kommission (2010), Beschluss 2010/87 der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. L 39 vom 12.2.2010. Zum Zeitpunkt der Abfassung des Handbuchs war die Verwendung von Standardvertragsklauseln als Grundlage für die Übermittlung personenbezogener Daten in die Vereinigten Staaten Gegenstand eines Gerichtsverfahrens vor dem irischen High Court.

700 EuGH, C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015.

701 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. L 207 vom 1.8.2016.

702 Für weitere Informationen siehe die [überarbeitete Klage](#) gegen Facebook Ireland Ltd, die Maximilian Schrems am 1. Dezember 2015 beim irischen Data Protection Commissioner einreichte.

dieser Entscheidung beschränkt war, vertrat der Beschwerdeführer die Auffassung, dass die aufgeworfenen Themen für eine Datenübermittlung auf Grundlage von Vertragsklauseln ebenso relevant seien. Zum Zeitpunkt der Abfassung des Handbuchs wurde die Rechtssache vor dem irischen High Court untersucht. Der Beschwerdeführer möchte die Rechtssache allem Anschein nach vor den EuGH bringen, mit dem Ziel, die Entscheidung der Europäischen Kommission über Standardvertragsklauseln anzufechten. Wie in [Kapitel 5](#) beschrieben, verfügt der EuGH über die alleinige Zuständigkeit für die Nichtigerklärung eines EU-Dokuments.

Datenübermittlung aufgrund verbindlicher interner Datenschutzvorschriften

Das **EU-Recht** erlaubt auch Übermittlungen personenbezogener Daten auf Grundlage von verbindlichen internen Datenschutzvorschriften für die internationale Datenübermittlung, die innerhalb derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, stattfindet.⁷⁰³ Bevor aufgrund verbindlicher interner Datenschutzvorschriften personenbezogene Daten übermittelt werden können, müssen sie seitens der zuständigen Aufsichtsbehörde nach den Vorgaben für verbindliche interne Datenschutzvorschriften und unter Anwendung des Kohärenzverfahrens genehmigt werden.

Um genehmigt zu werden, müssen die verbindlichen internen Datenschutzvorschriften rechtsverbindlich sein, sämtliche wesentlichen Datenschutzgrundsätze umfassen und für alle Mitglieder der Unternehmensgruppe gelten und von diesen durchgesetzt werden können. Sie müssen den betroffenen Personen ausdrücklich durchsetzbare Rechte übertragen, sämtliche wesentlichen Datenschutzgrundsätze umfassen und bestimmte formale Anforderungen einhalten, wie die Angabe der Unternehmensstruktur, die Beschreibung der Datenübermittlung und die Art und Weise der Anwendung der Datenschutzgrundsätze. Dies umfasst auch die Bereitstellung dieser Informationen an die betroffenen Personen. Die verbindlichen internen Datenschutzvorschriften müssen unter anderem die Rechte der betroffenen Personen präzisieren, sowie Bestimmungen in Bezug auf die Haftung für Verstöße gegen die Vorschriften enthalten.⁷⁰⁴ Bei der Genehmigung von verbindlichen internen Datenschutz-

⁷⁰³ DSGVO, Artikel 47.

⁷⁰⁴ Für eine genauere Beschreibung siehe DSGVO, Artikel 47.

vorschriften kommt das (in [Kapitel 5](#) beschriebene) Kohärenzverfahren für die Zusammenarbeit der Aufsichtsbehörden zur Anwendung.

Im Rahmen des Kohärenzverfahrens überprüft die federführende Aufsichtsbehörde die vorgeschlagenen verbindlichen internen Datenschutzvorschriften, erlässt einen Beschlussentwurf und übermittelt diesen dem EDSA. Der Ausschuss gibt eine Stellungnahme darüber ab und die federführende Aufsichtsbehörde kann die verbindlichen internen Datenschutzvorschriften offiziell genehmigen, wobei sie der Stellungnahme des Ausschusses „weitestgehend Rechnung tragen“ muss. Diese Stellungnahme ist nicht rechtsverbindlich, doch sofern die Aufsichtsbehörde die Nichtbefolgung der Stellungnahme beabsichtigt, wird das Streitbeilegungsverfahren ausgelöst und der Ausschuss wird um den mit einer Mehrheit von zwei Dritteln seiner Mitglieder erfolgenden Erlass eines verbindlichen Beschlusses ersucht.⁷⁰⁵

Im **Recht des Europarates** umfassen die für den Einzelfall formulierten oder standardisierten Garantien, die Bestandteil eines rechtsverbindlichen Dokuments sind,⁷⁰⁶ ebenfalls verbindliche interne Datenschutzvorschriften.

7.3.3. Ausnahmen für bestimmte Fälle

Im **EU-Recht** kann die Übermittlung personenbezogener Daten an ein Drittland selbst ohne Angemessenheitsbeschluss oder Garantien wie Standarddatenschutzklauseln oder verbindliche interne Datenschutzvorschriften unter den nachstehenden Voraussetzungen gerechtfertigt sein:

- die betroffene Person willigt ausdrücklich in die Datenverarbeitung ein;
- die betroffene Person geht ein Vertragsverhältnis ein oder bereitet sich darauf vor, in dessen Rahmen die Datenübermittlung ins Ausland erforderlich ist;
- zum Abschluss eines im Interesse der betroffenen Person von dem Verantwortlichen mit einem Dritten geschlossenen Vertrag;

705 a.a.O., Artikel 57 Absatz 1 Buchstabe s, Artikel 58 Absatz 1 Buchstabe l und j, Artikel 64 Absatz 1 Buchstabe f, Artikel 65 Absatz 1 und 2.

706 Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 3 Buchstabe b.

- aus wichtigen Gründen des öffentlichen Interesses;
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen;
- zum Schutz lebenswichtiger Interessen der betroffenen Person;
- zur Übermittlung von Daten aus öffentlichen Registern (hierbei handelt es sich um einen Fall von vorherrschenden Interessen der breiten Öffentlichkeit am Zugang zu in öffentlichen Registern gespeicherten Informationen).⁷⁰⁷

Wenn keiner dieser Fälle vorliegt und die Datenübermittlung nicht auf einen Angemessenheitsbeschluss oder geeignete Garantien gestützt werden kann, darf eine Übermittlung nur dann erfolgen, wenn sie nicht wiederholt erfolgt, eine begrenzte Zahl von betroffenen Personen betrifft und für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen der betroffenen Person nicht überwiegen.⁷⁰⁸ In diesen Fällen muss der Verantwortliche die Umstände der Datenübermittlung beurteilen und Garantien vorsehen. Darüber hinaus muss er die Aufsichtsbehörde und die betroffenen Personen von der Übermittlung und dem diese rechtfertigenden berechtigten Interesse in Kenntnis setzen.

Die Tatsache, dass Ausnahmen ein letztes Mittel für eine rechtmäßige Datenübermittlung darstellen⁷⁰⁹ (auf das lediglich in Ermangelung eines Angemessenheitsbeschlusses zurückgegriffen werden kann und sofern keine anderen Garantien bestehen) betont ihren Ausnahmecharakter und wird in den Erwägungsgründen der DSGVO noch zusätzlich hervorgehoben⁷¹⁰. Somit werden „Ausnahmen für bestimmte Fälle“ auf Grundlage einer Einwilligung toleriert oder wenn die Übermittlung gelegentlich erfolgt und im Rahmen eines Vertrags oder zur Geltendmachung von Rechtsansprüchen erforderlich ist⁷¹¹.

Nach Maßgabe der Leitlinien der Artikel-29-Datenschutzgruppe muss die Verwendung von Ausnahmen für bestimmte Fälle auf Ausnahmesituationen

⁷⁰⁷ DSGVO, Artikel 49.

⁷⁰⁸ a.a.O.

⁷⁰⁹ a.a.O., Artikel 49 Absatz 1.

⁷¹⁰ a.a.O., Artikel 49 Absatz 1 Buchstabe a, b und e, und Erwägungsgrund 113.

⁷¹¹ a.a.O.

in Einzelfällen beschränkt sein und kann weder für Datenübermittlungen in sehr großem Umfang noch für wiederholte Datenübermittlungen erfolgen.⁷¹² Auch der Europäische Datenschutzbeauftragte hob den Ausnahmecharakter der als Rechtsgrundlage für Datenübermittlungen im Rahmen der Verordnung (EG) Nr. 45/2001 hervor und wies darauf hin, dass diese Lösung „in [...] wenigen Fällen“ und „bei gelegentlichen Übermittlungen“ zum Einsatz kommen sollte.⁷¹³

Beispiel: Ein Unternehmen mit Hauptsitz in den Vereinigten Staaten, das ein Computer-Reservierungssystem anbietet, stellt ein Online-Buchungssystem für mehrere Fluggesellschaften, Hotels und Kreuzfahrtanbieter auf der ganzen Welt bereit und verarbeitet Daten von mehreren Dutzend Millionen Personen in der EU. Für die anfängliche Übermittlung von Daten an seine Server in den Vereinigten Staaten, beruft sich das Unternehmen auf die Ausnahme der Notwendigkeit für einen Vertragsabschluss als rechtmäßige Grundlage für die Datenübermittlung. Folglich liefert es keine anderen Garantien für die Übermittlung der aus Europa stammenden personenbezogenen Daten in die Vereinigten Staaten und deren anschließende Weiterübermittlung an Hotels auf der ganzen Welt (was bedeutet, dass das Unternehmen auch keine Garantien für die Weiterübermittlung der Daten liefert). Das Unternehmen hält die in der DSGVO dargelegten Anforderungen für rechtmäßige internationale Datenübermittlungen nicht ein, weil es sich auf eine Ausnahme als rechtmäßigen Grund für in sehr großem Umfang erfolgende Datenübermittlungen beruft.

Sofern kein Angemessenheitsbeschluss vorliegt, sind die EU oder ihre Mitgliedstaaten dazu befugt, der Übermittlung aus wichtigen Gründen des öffentlichen Interesses bestimmter Kategorien von personenbezogenen Daten an ein Drittland Grenzen zu setzen, ungeachtet dessen, ob andere Bedingungen für derartige Datenübermittlungen erfüllt sind oder nicht. Diese Grenzen sollten als Ausnahmen betrachtet werden und die Mitgliedstaaten sind zur Mitteilung der entsprechenden Bestimmungen an die Kommission verpflichtet.⁷¹⁴

712 Artikel-29-Datenschutzgruppe (2005), Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114, Brüssel, 25. November 2005.

713 Europäischer Datenschutzbeauftragter, *Die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU*, Positionspapier, Brüssel, 14. Juli 2014, S. 15.

714 Siehe DSGVO, Art. 49 Abs. 5.

Das **Recht des Europarates** erlaubt in den nachstehenden Fällen die Datenübermittlung an Hoheitsgebiete, die über keinen angemessenen Datenschutz verfügen:

- die betroffene Person hat ihre Einwilligung gegeben;
- die Interessen der betroffenen Person erfordern die Übermittlung;
- es bestehen überwiegende rechtmäßige Interessen, insbesondere wichtige öffentliche Interessen, die gesetzlich vorgesehen sind; und
- die Übermittlung stellt in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme dar.⁷¹⁵

7.3.4. Datenübermittlung auf Grundlage internationaler Abkommen

Die EU kann internationale Abkommen mit Drittländern schließen, die die Übermittlung von personenbezogenen Daten für bestimmte Zwecke regeln. Diese Abkommen müssen geeignete Garantien für die Gewährleistung des Schutzes der personenbezogenen Daten der betroffenen Personen enthalten. Internationale Abkommen werden von der DSGVO nicht berührt.⁷¹⁶

Auch die Mitgliedstaaten können völkerrechtliche Übereinkünfte mit Drittländern oder internationalen Organisationen schließen, die ein angemessenes Schutzniveau für die Grundrechte und Freiheiten der Personen umfassen, sofern sich diese Übereinkünfte nicht auf die Anwendung der DSGVO auswirken.

Eine ähnliche Bestimmung ist in Artikel 14 Absatz 3 Buchstabe a der Modernisierten Übereinkommens Nr. 108 enthalten.

Beispiele für internationale Abkommen, die die Übermittlung personenbezogener Daten beinhalten, sind die Abkommen über Fluggastdatensätze (PNR).

⁷¹⁵ Modernisiertes Übereinkommen Nr. 108, Artikel 14 Absatz 4.

⁷¹⁶ DSGVO, Erwägungsgrund 102.

Fluggastdatensätze

PNR-Daten werden von Fluggesellschaften während des Buchungsvorgangs erhoben und umfassen unter anderem Namen, Adressen, Angaben zur Kreditkarte und der Sitznummer von Fluggästen. Fluggesellschaften erheben diese Informationen auch für ihre eigenen gewerblichen Zwecke. Die EU hat mit bestimmten Drittländern (Australien, Kanada und den Vereinigten Staaten) Abkommen in Bezug auf die Übermittlung von PNR-Daten zur Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität geschlossen. Darüber hinaus nahm die Union im Jahr 2016 die als EU-PNR-Richtlinie bezeichnete Richtlinie (EU) 2016/681⁷¹⁷ an. Diese Richtlinie liefert den EU-Mitgliedstaaten einen Rechtsrahmen für die ebenfalls zur Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität erfolgende Übermittlung von PNR-Daten an die zuständigen Behörden in anderen Drittländern. Die Übermittlung von PNR-Daten an Behörden in Drittländern erfolgt für jeden Einzelfall und unterliegt einer individuellen Bewertung der Notwendigkeit der Übermittlung für die in der Richtlinie dargelegten Zwecke unter der Voraussetzung, dass die Grundrechte geachtet werden.

Was die PNR-Abkommen zwischen der EU und Drittländern betrifft, so wurde deren Vereinbarkeit mit den in der Charta der Grundrechte der EU verankerten Grundrechten auf Privatsphäre und Datenschutz angefochten. Als die EU im Anschluss an mit Kanada geführten Verhandlungen im Jahr 2014 ein Abkommen über die Übermittlung und Verarbeitung von PNR-Daten unterzeichnete, beschloss das Europäische Parlament, die Angelegenheit an den EuGH zu verweisen, der die Vereinbarkeit des Abkommens mit EU-Recht und insbesondere mit Artikel 7 und 8 der Charta bewerten sollte.

Beispiel: In seiner Stellungnahme über die Rechtmäßigkeit des EU-Kanada-PNR-Abkommens,⁷¹⁸ befand der EuGH, dass das geplante Abkommen in seiner gegenwärtigen Form mit den in der Charta anerkannten Grundrechten unvereinbar sei und daher nicht abgeschlossen werden könne. Da es die Verarbeitung personenbezogener Daten umfasste, stellte es einen

717 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, Abl. L 119 vom 4.5.2016.

718 EuGH, *Gutachten 1/15 des Gerichtshofs* [GK], 26. Juli 2017.

Eingriff in das durch Artikel 8 der Charta geschützte Recht auf Schutz personenbezogener Daten dar. Gleichzeitig stellt es auch eine Einschränkung des in Artikel 7 verankerten Rechts auf Achtung des Privatlebens dar, da die PNR-Daten zusammen betrachtet auf eine Weise angesammelt und analysiert werden können, die Reisegewohnheiten, Beziehungen zwischen verschiedenen Personen, Informationen über deren finanzielle Situation, ihre Ernährungsgewohnheiten oder ihren Gesundheitszustand offenbart und sich somit negativ auf ihr Privatleben auswirken kann.

Der Eingriff in die Grundrechte, der mit dem geplanten Abkommen erfolgen sollte, verfolgte ein dem Gemeinwohl dienendes Ziel, die in der öffentlichen Sicherheit und der Bekämpfung von Terrorismus und anderer grenzübergreifender schwerer Kriminalität bestand. Der EuGH rief jedoch in Erinnerung, dass ein Eingriff auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränkt sein muss, um gerechtfertigt zu sein. Im Anschluss an die Analyse der Bestimmungen des Abkommens befand der EuGH, dass das geplante Abkommen das Kriterium der „absoluten Notwendigkeit“ nicht erfülle. Um zu dieser Schlussfolgerung zu gelangen, berücksichtigte der EuGH unter anderem die nachstehenden Faktoren:

- Die Tatsache, dass das geplante Abkommen die Übermittlung sensibler Daten zur Folge hatte. Die nach Maßgabe des geplanten Abkommens erhobenen PNR-Daten könnten sensible Daten enthalten, wie Informationen, aus denen die rassische oder ethnische Herkunft, religiöse Überzeugungen oder der Gesundheitszustand der Fluggäste hervorgehen. Die Übermittlung und Verarbeitung sensibler Daten seitens der kanadischen Behörden könne eine Gefahr für den Grundsatz der Nichtdiskriminierung darstellen und folglich einer präzisen und fundierten Rechtfertigung bedürfen, die sich auf andere Gründe als die öffentliche Sicherheit und die Bekämpfung schwerer Kriminalität stützt. Dem geplanten Abkommen fehlt es an einer solchen Rechtfertigung.⁷¹⁹
- Die dauerhafte Speicherung der PNR-Daten sämtlicher Fluggäste über einen Zeitraum von fünf Jahren selbst nach ihrer Ausreise aus Kanada wurde ebenfalls als Überschreitung der Grenzen des absolut Notwendigen betrachtet. Der EuGH befand, dass es zulässig wäre, dass die kanadischen Behörden die Daten von Fluggästen speichern, in Bezug auf die es

719 a.a.O., Randnr. 165.

objektive Anhaltspunkte dafür gibt, dass sie selbst nach ihrer Ausreise aus Kanada eine Gefahr für die öffentliche Sicherheit darstellen können. Die Speicherung der personenbezogenen Daten *aller* Fluggäste, bezüglich derer es nicht einmal mittelbare Anhaltspunkte dafür gibt, dass sie eine Gefahr für die öffentliche Sicherheit darstellen, ist hingegen nicht gerechtfertigt.⁷²⁰

Der Beratende Ausschuss für das Übereinkommen 108 hat eine Stellungnahme zu den Datenschutz-Auswirkungen des PNR-Abkommen im Rahmen des Rechts des Europarates abgegeben.⁷²¹

Zahlungsverkehrsdaten

Das Unternehmen Society for Worldwide Interbank Financial Telecommunication (SWIFT) mit Sitz in Belgien, das der Auftragsverarbeiter für die meisten weltweiten Geldüberweisungen europäischer Banken ist, betrieb ein „Spiegelzentrum“ in den Vereinigten Staaten und wurde aufgefordert, Daten an das US-Finanzministerium für Zwecke der Terrorismusbekämpfung im Rahmen seines Programms zum Aufspüren der Finanzierung des Terrorismus weiterzugeben.⁷²²

Aus Sicht der EU bestand keine ausreichende Rechtsgrundlage für die Weitergabe dieser im Wesentlichen Staatsangehörige der EU betreffenden Daten, auf die in den Vereinigten Staaten nur Zugriff bestand, weil eines der Datenverarbeitungszentren von SWIFT in den Vereinigten Staaten lag.

2010 wurde ein Abkommen zwischen der EU und den Vereinigten Staaten abgeschlossen, das auch als SWIFT-Abkommen bekannt ist, und das die

720 a.a.O., Randnm. 204–207.

721 Europarat, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19. August 2016.

722 Siehe in diesem Zusammenhang Artikel-29-Datenschutzgruppe (2011), *Stellungnahme 14/2011 zu Fragen des Datenschutzes im Zusammenhang mit der Verhinderung von Geldwäsche und Terrorismusfinanzierung*, WP 186, Brüssel, 13. Juni 2011; Artikel-29-Datenschutzgruppe (2006), *Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, WP 128, Brüssel, 22. November 2006; belgische Datenschutzbehörde (Commission de la protection de la vie privée) (2008), „Kontroll- und Empfehlungsverfahren, eingeleitet gegen das Unternehmen SWIFT sarl“, Beschluss, 9. Dezember 2008.

erforderliche Rechtsgrundlage bieten und angemessene Datenschutzstandards gewährleisten soll.⁷²³

Nach diesem Abkommen werden von SWIFT gespeicherte Finanzdaten dem US-Finanzministerium für Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Terrorismus oder Terrorismusfinanzierung weiterhin zur Verfügung gestellt. Das US-Finanzministerium kann Finanzdaten bei SWIFT anfordern, sofern das Ersuchen:

- die Finanzdaten so klar wie möglich bezeichnet;
- den Bedarf an den Daten klar begründet;
- so restriktiv wie möglich formuliert ist, um die Menge der angeforderten Daten so klein wie möglich zu halten;
- keine Daten im Zusammenhang mit dem einheitlichen Euro-Zahlungsverkehrsraum (SEPA) anfordert.⁷²⁴

Europol erhält von jedem Ersuchen des US-Finanzministeriums eine Kopie und überprüft, ob den Grundsätzen des SWIFT-Abkommens Genüge getan wird oder nicht.⁷²⁵ Wenn die Grundsätze eingehalten werden, muss SWIFT die Finanzdaten unmittelbar an das US-Finanzministerium übermitteln. Das Ministerium muss die Finanzdaten in einem physisch sicheren Umfeld aufbewahren, wo nur Analysten des Terrorismus und seiner Finanzierung auf sie Zugriff haben, und die Finanzdaten dürfen nicht mit irgendeiner anderen Datenbank verknüpft werden. Im Allgemeinen sind von SWIFT erhaltene Finanzdaten spätestens fünf Jahre nach ihrem Erhalt zu löschen. Finanzdaten, die von besonderer Bedeutung für bestimmte Ermittlungen oder Strafverfolgungsmaßnahmen sind, dürfen so lange gespeichert werden, wie sie für diese Ermittlungen oder Strafverfolgungsmaßnahmen erforderlich sind.

723 Beschluss 2010/412/EU des Rates vom 13. Juli 2010 über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus, ABl. L 195 vom 27.7.2010, S. 3 und 4. Der Wortlaut des Abkommens ist diesem Beschluss beigefügt, ABl. L 195 vom 27.7.2010, S. 5–14.

724 a.a.O., Artikel 4 Absatz 2.

725 Die Gemeinsame Kontrollinstanz von Europol hat *Prüfungen der von Europol in diesem Bereich durchgeführten Maßnahmen* durchgeführt.

Das US-Finanzministerium darf Informationen aus den von SWIFT erhaltenen Daten an bestimmte Behörden in den Bereichen Strafverfolgung, öffentliche Sicherheit oder Terrorismusbekämpfung innerhalb oder außerhalb der Vereinigten Staaten ausschließlich für Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Terrorismus oder Terrorismusfinanzierung weitergeben. Ist von der Weitergabe von Finanzdaten ein Bürger eines EU-Mitgliedstaats oder eine Person mit Wohnsitz in einem solchen Land betroffen, bedarf die Weitergabe der Daten an die Behörden eines Drittlandes der vorherigen Zustimmung der zuständigen Behörden des betreffenden Mitgliedstaats. Ausnahmen sind möglich, wenn die Weitergabe der Daten für die Verhütung einer unmittelbar und ernsthaft drohenden Gefahr für die öffentliche Sicherheit wesentlich ist.

Unabhängige Aufsichtspersonen, einschließlich einer von der Europäischen Kommission ernannte Person, überwachen die Einhaltung der Grundsätze des SWIFT-Abkommens. Sie haben die Möglichkeit in Echtzeit und rückwirkend sämtliche Abfragen, die in Bezug auf die bereitgestellten Daten getätigt wurden durchzusehen, um weitere Informationen zur Rechtfertigung der Verknüpfung dieser Suchen mit dem Terrorismus anzufordern, und verfügen über die Befugnis zur Sperrung sämtlicher Suchabfragen, die unter Verstoß gegen die im Abkommen dargelegten Garantien durchgeführt wurden.

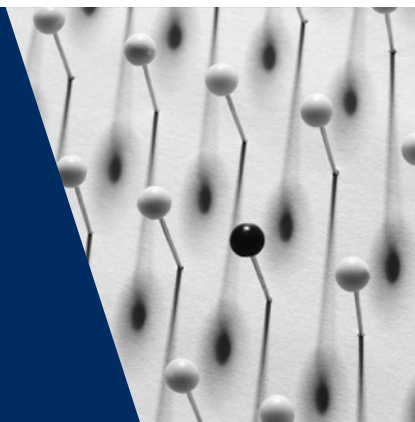
Betroffene Personen haben das Recht auf eine Bestätigung seitens der zuständigen EU-Aufsichtsbehörde, dass ihr Recht auf Schutz ihrer personenbezogenen Daten gewahrt wurde. Betroffene Personen haben ebenfalls das Recht auf Berichtigung, Löschung oder Sperrung aller ihrer durch das US-Finanzministerium im Rahmen des SWIFT-Abkommens erhobenen und gespeicherten Daten. Das Auskunftsrecht betroffener Personen kann allerdings gewissen gesetzlichen Einschränkungen unterliegen. Wird die Auskunft verweigert, muss die betroffene Person hierüber sowie über ihr Recht, bei Behörden und Gerichten in den Vereinigten Staaten Rechtsbehelf einzulegen, schriftlich unterrichtet werden.

Das SWIFT-Abkommen hat eine Laufzeit von fünf Jahren und sein erster Gültigkeitszeitraum lief im August 2015 aus. Danach verlängert es sich automatisch um jeweils ein Jahr, sofern nicht eine der Parteien der anderen mindestens sechs Monate im Voraus ihre Absicht mitteilt, das Abkommen nicht zu verlängern. Die automatische Verlängerung fand im August 2015, 2016 und 2017 statt und gewährleistet die Gültigkeit des SWIFT-Abkommens bis mindestens August 2018.⁷²⁶

⁷²⁶ a.a.O., Artikel 23 Absatz 2.

8

Datenschutz in den Bereichen Polizei und Strafjustiz



EU	Behandelte Themen	Europarat
Richtlinie (EU) 2016/680 (Datenschutzrichtlinie für Polizei und Strafjustiz)	Allgemein	Modernisiertes Übereinkommen Nr. 108
	Polizei	Polizei-Empfehlung Practical guide on the use of personal data in the police sector
	Überwachung	EGMR, <i>B.B. / Frankreich</i> , Nr. 5335/06, 2009 EGMR, <i>S. und Marper / Vereinigtes Königreich</i> [GK], Nrn. 30562/04 und 30566/04, 2008 EGMR, <i>Allan / Vereinigtes Königreich</i> , Nr. 48539/99, 2002 EGMR, <i>Malone / Vereinigtes Königreich</i> , Nr. 8691/79, 1984 EGMR, <i>Klass und andere / Deutschland</i> , Nr. 5029/71, 1978 EGMR, <i>Szabo und Vissy / Ungarn</i> , Nr. 37138/14, 2016 EGMR, <i>Vetter / Frankreich</i> , Nr. 59842/00, 2005
	Computerkriminalität	Cybercrime- Übereinkommen

EU	Behandelte Themen	Europarat
Sonstige spezifische Rechtsinstrumente		
Beschluss von Prüm	Für besondere Daten: Fingerabdrücke, DNA, Rowdytum, Fluggastdaten, Telekommunikationsdaten, usw.	Modernisiertes Übereinkommen Nr. 108, Artikel 6 Practical guide on the use of personal data in the police sector
Schwedische Initiative (Rahmenbeschluss 2006/960/JI des Rates)	Vereinfachung des Informations- und Nachrichtenaustauschs zwischen Strafverfolgungsbehörden	EGMR, <i>S. und Marper / Vereinigtes Königreich</i> [GK], Nrn. 30562/04 und 30566/04, 2008
Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, <i>Digital Rights Ireland und Kärntner Landesregierung und andere</i> [GK], 2014 EuGH, Verbundene Rechtssachen C-203/15 und C-698/15, <i>Tele2 Sverige und Home Department / Tom Watson und andere</i> [GK], 2016	Vorratsspeicherung personenbezogener Daten	EGMR, <i>B.B. / Frankreich</i> , Nr. 5335/06, 2009
Europol-Verordnung Eurojust-Beschluss	Durch spezielle Agenturen	Polizei-Empfehlung
Beschluss Schengen II VIS-Verordnung Eurodac-Verordnung ZIS-Beschluss	Durch spezielle gemeinsame Informationssysteme	Polizei-Empfehlung EGMR, <i>Dalea / Frankreich</i> , Nr. 964/07, 2010

Um die Interessen der Personen am Schutz ihrer Daten und die Interessen der Gesellschaft an der Datenerhebung für Zwecke der Kriminalitätsbekämpfung und zur Gewährleistung der nationalen und öffentlichen Sicherheit abzuwägen, haben der Europarat und die EU spezifische Rechtsinstrumente geschaffen. Der vorliegende Abschnitt liefert einen Überblick über das Datenschutzrecht des Europarates ([Abschnitt 8.1](#)) und das Datenschutzrecht der EU ([Abschnitt 8.2](#)) im Bereich Polizei und Strafjustiz.

8.1. Datenschutzrecht des Europarates im Bereich nationale Sicherheit, Polizei und Strafjustiz

Kernpunkte

- Das Modernisierte Übereinkommen Nr. 108 und die Polizei-Empfehlung des Europarates decken die Belange des Datenschutzes in allen Bereichen der Polizeiarbeit ab.
- Das Cybercrime-Übereinkommen (Budapester Übereinkommen) ist ein verbindliches internationales Rechtsinstrument, das sich mit Straftaten gegen elektronische Netzwerke und mit deren Hilfe begangenen Straftaten befasst. Es ist auch für die Untersuchung von Nicht-Cyber-Verbrechen, die elektronische Beweise erfordern, von Bedeutung.

Ein wichtiger Unterschied zwischen dem **Recht des Europarates** und dem EU-Recht besteht darin, dass das Recht des Europarates auch auf den nationalen Sicherheitsbereich Anwendung findet. Dies bedeutet, dass die Vertragsparteien selbst in Bezug auf Tätigkeiten im Zusammenhang mit der nationalen Sicherheit an Artikel 8 EMRK gebunden sind. Mehrere Urteile des EGMR betreffen staatliche Tätigkeiten in den sensiblen Bereichen des nationalen Sicherheitsrechts und der diesbezüglichen Praxis.⁷²⁷

In Bezug auf die Bereiche Polizei und Strafjustiz deckt das Modernisierte Übereinkommen Nr. 108 auf europäischer Ebene alle Bereiche der Verarbeitung personenbezogener Daten ab, und seine Bestimmungen sind dazu bestimmt, die Verarbeitung personenbezogener Daten im Allgemeinen zu regeln. Folglich findet das Modernisierte Übereinkommen Nr. 108 auf den Datenschutz in den Bereichen Polizei und Strafjustiz Anwendung. Die Verarbeitung von genetischen Daten, personenbezogenen Daten im Zusammenhang mit Straftaten, Strafverfahren, Verurteilungen und damit verbundenen Sicherheitsmaßnahmen, biometrischen Daten zur eindeutigen Identifizierung einer Person sowie sensiblen personenbezogenen Daten ist nur erlaubt, sofern geeignete Maßnahmen gegen die Risiken getroffen werden, die die Verarbeitung dieser Daten

⁷²⁷ Siehe beispielsweise EGMR, *Klass und andere / Deutschland*, Nr. 5029/71, 6. September 1978; EGMR, *Rotaru / Rumänien* [GK], Nr. 28341/95, 4. Mai 2000 und EGMR, *Szabó und Vissy / Ungarn*, Nr. 37138/14, 12. Januar 2016.

mit sich bringt für die Interessen, Rechte und Grundfreiheiten der betroffenen Person und insbesondere gegen die Gefahr der Diskriminierung.⁷²⁸

Die gesetzlichen Aufgaben von Polizei- und Strafjustizbehörden erfordern häufig eine Verarbeitung personenbezogener Daten, die für die betroffenen Personen schwerwiegende Konsequenzen haben kann. Die vom Europarat 1987 angenommene Polizei-Empfehlung bietet den Mitgliedstaaten des Europarates Orientierungshilfe in der Frage, wie sie die Grundsätze des Übereinkommens Nr. 108 im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Polizeibehörden umsetzen sollten.⁷²⁹ Die Empfehlung wurde durch einen praxisorientierten Leitfaden zur Nutzung personenbezogener Daten im Polizei-Bereich ergänzt, der vom Beratenden Ausschuss für das Übereinkommen 108 angenommen wurde.⁷³⁰

Beispiel: In der Rechtssache *D.L. gegen Bulgarien*⁷³¹ brachte das Sozialamt die Beschwerdeführerin infolge einer Gerichtsentscheidung in einer sicheren pädagogischen Einrichtung unter. Der gesamte schriftliche Austausch und sämtliche Telefongespräche unterlagen einer pauschalen und unterschiedslosen Überwachung seitens der Einrichtung. Der EGMR befand, dass eine Verletzung von Artikel 8 vorlag, da die besagte Maßnahme in einer demokratischen Gesellschaft nicht notwendig sei. Der Gerichtshof befand, dass alles dafür getan werden müsse, damit Minderjährige, die in einer Einrichtung untergebracht sind, ausreichende Kontakte zur Außenwelt haben, da dies integraler Bestandteil ihres Rechts sei, würdevoll behandelt zu werden, und unverzichtbar, um sie auf ihre Rückkehr in die Gesellschaft vorzubereiten. Dies fände auf Besuche ebenso Anwendung wie auf den schriftlichen Austausch oder Telefongespräche. Überdies wurde bei der Überwachung nicht unterschieden, ob es sich um den Austausch mit Familienmitgliedern oder um den Austausch mit Nichtregierungsorganisationen zur Vertretung von Kinderrechten oder Anwälten handelte. Darüber hinaus war die Überwachungsentscheidung nicht mit einer individuellen Analyse der Risiken in jedem Einzelfall begründet.

728 Modernisiertes Übereinkommen Nr. 108, Artikel 6.

729 Europarat, Ministerkomitee (1987), Empfehlung Rec(87)15 an die Mitgliedstaaten über die Nutzung personenbezogener Daten im Polizeibereich, 17. September 1987.

730 Europarat, Ausschuss für das Übereinkommen Nr. 108 (2018), *Practical Guide on the use of personal data in the police sector*, T-PD(2018)1.

731 EGMR, *D.L. / Bulgarien*, Nr. 7472/14, 19. Mai 2016.

Beispiel: In der Rechtssache *Dragojević gegen Kroatien*⁷³² wurde der Beschwerdeführer verdächtigt, in den Drogenhandel verwickelt zu sein. Er wurde verurteilt, nachdem ein Ermittlungsrichter den Einsatz geheimer Überwachungsmaßnahmen zum Abhören der Telefonanrufe des Beschwerdeführers genehmigt hatte. Der EGMR befand, dass diese Maßnahme, gegen die Beschwerde eingereicht wurde, einen Eingriff in das Recht auf Achtung des Privatlebens und der Korrespondenz darstelle. Die seitens des Ermittlungsrichters erteilte Genehmigung stütze sich lediglich auf die Aussage der Strafverfolgungsbehörde, wonach „die Ermittlungen auf keine andere Weise durchgeführt werden könnten“. Der EGMR stellte überdies fest, dass die Strafgerichte nur den Einsatz von Überwachungsmaßnahmen bewertet hatten und die Regierung es unterließ, Informationen über die verfügbaren Rechtsbehelfe vorzubringen. Folglich habe eine Verletzung von Artikel 8 stattgefunden.

8.1.1. Die Polizei-Empfehlung

Der EGMR hat wiederholt festgestellt, dass die Speicherung und Aufbewahrung personenbezogener Daten durch Polizei- oder nationale Sicherheitsbehörden einen Eingriff in Artikel 8 Absatz 1 EMRK darstellen. In vielen Urteilen des EGMR geht es um die Rechtfertigung solcher Eingriffe.⁷³³

Beispiel: Beim Beschwerdeführer in der Rechtssache *B.B. gegen Frankreich*⁷³⁴ handelte es sich um eine Person in einer Vertrauensposition, die aufgrund der Beteiligung an Sexualverbrechen an 15-jährigen Jugendlichen verurteilt worden war. Im Jahr 2000 hatte er seine Freiheitsstrafe verbüßt. Ein Jahr später ersuchte er um die Streichung der Angabe seiner Verurteilung aus seinem Strafregister, doch sein Ersuchen wurde abgewiesen. Im Jahr 2004 führte ein französisches Gesetz eine nationale Justizdatenbank von Sexualstraftätern ein und der Beschwerdeführer wurde über seine Erfassung in dieser Datenbank in Kenntnis gesetzt. Der EuGH befand, dass die Erfassung eines verurteilten Sexualstraftäters in einer nationalen Justizdatenbank unter

⁷³² EGMR, *Dragojević / Kroatien*, Nr. 68955/11, 15. Januar 2015.

⁷³³ Siehe zum Beispiel EGMR, *Leander / Schweden*, Nr. 9248/81, 26. März 1987; EGMR, *M.M. / Vereinigtes Königreich*, Nr. 24029/07, 13. November 2012; EGMR, *M.K. / Frankreich*, Nr. 19522/09, 18. April 2013 oder EGMR, *Aycaguer / Frankreich*, Nr. 8806/12, 22. Juni 2017.

⁷³⁴ EGMR, *B.B. / Frankreich*, Nr. 5335/06, 17. Dezember 2009.

Artikel 8 EMRK fällt. In Anbetracht der Tatsache allerdings, dass ausreichende Schutzgarantien angewandt worden waren, wie das Recht der betroffenen Person auf Löschung der Daten, die befristete Datenspeicherung und der eingeschränkte Zugriff auf diese Daten, sei in diesem Fall eine sorgfältige Abwägung der einander gegenüberstehenden privaten und öffentlichen Interessen vorgenommen worden. Der Gerichtshof befand, dass keine Verletzung von Artikel 8 EMRK vorlag.

Beispiel: In der Rechtssache *S. und Marper gegen Vereinigtes Königreich*⁷³⁵ waren beide Beschwerdeführer bestimmter Straftaten angeklagt, jedoch deswegen nicht verurteilt worden. Dessen ungeachtet bewahrte die Polizei ihre Fingerabdrücke, Zellproben und DNA-Profile weiter auf. Die unbefristete Speicherung biometrischer Daten war gesetzlich zulässig, wenn eine Person einer Straftat verdächtigt wurde, auch wenn der Beschuldigte später freigesprochen oder entlastet wurde. Der EGMR urteilte, dass die pauschale und unterschiedslose Speicherung personenbezogener Daten, die nicht befristet war, und bei der freigesprochene Personen nur begrenzte Möglichkeiten hatten, eine Löschung zu beantragen, einen unverhältnismäßigen Eingriff in das Recht der Beschwerdeführer auf Achtung des Privatlebens darstelle. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Ein wesentliches Thema im Zusammenhang mit elektronischer Kommunikation sind durch Behörden erfolgende Eingriffe in die Rechte auf Privatsphäre und Datenschutz. Mittel zur Überwachung oder zum Abfangen von Kommunikation wie beispielsweise Abhörgeräte sind nur zulässig, wenn sie gesetzlich vorgesehen sind und wenn sie in einer demokratischen Gesellschaft notwendig sind für:

- den Schutz der Sicherheit des Staates;
- die öffentliche Ordnung;
- das wirtschaftliche Wohl des Landes;
- die Verhütung von Straftaten; oder
- den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer.

⁷³⁵ EGMR, *S. und Marper / Vereinigtes Königreich* [GK], Nrn. 30562/04 und 30566/04, 4. Dezember 2008, Randnrn. 119 und 125.

In zahlreichen anderen Urteilen des EGMR geht es um die Rechtfertigung des Eingriffs in das Recht auf Privatsphäre durch Überwachung.

Beispiel: In der Rechtssache *Allan gegen Vereinigtes Königreich*⁷³⁶ waren Privatgespräche eines Häftlings mit einem Freund im Besuchsbereich des Gefängnisses und mit einem Mitangeklagten in einer Zelle von den Behörden heimlich aufgezeichnet worden. Der EGMR war der Auffassung, dass der Einsatz von Audio- und Videoüberwachungsgeräten in der Zelle des Beschwerdeführers, im Besuchsbereich des Gefängnisses und bei einem Mithäftling einen Eingriff in das Recht des Beschwerdeführers auf Achtung des Privatlebens darstelle. Da der Einsatz verdeckter Aufzeichnungsgeräte durch die Polizei seinerzeit gesetzlich nicht geregelt war, sei dieser Eingriff rechtswidrig gewesen. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Beispiel: In der Rechtssache *Roman Zakharov gegen Russland*⁷³⁷ leitete der Beschwerdeführer gerichtliche Schritte gegen drei Betreiber von Mobilfunknetzen ein. Er argumentierte, dass sein Recht auf die Privatheit seiner Telefonkommunikation verletzt wurde, da die Mobilfunkbetreiber Geräte installiert hätten, die es dem Geheimdienst erlaubten, seine Telefongespräche ohne vorhergehende richterliche Genehmigung abzuhören. Der EGMR befand, dass die innerstaatlichen Rechtsvorschriften für das Abhören von Kommunikation keine angemessenen und wirksamen Garantien gegen Willkür und die Gefahr eines Missbrauchs vorsahen. Insbesondere sahen die nationalen Rechtsvorschriften keine Löschung der gespeicherten Daten nach Erreichung der Zwecke, für die die Speicherung durchgeführt wurde, vor. Zudem war trotz des Erfordernisses einer richterlichen Genehmigung der Umfang der richterlichen Überprüfung beschränkt.

Beispiel: In der Rechtssache *Szabó und Vissy gegen Ungarn*⁷³⁸ behaupteten die Beschwerdeführer, dass das ungarische Recht gegen Artikel 8 EMRK verstoße, da es nicht ausreichend detailliert und präzise sei. Darüber hinaus wurde argumentiert, dass das ungarische Recht keine ausreichenden Garantien gegen Missbrauch und Willkür enthalte. Der EGMR befand, dass

736 EGMR, *Allan / Vereinigtes Königreich*, Nr. 48539/99, 5. November 2002.

737 EGMR, *Roman Zakharov / Russland* [GK], Nr. 47143/06, 4. Dezember 2015.

738 EGMR, *Szabó und Vissy / Ungarn*, Nr. 37138/14, 12. Januar 2016.

nach ungarischem Recht die Überwachung keiner richterlichen Genehmigung bedarf. Zudem wies der Gerichtshof darauf hin, dass die Überwachung der Genehmigung des Justizministers bedarf, was ein höchst politischer Vorgang sei, der ungeeignet sei, die erforderliche Beurteilung der „unbedingten Notwendigkeit“ sicherzustellen. Überdies gewährleiste das innerstaatliche Recht keine gerichtliche Nachprüfung, da die Verständigung der betroffenen Personen nicht vorgesehen sei. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Da Verarbeitungen von Daten durch Polizeibehörden erhebliche Auswirkungen auf die betroffenen Personen haben können, sind detaillierte Datenschutzvorschriften für die Verarbeitung personenbezogener Daten in diesem Bereich besonders notwendig. Die Polizei-Empfehlung des Europarates nahm sich diesem Thema an und formulierte Leitlinien zu folgenden Fragen: Wie sollen Daten für die polizeiliche Arbeit erhoben werden; wie sollen Dateien in diesem Bereich gespeichert werden; wer soll Zugriff auf diese Daten haben und unter welchen Bedingungen dürfen Daten an ausländische Polizeibehörden übermittelt werden; wie können betroffene Personen ihre Datenschutzrechte ausüben, und wie ist die Kontrolle durch unabhängige Behörden durchzuführen. Ferner geht es darin um die Verpflichtung, für eine angemessene Datensicherheit zu sorgen.

Die Empfehlung sieht keine unbefristete, unterschiedslose Erhebung von Daten durch Polizeibehörden vor. Sie begrenzt die Erhebung personenbezogener Daten durch Polizeibehörden auf das für die Abwehr einer echten Gefahr oder die Verfolgung einer konkreten Straftat erforderliche Maß. Eine weitergehende Erhebung von Daten muss sich auf entsprechende einzelstaatliche Rechtsvorschriften stützen. Die Verarbeitung sensibler Daten sollte auf das im Rahmen einer bestimmten Ermittlung unbedingt Erforderliche beschränkt sein.

Werden personenbezogene Daten ohne Wissen der betroffenen Person erhoben, ist die betroffene Person über die Datenerhebung zu informieren, sobald diese Information die Ermittlungen nicht länger beeinträchtigt. Für die Erhebung von Daten durch technische Überwachung oder andere automatisierte Mittel muss es eine spezifische Rechtsgrundlage geben.

Beispiel: In der Rechtssache *Versini-Campinchi und Crasnianski gegen Frankreich*⁷³⁹ führte die Beschwerdeführerin, eine Rechtsanwältin, ein Telefonat mit einem Mandanten, dessen Telefonleitung auf Antrag eines Ermittlungsrichters abgehört wurde. Die Niederschrift des Telefonats zeigte, dass sie dabei Informationen offengelegt hatte, die unter die Vertraulichkeit der anwaltlichen Korrespondenz fielen. Der Staatsanwalt übermittelte diese Informationen an die Anwaltskammer, die eine Geldbuße gegen die Beschwerdeführerin verhängte. Der EGMR erkannte das Vorliegen eines Eingriffs in das Recht auf Achtung des Privatlebens und der Korrespondenz an, und dies nicht nur in Bezug auf die Person, deren Telefon angezapft wurde, sondern auch in Bezug auf die Beschwerdeführerin, deren Kommunikation abgehört und niedergeschrieben wurde. Der Eingriff erfolgte in Übereinstimmung mit dem Gesetz und verfolgte das rechtmäßige Ziel der Aufrechterhaltung der Ordnung. Im Rahmen des gegen die Beschwerdeführerin eingeleiteten Disziplinarverfahrens wurde die Rechtmäßigkeit der Übermittlung der Niederschrift der Aufzeichnungen der Telefonüberwachung überprüft. Obgleich es ihr nicht gelang, die Aufhebung der Niederschrift des Telefonats zu erwirken, befand der EGMR, dass eine wirksame Kontrolle stattgefunden habe, durch die der beanstandete Eingriff auf das in einer demokratischen Gesellschaft notwendige Maß beschränkt werden konnte. Der EGMR stellte fest, dass das Argument, wonach die Möglichkeit der auf Grundlage der Niederschrift erfolgenden Einleitung eines Strafverfahrens gegen einen Rechtsanwalt eine abschreckende Wirkung auf die Freiheit der Kommunikation zwischen einem Rechtsanwalt und seinem Mandanten und folglich auf die Verteidigungsrechte des Mandanten haben könne, nicht überzeuge wenn die Offenlegung seitens der Rechtsanwältin selbst erfolgte und unrechtmäßiges Verhalten bezeichnend sein könne. Folglich wurde kein Verstoß gegen Artikel 8 festgestellt.

Die Polizei-Empfehlung des Europarates sieht vor, dass bei der Speicherung personenbezogener Daten klar zu unterscheiden ist zwischen administrativen und polizeilichen Daten, personenbezogenen Daten verschiedener Arten betroffener Personen, wie Beschuldigten, verurteilten Personen, Opfern und Zeugen, Daten, die auf harten Fakten beruhen, und Daten, die auf Verdachtsmomenten oder Spekulation beruhen.

Der Zweck, für den polizeiliche Daten verwendet werden dürfen, muss eng begrenzt sein. Dies hat Konsequenzen für die Weitergabe polizeilicher Daten

⁷³⁹ EGMR, *Versini-Campinchi und Crasnianski / Frankreich*, Nr. 49176/11, 16. Juni 2016.

an Dritte: für die Übermittlung oder Offenlegung solcher Daten innerhalb des Polizeibereichs sollte entscheidend sein, ob ein berechtigtes Interesse an der Weitergabe der Daten besteht oder nicht. Eine Übermittlung oder Offenlegung solcher Daten an Empfänger außerhalb des Polizeibereichs sollte nur erlaubt sein, wenn eine eindeutige gesetzliche Verpflichtung oder Befugnis vorliegt.

Beispiel: In der Rechtssache *Karabeyoğlu gegen Türkei*⁷⁴⁰ wurden die Telefonleitungen des Beschwerdeführers, eines Richters, im Rahmen einer strafrechtlichen Ermittlung über eine illegale Organisation zu der er im Verdacht stand, zu gehören, oder ihr Hilfe und Unterstützung bereitzustellen, überwacht. Im Anschluss an die Einstellungsentscheidung vernichtete der für die strafrechtliche Ermittlung zuständige Staatsanwalt die betreffenden Aufzeichnungen. Eine Kopie dieser Aufzeichnungen war jedoch im Besitz der gerichtlichen Ermittler verblieben, die das entsprechende Material in der Folge im Zusammenhang mit den Ermittlungen im Rahmen eines Disziplinarverfahrens gegen den Beschwerdeführer verwendeten. Der EGMR stellte einen Verstoß gegen die einschlägigen Gesetze fest, da die Informationen für andere Zwecke verwendet wurden als die, für die sie eingeholt wurden, und nicht innerhalb der gesetzlich vorgesehenen Frist vernichtet worden waren. Der Eingriff in das Recht des Beschwerdeführers auf Achtung seines Privatlebens verstieß im Hinblick auf das gegen ihn eingeleitete Disziplinarverfahren gegen das Gesetz.

Internationale Übermittlungen oder Weitergaben sollten auf ausländische Polizeibehörden beschränkt sein und sich auf spezielle Rechtsvorschriften und möglicherweise internationale Abkommen stützen, sofern sie nicht für die Abwehr ernsthafter und unmittelbarer Gefahr erforderlich sind.

Damit die Datenverarbeitung durch die Polizei im Einklang mit dem innerstaatlichen Datenschutzrecht steht, ist sie einer unabhängigen Kontrolle zu unterziehen. Betroffene Personen müssen alle im Modernisierten Übereinkommen Nr. 108 aufgeführten Auskunftsrechte wahrnehmen können. Wurden die Auskunftsrechte der betroffenen Person gemäß Artikel 9 des Übereinkommens Nr. 108 im Interesse wirksamer polizeilicher Ermittlungen und im Interesse der Strafvollstreckung eingeschränkt, muss die betroffene Person nach innerstaatlichem Recht die Möglichkeit haben, bei der nationalen Datenschutzaufsichtsbehörde oder einer anderen unabhängigen Stelle Rechtsbehelf einzulegen.

⁷⁴⁰ EGMR, *Karabeyoğlu / Türkei*, Nr. 30083/10, 7. Juni 2016.

8.1.2. Das Budapester Übereinkommen über Computerkriminalität

Da kriminelle Handlungen zunehmend elektronische Datenverarbeitungssysteme nutzen und diese betreffen, sind neue strafrechtliche Bestimmungen erforderlich, um dieser Herausforderung begegnen zu können. Der Europarat hat daher ein internationales Rechtsinstrument angenommen, das Übereinkommen über Computerkriminalität – auch bekannt als das Budapester Übereinkommen –, das sich mit Straftaten gegen und mit Hilfe elektronischer Netze befasst.⁷⁴¹ Diesem Übereinkommen können auch Nicht-Mitglieder des Europarates beitreten. Anfang 2018 waren 14 nicht dem Europarat angehörende Staaten⁷⁴² Vertragsparteien des Übereinkommens und sieben weitere Nicht-Mitglieder waren zum Beitritt eingeladen worden.

Das Übereinkommen über Computerkriminalität bleibt der einflussreichste internationale Vertrag, der sich mit Gesetzesverstößen im Internet oder anderen Datenleitungen befasst. Es verpflichtet die Vertragsparteien, ihre strafrechtlichen Vorschriften gegen Hacking und andere Sicherheitsübergreife einschließlich Verstöße gegen das Urheberrecht, computergestützten Betrug, Kinderpornografie und andere illegale Cyberaktivitäten zu überarbeiten und zu harmonisieren. Das Übereinkommen sieht auch die verfahrensrechtlichen Befugnisse für die Durchsuchung von Computernetzen und das Abfangen von Kommunikation bei der Bekämpfung von Computerkriminalität vor. Schließlich ermöglicht es eine wirksame internationale Zusammenarbeit. Ein Zusatzprotokoll zum Übereinkommen befasst sich mit der strafrechtlichen Verfolgung rassistischer und fremdenfeindlicher Propaganda in Computernetzwerken.

Das Übereinkommen ist zwar kein Instrument, das auf die Förderung des Datenschutzes abzielt, doch kriminalisiert es Tätigkeiten, die möglicherweise das Recht der betroffenen Person auf Schutz ihrer Daten verletzen. Überdies verpflichtet es die Vertragsparteien, gesetzgeberische Maßnahmen zu treffen, um ihren nationalen Behörden die Erhebung von Verkehrs- und Inhaltsdaten zu ermöglichen.⁷⁴³ Weiter verpflichtet es die Vertragsparteien, bei der Umset-

⁷⁴¹ Europarat, Ministerkomitee (2001), Übereinkommen über Computerkriminalität, SEV Nr. 185, Budapest, 23. November 2001, in Kraft getreten am 1. Juli 2004.

⁷⁴² Australien, Kanada, Chile, die Dominikanische Republik, Israel, Japan, Kolumbien, Mauritius, Panama, Senegal, Sri Lanka, Tonga, Tunesien und die Vereinigten Staaten. Siehe [Unterschriften und Ratifikationsstand des Vertrags 185, Datum Juli 2017](#).

⁷⁴³ Europarat, Ministerkomitee (2001), Übereinkommen über Computerkriminalität, SEV Nr. 185, Budapest, 23. November 2001, Artikel 20 und 21.

zung des Übereinkommens einen angemessenen Schutz der Menschenrechte und Freiheiten einschließlich der unter der EMRK garantierten Rechte, wie des Rechts auf Datenschutz, vorzusehen.⁷⁴⁴ Um dem Budapester Übereinkommen über Computerkriminalität beizutreten zu können, sind die Vertragsstaaten nicht dazu verpflichtet, auch dem Übereinkommen Nr. 108 beizutreten.

8.2. EU-Datenschutzrecht im Bereich Polizei und Strafjustiz

Kernpunkte

- Innerhalb der EU ist der Datenschutz in den Bereichen Polizei und Strafjustiz sowohl im Zusammenhang mit der nationalen als auch im Zusammenhang mit der grenzüberschreitenden Datenverarbeitung von Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten und EU-Akteure geregelt.
- Auf Ebene der Mitgliedstaaten ist die Datenschutzrichtlinie für Polizei und Strafjustiz in innerstaatliches Recht umzusetzen.
- Spezifische Rechtsinstrumente regeln den Datenschutz im Bereich der grenzüberschreitenden Zusammenarbeit von Polizei und Strafverfolgung, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität.
- Spezielle Datenschutzvorschriften gibt es für das Europäische Polizeiamt (Europol), die Europäische Stelle für justizielle Zusammenarbeit (Eurojust) und die neu errichtete Europäische Staatsanwaltschaft, bei denen es sich um EU-Einrichtungen handelt, die bei der grenzüberschreitenden Strafverfolgung Unterstützung leisten und sie fördern.
- Spezielle Datenschutzvorschriften gibt es auch für die gemeinsamen Informationssysteme, die auf EU-Ebene für den grenzüberschreitenden Informationsaustausch zwischen den zuständigen Polizei- und Justizbehörden eingerichtet wurden. Wichtige Beispiele hierfür sind das Schengener Informationssystem der zweiten Generation (SIS II), das Visa-Informationssystem (VIS) und Eurodac, eine zentrale Datenbank, in der Fingerabdrücke von Drittstaatsangehörigen und Staatenlosen gespeichert sind, die in einem der EU-Mitgliedstaaten Asyl beantragt haben.
- Die EU ist gerade dabei, die oben dargelegten Datenschutzbestimmungen zu aktualisieren, damit diese mit den Bestimmungen der Datenschutzrichtlinie für Polizei und Strafjustiz übereinstimmen.

⁷⁴⁴ a.a.O., Artikel 15 Absatz 1.

8.2.1. Datenschutzrichtlinie für Polizei- und Strafverfolgungsbehörden

Die Richtlinie 2016/680/EU 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 (die Datenschutzrichtlinie für Polizei und Strafjustiz)⁷⁴⁵ zielt auf den Schutz personenbezogener Daten ab, die zu den nachstehenden Strafjustizzwecken erhoben und verarbeitet werden:

- Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;
- Strafvollstreckung; und
- in Fällen, in denen die Polizei oder andere Strafverfolgungsbehörden tätig sind, um das Recht zu wahren und zum Schutz vor und zur Vorbeugung von Bedrohungen der öffentlichen Sicherheit und der Grundrechte, die eine Straftat darstellen könnten.

Die Datenschutzrichtlinie für Polizei und Strafjustiz schützt die personenbezogenen Daten verschiedener Personengruppen, die in Strafverfahren verwickelt sind, wie Zeugen, Informanten, Opfern, Beschuldigten und an der Straftat beteiligten. Polizei- und Strafverfolgungsbehörden müssen die Vorgaben der Richtlinie innerhalb des persönlichen und sachlichen Geltungsbereichs der Richtlinie einhalten, wenn sie personenbezogene Daten zu Strafverfolgungszwecken verarbeiten.⁷⁴⁶

Unter bestimmten Voraussetzungen ist jedoch auch die Verwendung der Daten für einen anderen Zweck zulässig. Die Verarbeitung von Daten zu einem anderen Strafverfolgungszweck als dem, für den die Daten erhoben wurden, ist nur

⁷⁴⁵ Richtlinie 2016/680/EU 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 4.5.2016, S. 89 (Datenschutzrichtlinie für Polizei und Strafjustiz).

⁷⁴⁶ Datenschutzrichtlinie für Polizei und Strafjustiz, Artikel 2 Absatz 1.

erlaubt, sofern dies nach nationalem Recht oder EU-Recht gesetzlich vorgesehen, erforderlich und verhältnismäßig ist.⁷⁴⁷ In Bezug auf andere Zwecke gelten die (sonstigen) Vorgaben der DSGVO. Die Protokollierung und Dokumentation des Datenaustauschs zählt zu den ausdrücklich den Verantwortlichen zugewiesenen Aufgaben, um im Falle von Beschwerden so weit wie möglich die Identifizierung der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers solcher personenbezogenen Daten festzustellen.

Bei den im Bereich Polizei und Strafjustiz tätigen zuständigen Stellen handelt es sich um staatliche Stellen oder um Stellen, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;⁷⁴⁸ wie beispielsweise privat betriebene Strafvollzugsanstalten.⁷⁴⁹ Der Geltungsbereich der Richtlinie erstreckt sich sowohl auf die innerstaatliche und grenzüberschreitende Datenverarbeitung zwischen den Polizei- und Justizbehörden der Mitgliedstaaten als auch auf die internationale Datenübermittlung an Drittländer oder internationale Organisationen.⁷⁵⁰ Er erstreckt sich nicht auf die Landesverteidigung und die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der EU.⁷⁵¹

Die Richtlinie stützt sich weitgehend auf die in der DSGVO enthaltenen Grundsätze und Definitionen unter Berücksichtigung der Besonderheiten von Polizei und Strafjustiz. Die Überwachung kann seitens derselben Behörden der Mitgliedstaaten erfolgen wie auch im Rahmen der DSGVO. Die Benennung von Datenschutzbeauftragten und die Durchführung von Datenschutz-Folgenabschätzungen wurden als neue Pflichten für Polizei- und

747 a.a.O., Artikel 4 Absatz 2.

748 a.a.O., Artikel 3 Absatz 7.

749 Europäische Kommission (2016), Mitteilung der Kommission an das Europäische Parlament gemäß Artikel 294 Absatz 6 des Vertrags über die Arbeitsweise der Europäischen Union betreffend den Standpunkt des Rates im Hinblick auf den Erlass einer Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, COM(2016) 213 final, Brüssel, 11. April 2016.

750 Datenschutzrichtlinie für Polizei und Strafjustiz, Kapitel V.

751 a.a.O., Artikel 2 Absatz 3.

Strafverfolgungsbehörden in die Richtlinie aufgenommen.⁷⁵² Wenngleich diese Konzepte von der DSGVO inspiriert sind, stellt die Richtlinie auf die Besonderheiten der Polizei- und Strafverfolgungsbehörden ab. Im Vergleich zu der in der Verordnung geregelten Datenverarbeitung zu gewerblichen Zwecken kann die Datenverarbeitung zu Sicherheitszwecken ein gewisses Maß an Flexibilität erfordern. Wenn der betroffenen Person zum Beispiel das gleiche Schutzniveau in Bezug auf das Recht auf Information, Zugang zu oder Löschung ihrer personenbezogenen Daten gemäß der DSGVO gewährt wird, könnte dies bedeuten, dass zu Strafverfolgungszwecken durchgeführte Überwachungsaktionen ihren Zweck zur Strafverfolgung nicht erfüllen können. Daher ist der Grundsatz der Transparenz nicht in der Richtlinie enthalten. Ebenso sind die Grundsätze der Datenminimierung und der Zweckbindung, die erfordern, dass die personenbezogenen Daten auf das für die Verarbeitungszwecke notwendige Maß beschränkt sind und für festgelegte und eindeutige Zwecke verarbeitet werden, bei der Datenverarbeitung zu Sicherheitszwecken ebenfalls flexibel anzuwenden. Die seitens der zuständigen Behörden für einen bestimmten Fall erhobenen und gespeicherten Informationen können bei der Aufklärung künftig auftretender Fälle äußerst hilfreich sein.

Grundsätze in Bezug auf die Verarbeitung

Die Datenschutzrichtlinie für Polizei und Strafjustiz enthält einige elementare Garantien in Bezug auf die Verwendung personenbezogener Daten. Sie erläutert auch die für die Verarbeitung dieser Daten geltenden Grundsätze. Die Mitgliedstaaten müssen gewährleisten, dass personenbezogene Daten

- auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden;
- für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden;
- dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind;
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene

⁷⁵² a.a.O., Artikel 32 bzw. Artikel 27.

Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;

- nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht;
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.⁷⁵³

Nach Maßgabe der Richtlinie ist die Verarbeitung nur soweit rechtmäßig als sie für die Erfüllung der entsprechenden Aufgabe erforderlich ist. Überdies sollte die Verarbeitung seitens einer zuständigen Behörde unter Verfolgung der in der Richtlinie dargelegten Ziele und auf Grundlage des EU-Rechts oder des nationalen Rechts erfolgen.⁷⁵⁴ Die Daten dürfen nicht länger als nötig gespeichert werden und sind danach zu löschen oder innerhalb bestimmter Fristen regelmäßig zu überprüfen. Die Daten dürfen nur seitens einer zuständigen Behörde und für den Zweck verwendet werden, für den sie erhoben, übermittelt oder bereitgestellt wurden.

Rechte der betroffenen Person

Die Richtlinie legt auch die Rechte der betroffenen Person dar. Dazu gehören u. a.:

- Das Recht auf Unterrichtung. Die Mitgliedstaaten müssen den Verantwortlichen dazu verpflichten, der betroffenen Person die nachstehenden Informationen bereitzustellen: 1) den Namen und die Kontaktdaten des Verantwortlichen, 2) die Kontaktdaten des Datenschutzbeauftragten, 3) die Zwecke der beabsichtigten Verarbeitung, 4) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten und 5) das Bestehen eines Rechts auf Auskunft, Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung der Daten.⁷⁵⁵ Zusätzlich zu diesen allgemeinen

⁷⁵³ a.a.O., Artikel 4 Absatz 1.

⁷⁵⁴ a.a.O., Artikel 8.

⁷⁵⁵ a.a.O., Artikel 13 Absatz 1.

Informationen sieht die Richtlinie vor, dass Verantwortliche den betroffenen Personen in besonderen Fällen Informationen über die Rechtsgrundlage der Verarbeitung und die Speicherdauer der Daten erteilen, um diesen die Ausübung ihrer Rechte zu ermöglichen. Sofern die personenbezogenen Daten an andere Empfänger einschließlich Drittländer oder internationale Organisationen übermittelt werden, müssen die betroffenen Personen über die Kategorien dieser Empfänger unterrichtet werden. Schließlich müssen die Verantwortlichen entsprechend den spezifischen Umständen weitere Informationen zur Verfügung stellen – beispielsweise für den Fall, dass personenbezogene Daten im Zuge einer verdeckten Überwachung erhoben wurden, d. h. ohne Wissen der betroffenen Person. Dies gewährleistet der betroffenen Person eine Verarbeitung nach Treu und Glauben.⁷⁵⁶

- Das Auskunftsrecht über personenbezogene Daten. Die Mitgliedstaaten müssen gewährleisten, dass die betroffene Person das Recht hat, zu erfahren, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so sollte die betroffene Person Auskunft zu bestimmten Informationen wie beispielsweise zu den Kategorien der verarbeiteten Daten erhalten.⁷⁵⁷ Dieses Recht kann jedoch eingeschränkt werden, um beispielsweise die Ermittlungen nicht zu behindern und die Strafverfolgung nicht zu beeinflussen, oder zum Schutz der öffentlichen Sicherheit und der Rechte und Freiheiten anderer.⁷⁵⁸
- Das Recht auf die Berichtigung personenbezogener Daten. Die Mitgliedstaaten sind verpflichtet, zu gewährleisten, dass eine betroffene Person unverzüglich die Berichtigung unrichtiger personenbezogener Daten erwirken kann. Darüber hinaus hat die betroffene Person auch das Recht auf die Vervollständigung unvollständiger personenbezogener Daten.⁷⁵⁹
- Das Recht auf Löschung personenbezogener Daten und Einschränkung der Verarbeitung. In bestimmten Fällen muss der Verantwortliche personenbezogene Daten löschen. Außerdem kann die betroffene Person im Falle der unrechtmäßigen Verarbeitung ihrer personenbezogenen Daten deren

756 *a.a.O.*, Artikel 13 Absatz 2.

757 *a.a.O.*, Artikel 14.

758 *a.a.O.*, Artikel 15.

759 *a.a.O.*, Artikel 16 Absatz 1.

Löschung erwirken.⁷⁶⁰ Anstatt die personenbezogenen Daten zu löschen, kann deren Verarbeitung in bestimmten Situationen eingeschränkt werden. Dies kann in den nachstehenden Fällen erfolgen: 1) wenn die Richtigkeit der personenbezogenen Daten bestritten wurde, dies jedoch nicht einwandfrei festgestellt werden kann, oder 2) wenn die personenbezogenen Daten für Beweiszwecke benötigt werden.⁷⁶¹

Verweigert der Verantwortliche die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung ihrer Verarbeitung, so ist die betroffene Person schriftlich davon in Kenntnis zu setzen. Die Mitgliedstaaten können dieses Recht auf Unterrichtung aus denselben Gründen wie das Auskunftsrecht einschränken, um unter anderem die öffentliche Sicherheit oder die Rechte und Freiheiten anderer zu schützen.⁷⁶²

Die betroffene Person hat normalerweise das Recht auf Unterrichtung über die Verarbeitung der sie betreffenden personenbezogenen Daten, sowie das Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, das direkt beim Verantwortlichen ausgeübt werden kann. Im Falle einer Einschränkung der Rechte der betroffenen Personen ist nach Maßgabe der Datenschutzrichtlinie für Polizei und Strafjustiz ersatzweise auch die indirekte Ausübung der Rechte der betroffenen Person über ihre Datenschutzaufsichtsbehörde möglich und kommt im Falle einer Einschränkung der Rechte der betroffenen Person seitens des Verantwortlichen zur Anwendung.⁷⁶³ Artikel 17 der Richtlinie erfordert, dass die Mitgliedstaaten dafür sorgen, dass die Rechte der betroffenen Person auch über ihre Aufsichtsbehörde ausgeübt werden können. Aus diesem Grund muss der Verantwortliche die betroffene Person über ihr Recht auf Befassung der Aufsichtsbehörde unterrichten.

Pflichten des Verantwortlichen und des Auftragsverarbeiters

Im Rahmen der Datenschutzrichtlinie für Polizei und Strafjustiz sind unter „Verantwortlichen“ die zuständigen Behörden oder andere Stellen, die mit den entsprechenden hoheitlichen Befugnissen und einer Amtsstellung ausgestattet sind zu verstehen, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen

⁷⁶⁰ a.a.O., Artikel 16 Absatz 2.

⁷⁶¹ a.a.O., Artikel 16 Absatz 3.

⁷⁶² a.a.O., Artikel 16 Absatz 4.

⁷⁶³ a.a.O., Artikel 17.

Daten entscheiden. Zur Gewährleistung eines hohen Schutzniveaus der zu Strafverfolgungszwecken verarbeiteten personenbezogenen Daten setzt die Richtlinie mehrere Pflichten für die Verantwortlichen fest.

Die zuständigen Behörden müssen für die von ihnen durchgeführten Verarbeitungsvorgänge Protokolle in automatisierten Verarbeitungssystemen führen. Zumindest die Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung der personenbezogenen Daten muss protokolliert werden.⁷⁶⁴ Die Richtlinie sieht vor, dass die Protokolle über Abfragen und Offenlegungen es ermöglichen müssen, das Datum und die Uhrzeit der Vorgänge, ihre Begründung und so weit wie möglich die Identifizierung der Person, die das System abgefragt oder die personenbezogenen Daten offengelegt hat, und die Empfänger der betreffenden personenbezogenen Daten festzustellen. Die Protokolle werden ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren verwendet.⁷⁶⁵ Auf Anforderung der Aufsichtsbehörde stellen der Verantwortliche und der Auftragsverarbeiter dieser die Protokolle zur Verfügung.

Insbesondere ergibt sich aus der Richtlinie eine generelle Verpflichtung für Verantwortliche zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um sicherzustellen, dass die Verarbeitung in Übereinstimmung mit der Richtlinie erfolgt und um den Nachweis für die Rechtmäßigkeit der Verarbeitung erbringen zu können.⁷⁶⁶ Bei der Planung dieser Maßnahmen müssen sie die Art, den Umfang, die Umstände der Verarbeitung sowie insbesondere alle potenziellen Risiken für die Rechte und Freiheiten der Personen berücksichtigen. Die Verantwortlichen sollen interne Leitlinien verabschieden und Maßnahmen treffen, die die Einhaltung der Grundsätze des Datenschutzes, insbesondere des Grundsatzes Datenschutz durch Technik und entsprechende Voreinstellungen, unterstützen.⁷⁶⁷ Wenn die Verarbeitung beispielsweise aufgrund der Verwendung neuer Technologien voraussichtlich ein hohes Risiko für die Rechte der betroffenen Personen zur Folge hat, müssen die Verantwortlichen vor Beginn der Verarbeitung eine Datenschutz-Folgenabschätzung

⁷⁶⁴ a.a.O., Artikel 25 Absatz 1.

⁷⁶⁵ a.a.O., Artikel 25 Absatz 2.

⁷⁶⁶ a.a.O., Artikel 19.

⁷⁶⁷ a.a.O., Artikel 20.

durchführen.⁷⁶⁸ Die Richtlinie listet auch die Maßnahmen auf, die die Verantwortlichen zur Gewährleistung der Sicherheit der Verarbeitung umsetzen müssen. Dazu zählen Maßnahmen zur Verhinderung des unbefugten Zugangs zu den von ihnen verarbeiteten personenbezogenen Daten, zur Gewährleistung, dass berechnigte Personen ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben, zur Gewährleistung, dass das Verarbeitungssystem richtig funktioniert und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.⁷⁶⁹ Sofern eine Verletzung des Schutzes personenbezogener Daten erfolgt, setzt der Verantwortliche die Aufsichtsbehörde innerhalb einer Frist von drei Tagen unter Angabe der Art der Verletzung, ihrer wahrscheinlichen Folgen, der davon betroffenen Kategorien personenbezogener Daten und der ungefähren Zahl der betroffenen Personen darüber in Kenntnis. Wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge hat, ist diese darüber hinaus „unverzüglich“ darüber zu benachrichtigen.⁷⁷⁰

Die Richtlinie enthält den Grundsatz der Rechenschaftspflicht und verpflichtet die Verantwortlichen, Maßnahmen zur Gewährleistung der Einhaltung dieses Grundsatzes zu treffen. Die Verantwortlichen führen Verzeichnisse aller Kategorien von Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Der genaue Inhalt dieser Verzeichnisse ist in Artikel 24 der Richtlinie dargelegt. Die Verzeichnisse sind der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen, damit diese die Verarbeitungsvorgänge des Verantwortlichen überwachen kann. Eine weitere wichtige Maßnahme zur Verbesserung der Rechenschaftspflicht ist die Benennung eines Datenschutzbeauftragten (DSB). Die Verantwortlichen müssen einen DSB benennen, wenngleich die Richtlinie den Mitgliedstaaten erlaubt, Gerichte und andere unabhängige Justizbehörden von dieser Pflicht zu befreien.⁷⁷¹ Die Aufgaben des DSB gleichen denen im Anwendungsbereich der DSGVO. Der DSB überwacht die Einhaltung der Richtlinie und unterrichtet und berät die Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach den Datenschutzvorschriften. Der DSB berät auch in Bezug auf das Erfordernis zur Durchführung einer Datenschutz-Folgenabschätzung und ist die Anlaufstelle für die Aufsichtsbehörde.

⁷⁶⁸ a.a.O., Artikel 27.

⁷⁶⁹ a.a.O., Artikel 29.

⁷⁷⁰ a.a.O., Artikel 30 und 31.

⁷⁷¹ a.a.O., Artikel 32.

Datenübermittlung an Drittländer oder internationale Organisationen

Ebenso wie die DSGVO setzt die Richtlinie Voraussetzungen für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen fest. Im Falle einer nicht regulierten Datenübermittlung außerhalb der Rechtsordnung der EU könnten die im EU-Recht bereitgestellten Garantien und der starke Schutz untergraben werden. Gleichwohl unterscheiden sich diese Voraussetzungen von den Vorgaben der DSGVO. Die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisation ist erlaubt, sofern⁷⁷²

- die Übermittlung für die mit der Richtlinie verfolgten Ziele erforderlich ist;
- die personenbezogenen Daten an eine im Sinne der Richtlinie zuständige Behörde in einem Drittland oder eine internationale Organisation übermittelt werden, wenngleich es im speziellen Einzelfall eine Ausnahme von dieser Vorgabe gibt;⁷⁷³
- in Fällen der Übermittlung von im Zuge der grenzüberschreitenden Zusammenarbeit erhaltenen personenbezogenen Daten an Drittländer oder internationale Organisationen der Mitgliedstaat, aus dem die Daten stammen, die Übermittlung genehmigt hat;
- die Kommission einen Angemessenheitsbeschluss gefasst hat, geeignete Garantien eingerichtet wurden oder Ausnahmen für Datenübermittlungen in bestimmten Fällen anwendbar sind;
- im Fall der Weiterübermittlung personenbezogener Daten an ein anderes Drittland oder eine andere internationale Organisation die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, die Weiterübermittlung unter Berücksichtigung von unter anderem der Schwere der Straftat und des Datenschutzniveaus im Zielland zuvor genehmigt hat.⁷⁷⁴

Gemäß der Richtlinie kann die Übermittlung personenbezogener Daten stattfinden, sofern eine der drei nachstehenden Bedingungen erfüllt ist. Die erste Bedingung ist, dass die Europäische Kommission im Rahmen der Richtlinie einen Angemessenheitsbeschluss erlassen hat. Dieser Beschluss kann auf

⁷⁷² a.a.O., Artikel 35.

⁷⁷³ a.a.O., Artikel 39.

⁷⁷⁴ a.a.O., Artikel 35 Absatz 1.

das gesamte Gebiet eines Drittlands oder auf spezifische Sektoren in diesem Drittland oder auf eine internationale Organisation Anwendung finden. Dies kann jedoch nur erfolgen, sofern ein angemessenes Schutzniveau geboten ist und die in der Richtlinie dargelegten Bedingungen erfüllt sind.⁷⁷⁵ In diesen Fällen bedarf die Übermittlung personenbezogener Daten keiner Genehmigung des Mitgliedstaates.⁷⁷⁶ Die Europäische Kommission muss die Entwicklungen überwachen, die die Wirkungsweise des Angemessenheitsbeschlusses beeinträchtigen könnten. Darüber hinaus muss der Beschluss eine regelmäßige Überprüfung vorsehen. Soweit entsprechende Informationen dahingehend vorliegen, dass die Bedingungen in einem Drittland oder in einer internationalen Organisation kein angemessenes Schutzniveau mehr gewährleisten, kann die Kommission einen Beschluss auch widerrufen, ändern oder aussetzen. In diesem Fall nimmt die Kommission Beratungen mit dem Drittland oder der internationalen Organisation auf, um zu versuchen, Abhilfe für die Situation zu schaffen.

In Ermangelung eines Angemessenheitsbeschlusses kann sich die Datenübertragung auf geeignete Garantien stützen. Diese können entweder in einem rechtsverbindlichen Instrument festgelegt sein oder der Verantwortliche führt eine Selbstbeurteilung der Umstände durch, die bei der Übermittlung der personenbezogenen Daten eine Rolle spielen, und gelangt zu der Auffassung, dass geeignete Garantien bestehen. Die Selbstbeurteilung sollte mögliche Kooperationsvereinbarungen zwischen Europol oder Eurojust und dem Drittland oder der internationalen Organisation, das Vorliegen von Geheimhaltungspflichten und die Zweckbindung berücksichtigen, sowie Zusicherungen, dass die Daten für keine Form der grausamen und unmenschlichen Behandlung einschließlich der Todesstrafe verwendet werden.⁷⁷⁷ In letzterem Fall unterrichtet der Verantwortliche die zuständige Aufsichtsbehörde über die unter diese Fallgruppe fallenden Kategorien von Übermittlungen.⁷⁷⁸

Falls weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen, kann die Datenübermittlung in den in der Richtlinie dargelegten bestimmten Fällen dennoch erlaubt sein. Dazu zählen unter anderem der

⁷⁷⁵ a.a.O., Artikel 36.

⁷⁷⁶ a.a.O., Artikel 36 Absatz 1.

⁷⁷⁷ a.a.O., Erwägungsgrund 71.

⁷⁷⁸ a.a.O., Artikel 37 Absatz 1.

Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person und die Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit des Mitgliedstaats oder eines Drittlandes.⁷⁷⁹

In speziellen Einzelfällen kann die Datenübermittlung seitens der zuständigen Behörden an in Drittländern niedergelassene Empfänger erfolgen, bei denen es sich nicht um zuständige Behörden handelt, sofern zusätzlich zu einer der vorstehend beschriebenen drei Bedingungen die in Artikel 39 der Richtlinie dargelegten Bedingungen erfüllt sind. In diesem Fall muss die Übermittlung insbesondere für die Ausübung einer Aufgabe der übermittelnden zuständigen Behörde unbedingt erforderlich sein. Diese muss auch feststellen, dass keine Grundrechte und Grundfreiheiten der Personen das öffentliche Interesse an einer Übermittlung überwiegen. Solche Übermittlungen müssen dokumentiert werden und die übermittelnde zuständige Behörde muss die zuständige Aufsichtsbehörde darüber unterrichten.⁷⁸⁰

Im Zusammenhang mit Drittländern und internationalen Organisationen erfordert die Richtlinie schließlich auch die Entwicklung von Mechanismen der internationalen Zusammenarbeit zur Erleichterung der wirksamen Durchsetzung der Rechtsvorschriften, und erleichtert somit die Zusammenarbeit der Datenschutzaufsichtsbehörden mit Aufsichtsbehörden in anderen Ländern.⁷⁸¹

Unabhängige Überwachung und Rechtsbehelfe für die betroffenen Personen

Jeder Mitgliedstaat muss gewährleisten, dass eine oder mehrere unabhängige nationale Aufsichtsbehörden für Beratungstätigkeiten und für die Überwachung der Anwendung der nach Maßgabe der Richtlinie angenommenen Bestimmungen zuständig sind.⁷⁸² Bei der in Umsetzung der Richtlinie eingerichteten Aufsichtsbehörde kann es sich um dieselbe Aufsichtsbehörde handeln, die im Rahmen der DSGVO eingerichtet wurde, doch den Mitgliedstaaten ist es freigestellt, eine andere Behörde zu benennen, vorausgesetzt, diese erfüllt das Kriterium der

779 a.a.O., Artikel 38 Absatz 1.

780 a.a.O., Artikel 37 Absatz 3.

781 a.a.O., Artikel 40.

782 a.a.O., Artikel 41.

Unabhängigkeit. Die Aufsichtsbehörden nehmen auch Beschwerden entgegen, die Personen in Bezug auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten seitens der zuständigen Behörden einlegen.

Wenn der betroffenen Person die Ausübung ihrer Rechte aus zwingenden Gründen verweigert wird, muss sie das Recht auf Anrufung der zuständigen Aufsichtsbehörde oder eines Gerichts haben. Erleidet eine Person aufgrund einer Verletzung des die Richtlinie umsetzenden nationalen Rechts Schaden, hat sie ein Recht auf Schadenersatz seitens des Verantwortlichen oder jeder sonst nach dem Recht der Mitgliedstaaten zuständigen Stelle.⁷⁸³ Grundsätzlich müssen die betroffenen Personen bei jeder Verletzung ihrer, in Umsetzung der Richtlinie gewährten nationalen Rechte, Zugang zu einem gerichtlichen Rechtsbehelf haben.⁷⁸⁴

8.3. Sonstige spezifische Rechtsinstrumente für den Datenschutz im Bereich der Strafverfolgung

Über die Datenschutzrichtlinie für Polizei und Strafjustiz hinaus wird der Informationsaustausch zwischen Mitgliedstaaten in bestimmten Bereichen noch durch eine Reihe weiterer Rechtsinstrumente geregelt, so z. B. den Rahmenbeschluss 2009/315/JI des Rates über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten, den Beschluss 2000/642/JI des Rates über Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen und den Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union.⁷⁸⁵

783 a.a.O., Artikel 56.

784 a.a.O., Artikel 54.

785 Rat der Europäischen Union (2009), Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten, ABl. L 93 vom 7.4.2009; Rat der Europäischen Union (2000), Beschluss 2000/642/JI des Rates vom 17. Oktober 2000 über Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen, ABl. L 271 vom 24.10.2000; Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, ABl. L 386 vom 29.12.2006.

Wichtig ist auch, dass bei der grenzüberschreitenden Zusammenarbeit⁷⁸⁶ zwischen den zuständigen Behörden zunehmend Daten über Immigration ausgetauscht werden. Dieser Rechtsbereich gilt zwar nicht als Bestandteil der Bereiche Polizei und Strafjustiz, ist aber in vielerlei Hinsicht für die Arbeit von Polizei- und Justizbehörden relevant. Gleiches gilt für Daten über Waren, die in die EU eingeführt oder aus der EU ausgeführt werden. Die Abschaffung der Kontrollen an den Binnengrenzen innerhalb des Schengen-Raums hat das Betrugsrisiko deutlich vergrößert und verlangte daher von den Mitgliedstaaten eine engere Zusammenarbeit, insbesondere durch einen Ausbau des grenzüberschreitenden Informationsaustauschs, um auf diese Weise Verstöße gegen das Zollrecht der Mitgliedstaaten und der EU wirksamer aufdecken und ahnden zu können. Darüber hinaus erlebte die Welt in den letzten Jahren einen Anstieg der schweren und organisierten Kriminalität, die mit Reisen in andere Länder einhergehen kann und in vielen Fällen den Bedarf nach einer verstärkten grenzübergreifenden Zusammenarbeit der Polizei- und Strafverfolgungsbehörden offenbart hat.⁷⁸⁷

Der Beschluss von Prüm

Ein wichtiges Beispiel für institutionalisierte grenzüberschreitende Zusammenarbeit durch Austausch von im Besitz einzelner Länder befindlicher Daten ist der Beschluss 2008/615/JI des Rates und die darin enthaltenen Durchführungsbestimmungen zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität („Beschluss von Prüm“), mit dem der Vertrag von Prüm 2008 in das EU-Recht aufgenommen wurde.⁷⁸⁸ Der Vertrag von Prüm war ein 2005 von Österreich, Belgien, Frankreich, Deutschland, Luxemburg, den Niederlanden und Spanien unterzeichnetes internationales Abkommen über die polizeiliche Zusammenarbeit.⁷⁸⁹

⁷⁸⁶ Europäische Kommission (2012), Mitteilung der Kommission an das Europäische Parlament und den Rat – Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch (EIXM), COM(2012) 735 final, Brüssel, 7. Dezember 2012.

⁷⁸⁷ Siehe Europäische Kommission (2011), Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, COM(2011) 32 final, Brüssel, 2. Februar 2011, S. 1.

⁷⁸⁸ Rat der Europäischen Union (2008), Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl. L 210 vom 6.8.2008.

⁷⁸⁹ Vertrag zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration.

Ziel des Beschlusses von Prüm ist es, unterzeichnenden Mitgliedstaaten bei der Verbesserung des Informationsaustauschs für Zwecke der Abwehr und Bekämpfung von Kriminalität in drei Bereichen zu helfen: Terrorismus, grenzüberschreitende Kriminalität und illegale Migration. Zu diesem Zweck enthält der Beschluss Bestimmungen über:

- den automatisierten Zugriff auf DNA-Profile, Fingerabdruckdaten und bestimmte einzelstaatliche Fahrzeugregisterdaten;
- die Übermittlung von Daten im Zusammenhang mit Großveranstaltungen mit grenzüberschreitendem Bezug;
- die Übermittlung von Informationen zur Verhinderung terroristischer Straftaten;
- sonstige Maßnahmen zur Intensivierung der grenzüberschreitenden polizeilichen Zusammenarbeit.

Die gemäß dem Beschluss von Prüm aufgebauten Datenbanken unterstehen in vollem Umfang einzelstaatlichem Recht, der Datenaustausch wird darüber hinaus jedoch auch im Beschluss geregelt, dessen Übereinstimmung mit der Datenschutzrichtlinie für Polizei und Strafjustiz geprüft werden muss. Zuständig für die Kontrolle dieses Datenverkehrs sind die nationalen Datenschutzaufsichtsbehörden.

Rahmenbeschluss 2006/960/JI – die Schwedische Initiative

Der Rahmenbeschluss 2006/960/JI (die „Schwedische Initiative“)⁷⁹⁰ ist ein weiteres Beispiel für die grenzüberschreitende Zusammenarbeit in Bezug auf den Austausch von Daten nationaler Strafverfolgungsbehörden. Die Schwedische Initiative konzentriert sich insbesondere auf den Austausch von Erkenntnissen und Informationen und sieht in Artikel 8 spezielle Datenschutzvorschriften vor.

Dieses Rechtsinstrument sieht vor, dass die Verwendung von ausgetauschten Informationen und Erkenntnissen den nationalen Datenschutzbestimmungen des Mitgliedstaats unterliegen muss, der die Informationen empfängt, so dass dieselben Vorschriften gelten, als wären sie in diesem Mitgliedstaat gesammelt worden.

⁷⁹⁰ Rat der Europäischen Union (2006), Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, ABl. L 386 vom 29.12.2006, S. 89.

Artikel 8 geht noch weiter und legt dar, dass die zuständige Strafverfolgungsbehörde, die Informationen und Erkenntnisse zur Verfügung stellt, in Übereinstimmung mit ihrem nationalen Recht Bedingungen für deren Verwendung durch die empfangende zuständige Strafverfolgungsbehörde festlegen kann. Diese Bedingungen können auch auf die Mitteilung der Ergebnisse der strafrechtlichen Ermittlungen oder auf polizeiliche Erkenntnisgewinnungsverfahren Anwendung finden, für die der Austausch der Informationen und Erkenntnisse angefordert wurde. Sofern das nationale Recht jedoch Abweichungen von den Verwendungsbeschränkungen vorsieht (z. B. für Gerichte, an der Gesetzgebung beteiligte Institutionen, usw.) dürfen die Informationen und Erkenntnisse nur nach vorheriger Konsultierung des übermittelnden Mitgliedstaats verwendet werden.

Die bereitgestellten Informationen und Erkenntnisse dürfen für die nachstehenden Zwecke verwendet werden:

- für die Zwecke, für die sie übermittelt wurden, oder
- zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit.

Die Verarbeitung zu anderen Zwecken kann gestattet werden, bedarf jedoch der vorherigen Genehmigung des übermittelnden Mitgliedstaats.

Die Schwedische Initiative legt überdies dar, dass die verarbeiteten personenbezogenen Daten gemäß internationaler Rechtsinstrumente zu schützen sind, wie:

- dem Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten;⁷⁹¹
- dem Zusatzprotokoll zu diesem Übereinkommen vom 8. November 2001 bezüglich Aufsichtsbehörden und grenzüberschreitendem Datenverkehr;⁷⁹²
- der Empfehlung R (87) 15 des Europarats über die Nutzung personenbezogener Daten im Polizeibereich.⁷⁹³

791 Europarat (1981), Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, SEV Nr. 108.

792 Europarat (2001), Zusatzprotokoll zum Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, SEV Nr. 108.

793 Europarat (1987), Empfehlung R (87) 15 des Ministerkomitees an die Mitgliedstaaten über die Nutzung personenbezogener Daten im Polizeibereich (Seitens des Ministerkomitees am 17. September 1987 auf der 410. Sitzung der Ministerstellvertreter angenommen).

Die EU-PNR-Richtlinie

Fluggastdatensätze (PNR-Daten) beziehen sich auf Informationen über Fluggäste, die die Fluggesellschaften für ihre eigenen geschäftlichen Zwecke in ihren Buchungs- und Abfertigungssystemen erfassen und speichern. Diese Datensätze enthalten verschiedene Arten von Informationen wie Reisedaten, Reiseroute, Flugscheininformationen, Kontaktangaben, das Reisebüro, bei dem der Flug gebucht wurde, Zahlungsart, Sitznummer und Angaben zum Gepäck.⁷⁹⁴ Die Verarbeitung von PNR-Daten kann den Strafverfolgungsbehörden bei der Identifizierung bekannter oder potenzieller Verdächtiger und bei der Durchführung von Überprüfungen auf Grundlage des Reiseverhaltens und anderer Indikatoren helfen, die typischerweise mit kriminellen Handlungen in Verbindung gebracht werden. Die Analyse der PNR-Daten ermöglicht auch die nachträgliche Verfolgung von Reiserouten und Kontakten von Personen, die der Beteiligung an kriminellen Handlungen verdächtigt werden, was den Strafverfolgungsbehörden die Identifizierung krimineller Netzwerke ermöglichen kann.⁷⁹⁵ Wie in [Kapitel 7](#) erläutert, hat die EU einige Abkommen mit Drittländern für den Austausch von PNR-Daten geschlossen. Überdies führte sie mittels der Richtlinie 2016/681/EU über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (EU-PNR-Richtlinie) die Verarbeitung von PNR-Daten in der EU ein.⁷⁹⁶ Diese Richtlinie verpflichtet die Fluggesellschaften zur Übermittlung der PNR-Daten an die zuständigen Behörden und führt strenge Sicherheitsvorkehrungen für die Verarbeitung und Erhebung dieser Daten ein. Die EU-PNR-Richtlinie findet auf internationale Flüge in die und aus der EU Anwendung und sofern sich ein Mitgliedstaat dafür entscheidet, auch auf EU-Flüge.⁷⁹⁷

Die erhobenen PNR-Daten dürfen ausschließlich die durch die EU-PNR-Richtlinie erlaubten Informationen enthalten. Sie sind in jedem Mitgliedstaat in einer Zentralstelle an einem gesicherten Ort vorzuhalten. Die PNR-Daten sind sechs Monate nach ihrer Übermittlung von der Fluggesellschaft zu entpersonalisieren und für einen

794 Europäische Kommission (2011), Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, COM(2011) 32 final, Brüssel, 2. Februar 2011, S. 3.

795 Europäische Kommission (2015), Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives, Brüssel, 11. Januar 2015.

796 [Richtlinie \(EU\) 2016/681](#) des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. L 119 vom 4.5.2016, S. 132.

797 PNR-Richtlinie, ABl. L 119 vom 4.5.2016, S. 132, Artikel 1 Absatz 1 und Artikel 2 Absatz 1.

Zeitraum von maximal fünf Jahren vorzuhalten.⁷⁹⁸ Die PNR-Daten werden zwischen den Mitgliedstaaten, zwischen den Mitgliedstaaten und Europol und nur im Einzelfall mit Drittländern ausgetauscht.

Die Übermittlung und Verarbeitung der PNR-Daten und die den betroffenen Personen garantierten Rechte müssen mit der Datenschutzrichtlinie für Polizei und Strafjustiz übereinstimmen und das in der Charta, im Modernisierten Übereinkommen Nr. 108 und in der EMRK geforderte hohe Schutzniveau für die Privatsphäre und die personenbezogenen Daten gewährleisten.

Den im Rahmen der Datenschutzrichtlinie für Polizei und Strafjustiz zuständigen unabhängigen nationalen Aufsichtsbehörden obliegt auch die Beratung und Überwachung der Anwendung von Umsetzungsrechtsakten nach Maßgabe der EU-PNR-Richtlinie angenommenen Bestimmungen.

Vorratsspeicherung von Telekommunikationsdaten

Nach der Richtlinie über die Vorratsspeicherung von Daten⁷⁹⁹, die am 8. April 2014 im Rahmen der Rechtssache *Digital Rights Ireland* für ungültig erklärt wurde, waren Anbieter von Kommunikationsdiensten verpflichtet, für den Zweck der Bekämpfung schwerer Kriminalität für einen Zeitraum von mindestens sechs und höchstens 24 Monaten Metadaten bereitzuhalten, unabhängig davon, ob der Anbieter diese Daten noch für die Gebührenabrechnung oder die technische Bereitstellung des Dienstes benötigte oder nicht.

Die Vorratsspeicherung von Telekommunikationsdaten ist eindeutig ein Eingriff in das Recht auf Datenschutz.⁸⁰⁰ Ob dieser Eingriff gerechtfertigt ist oder nicht, war Gegenstand mehrerer Verfahren vor Gerichten in EU-Mitgliedstaaten.⁸⁰¹

⁷⁹⁸ a.a.O., Artikel 12 Absatz 1 und Artikel 12 Absatz 2.

⁷⁹⁹ Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.5.2006.

⁸⁰⁰ EDSB (2011), Stellungnahme vom 31. Mai 2011 zum Bewertungsbericht der Kommission an den Rat und das Europäische Parlament zur Richtlinie über die Vorratsspeicherung von Daten (Richtlinie 2006/24/EG), 31. Mai 2011.

⁸⁰¹ Deutschland, Bundesverfassungsgericht, 1 BvR 256/08, 2. März 2010; Rumänien, Verfassungsgerichtshof (*Curtea Constituțională a României*), Nr. 1258, 8. Oktober 2009; Tschechische Republik, Verfassungsgerichtshof (Ústavní soud České republiky), 94/2011 Coll., 22. März 2011.

Beispiel: In der Rechtssache *Digital Rights Ireland und Kärntner Landesregierung und andere*⁸⁰² erhoben die Gruppe Digital Rights und Herr Seitlinger Klage vor dem irischen High Court bzw. vor dem österreichischen Verfassungsgerichtshof, mit der sie die Rechtmäßigkeit nationaler Maßnahmen in Abrede stellten, die die Vorratsspeicherung elektronischer Telekommunikationsdaten erlaubten. Digital Rights ersuchte das irische Gericht um die Feststellung der Unwirksamkeit der Richtlinie 2006/24 und des Teils des nationalen Gesetzes über terroristische Straftaten. Ebenso forcht Herr Seitlinger zusammen mit über 11 000 weiteren Antragstellern eine Bestimmung des österreichischen Telekommunikationsgesetzes zur Umsetzung der Richtlinie 2006/24 an und ersuchte um deren Nichtigerklärung.

Der EuGH erklärte die Richtlinie über die Vorratsspeicherung von Daten für ungültig. Nach Ansicht des EuGH lieferte die Gesamtheit der Daten, die nach Maßgabe der Richtlinie gespeichert werden konnten, genaue Informationen über die Personen. Darüber hinaus untersuchte der EuGH die Schwere des Eingriffs in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten. Er befand, dass die Vorratsspeicherung ein Ziel von öffentlichem Interesse verfolge, das in der Bekämpfung schwerer Kriminalität und somit im Schutz der öffentlichen Sicherheit bestehe. Gleichwohl stellte der EuGH fest, dass der EU-Gesetzgeber beim Erlass der Richtlinie gegen den Grundsatz der Verhältnismäßigkeit verstoßen habe. Obgleich die Richtlinie zur Erreichung des erforderlichen Ziels geeignet sein mag, „ist festzustellen, dass die Richtlinie einen Eingriff in die Grundrechte [auf Achtung des Privatlebens und auf Schutz personenbezogener Daten] beinhaltet, der [...] von großem Ausmaß und von besonderer Schwere ist, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.“

In Ermangelung spezifischer Rechtsvorschriften über die Vorratsdatenspeicherung ist die Vorratsdatenspeicherung als Ausnahme von der in der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)⁸⁰³ dargelegten Vertraulichkeit der Telekommunikationsdaten als vorbeugende

802 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014, Randnr. 65.

803 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002.

Maßnahme erlaubt, muss jedoch auf den alleinigen Zweck der Bekämpfung schwerer Kriminalität beschränkt sein. Eine solche Vorratsspeicherung muss in Bezug auf die Kategorien der auf Vorrat gespeicherten Daten, die betroffenen Kommunikationsmittel, die betroffenen Personen und die gewählte Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt sein. Nationale Behörden können unter strengen Bedingungen, darunter der vorherigen Überprüfung seitens einer unabhängigen Behörde, Zugang zu den auf Vorrat gespeicherten Daten erhalten. Die Daten sind innerhalb der EU aufzubewahren.

Beispiel: Im Anschluss an das Urteil in der Rechtssache *Digital Rights Ireland und Kärntner Landesregierung und andere*⁸⁰⁴, wurden zwei weitere Rechtssachen vor den EuGH gebracht, in denen es um die den Anbietern elektronischer Kommunikationsdienste in Schweden und im Vereinigten Königreich auferlegte allgemeine Pflicht zur Vorratsspeicherung von Telekommunikationsdaten ging, wie in der für ungültig erklärten Richtlinie über die Vorratsspeicherung von Daten gefordert. In der Rechtssache *Tele2 Sverige und Home Department gegen Tom Watson und andere*⁸⁰⁵ entschied der EuGH, dass eine nationale Regelung, die die allgemeine und unterschiedslose Vorratsdatenspeicherung vorschreibt, ohne einen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit zu verlangen und ohne Angabe von Bedingungen wie beispielsweise der Zeitdauer der Vorratsspeicherung, des geografischen Gebiets oder des Personenkreises, der in eine schwere Straftat verwickelt sein könnte, die Grenzen des absolut Notwendigen überschreitet und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden kann, wie es die Richtlinie 2002/58/EG im Licht der Charta der Grundrechte der EU verlangt.

Ausblick

Im Januar 2017 veröffentlichte die Europäische Kommission einen Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation, der die

804 EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014.

805 EuGH, Verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB / Post- och telestyrelsen und Secretary of State for the Home Department / Tom Watson und andere* [GK], 21. Dezember 2016.

Richtlinie 2002/58/EG aufheben und ersetzen sollte.⁸⁰⁶ Der Vorschlag enthält keine speziellen Bestimmungen über die Vorratsdatenspeicherung. Er sieht jedoch vor, dass die Mitgliedstaaten einige in der Verordnung enthaltenen Pflichten und Rechte mittels Rechtsvorschriften beschränken können, wenn diese Beschränkung eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter öffentlicher Interessen darstellt, wozu die nationale Sicherheit, die Verteidigung, die öffentliche Sicherheit und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zählen.⁸⁰⁷ Daher könnten die Mitgliedstaaten nationale Bestimmungen für die Vorratsdatenspeicherung schaffen oder beibehalten, die gezielte Vorratsspeicherungen vorsehen, sofern solche Bestimmungen unter Beachtung der Rechtsprechung des EuGH zur Auslegung der e-Datenschutzrichtlinie und der Charta der Grundrechte der EU mit dem Unionsrecht vereinbar sind.⁸⁰⁸ Zum Zeitpunkt der Abfassung des vorliegenden Handbuchs wurde über den Erlass der Verordnung noch diskutiert.

EU-US-Datenschutz-Rahmenabkommen („Umbrella Agreement“) über den Schutz von zu Strafverfolgungszwecken ausgetauschten personenbezogenen Daten

Am 1. Februar 2017 trat das EU-US-Rahmenabkommen für die Verarbeitung personenbezogener Daten zur Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten in Kraft.⁸⁰⁹ Das EU-US-Rahmenabkommen will ein hohes Datenschutzniveau für Unionsbürger unter gleichzeitiger Verbesserung der Zusammenarbeit zwischen den Strafverfolgungsbehörden der EU und der USA gewährleisten. Es ergänzt die zwischen der EU und den Vereinigten Staaten sowie den Mitgliedstaaten und den Vereinigten Staaten bestehenden Abkommen zwischen Strafverfolgungsbehörden und schafft gleichzeitig klare und harmonisierte Datenschutzvorschriften für künftige Vereinbarungen in diesem Bereich. Diesbezüglich will das Abkommen einen dauerhaften Rechtsrahmen zur Erleichterung des Austauschs von Informationen schaffen.

806 Europäische Kommission (2017), 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, Brüssel, 10. Januar 2017.

807 *a.a.O.*, Erwägungsgrund 26.

808 Siehe die Begründung zum Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation COM(2017) 10 final, Punkt 1.3.

809 Siehe Rat der EU (2016), „Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign ‘Umbrella agreement’“, Pressemitteilung 305/16, 2. Juni 2016.

Das Abkommen stellt keine Rechtsgrundlage für den Austausch personenbezogener Daten dar, bietet den betroffenen Personen jedoch angemessene Garantien. Es deckt jedwede für die Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus erforderliche Verarbeitung personenbezogener Daten ab.⁸¹⁰

Das Abkommen legt zahlreiche Garantien zur Gewährleistung der ausschließlichen Verwendung der personenbezogenen Daten für die im Abkommen dargelegten Zwecke fest. Insbesondere stellt es den Unionsbürgern die nachstehenden Garantien bereit:

- Beschränkungen der Verwendung personenbezogener Daten: personenbezogene Daten dürfen nur für den Zweck der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten verwendet werden;
- Schutz vor willkürlicher und ungerechtfertigter Diskriminierung;
- Weiterübermittlungen: jede Weiterübermittlung an ein Land außerhalb der Vereinigten Staaten, außerhalb der EU oder an eine internationale Organisation unterliegt der vorherigen Zustimmung der zuständigen Behörde des Landes, das die Daten ursprünglich übermittelt hat;
- Datenqualität: personenbezogene Daten sind unter Berücksichtigung ihrer Genauigkeit, Relevanz, Aktualität und Vollständigkeit aufzubewahren;
- Verarbeitungssicherheit einschließlich der Meldung von Verletzungen des Schutzes personenbezogener Daten;
- sensible Daten dürfen nur unter Wahrung angemessener Garantien im Einklang mit dem Recht verarbeitet werden;
- Speicherfristen: personenbezogene Daten dürfen nicht länger gespeichert werden, als notwendig oder angemessen;

⁸¹⁰ Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union vom 18. Mai 2016 über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten, (OR.en) 8557/16, Artikel 3 Absatz 1. Siehe auch Mitteilung der Kommission über die Verhandlungen vom 26. Mai 2010 über das EU-US-Datenschutzabkommen, MEMO/10/216 und die Pressemitteilung der EU-Kommission (2010) vom 26. Mai 2010 über die strengen Regeln für den Schutz der Privatsphäre im EU-US-Datenschutzabkommen, IP 10/609.

- Rechte auf Auskunft und Berichtigung: jede Person hat unter gewissen Voraussetzungen Zugang zu ihren personenbezogenen Daten und kann die Berichtigung unrichtiger Daten verlangen;
- automatisierte Entscheidungen erfordern angemessene Garantien einschließlich der Möglichkeit, das Eingreifen eines Menschen zu erwirken;
- wirksame Aufsicht einschließlich der Zusammenarbeit zwischen den Aufsichtsbehörden der EU und der Vereinigten Staaten, und
- gerichtlichen Rechtsbehelf und Durchsetzbarkeit: Unionsbürger haben das Recht⁸¹¹ zur Einlegung von Rechtsbehelfen bei Gerichten in den Vereinigten Staaten, sofern ihnen die US-Behörden das Recht auf Auskunft oder Berichtigung ihrer personenbezogenen Daten verweigern oder diese unrechtmäßig offenlegen.

Unter dem „Rahmenabkommen“ wurde auch ein System eingerichtet, in dessen Rahmen die zuständige Aufsichtsbehörde im Mitgliedstaat der betroffenen Personen bei Bedarf über alle Datenschutzverletzungen benachrichtigt wird. Die im Abkommen vorgesehenen gesetzlichen Garantien gewährleisten im Falle einer Datenschutzverletzung die Gleichbehandlung von Unionsbürgern in den Vereinigten Staaten.⁸¹²

8.3.1. Datenschutz in den Justiz- und Strafverfolgungsbehörden der EU

Europol

Europol, die Strafverfolgungsbehörde der EU, hat ihren Sitz in Den Haag und verfügt in jedem Mitgliedstaat über eine nationale Europol-Stelle (ENU). Europol wurde

811 Das [US-Gesetz über den gerichtlichen Rechtsbehelf](#) wurde von Präsident Obama am 24. Februar 2016 unterzeichnet.

812 Der Europäische Datenschutzbeauftragte gab eine Stellungnahme zum Abkommen zwischen den Vereinigten Staaten und der Europäischen Union ab, in der er unter anderem die nachstehenden Anpassungen empfahl: 1) Hinzufügung von „zu den spezifischen Zwecken, zu denen sie übermittelt wurden“ zu dem Artikel, in dem es darum geht, dass die Daten nicht länger gespeichert werden, als notwendig und angemessen ist, und 2) Ausschluss der möglichen massenhaften Übermittlung sensibler Daten. Siehe [Europäischer Datenschutzbeauftragter, Stellungnahme 1/2016](#), Vorläufige Stellungnahme zum Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei deren Übermittlung und Verarbeitung zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten, § 35.

1998 errichtet; ihr derzeitiger rechtlicher Status als EU-Organ stützt sich auf die Verordnung über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol-Verordnung).⁸¹³ Ziel von Europol ist es, bei der Abwehr und Untersuchung von organisierter Kriminalität, Terrorismus und anderen Formen schwerer Kriminalität, wie sie im Anhang I der Europol-Verordnung aufgeführt sind, wenn zwei oder mehr Mitgliedstaaten betroffen sind, zu helfen. Dies erfolgt durch den Austausch von Informationen und durch die Rolle eines Informationszentrums der EU, das die Informationen der Nachrichtendienste auswertet und Bedrohungsanalysen erstellt.

Um diese Ziele zu erreichen, hat Europol das Europol-Informationssystem aufgebaut, das den Mitgliedstaaten eine Datenbank für den Austausch kriminalpolizeilicher Erkenntnisse und Informationen über ihre ENU bietet. Das Europol-Informationssystem kann benutzt werden, um folgende Daten zur Verfügung zu stellen: Daten über Personen, die einer Straftat oder der Beteiligung an einer Straftat, für die Europol zuständig ist, verdächtigt werden, oder Personen, in deren Fall faktische Anhaltspunkte oder triftige Gründe dafür vorliegen, dass sie solche Straftaten begehen werden. Europol und die ENU dürfen Daten direkt in das Europol-Informationssystem eingeben und daraus abrufen. Nur die Stelle, die die Daten in das System eingegeben hat, darf sie ändern, berichtigen oder löschen. Auch EU-Einrichtungen, Drittländer und internationale Organisationen können Europol Informationen bereitstellen.

Europol kann Informationen einschließlich personenbezogener Daten auch aus öffentlich zugänglichen Quellen wie dem Internet einholen. Die Übermittlung personenbezogener Daten an EU-Einrichtungen ist nur erlaubt, sofern sie für die Durchführung der Aufgabe von Europol oder der die Daten empfangenden EU-Einrichtung erforderlich ist. Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen sind nur möglich, wenn die Europäische Kommission beschließt, dass das betreffende Land oder die betreffende internationale Organisation ein angemessenes Datenschutzniveau gewährleistet („Angemessenheitsbeschluss“) oder ein internationales Abkommen oder ein Kooperationsabkommen vorliegt. Europol kann personenbezogene Daten von privaten Parteien und Privatpersonen unter der strikten Bedingung empfangen und verarbeiten, dass diese Daten von einer ENU nach deren nationalem Recht, von einer Kontaktstelle in einem Drittstaat oder von einer

813 [Verordnung \(EU\) 2016/794](#) des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. L 135 vom 24.5.2016, S. 53.

internationalen Organisation, mit der eine Zusammenarbeit aufgrund eines Kooperationsabkommens besteht, oder von einer Behörde eines Drittstaats oder von einer internationalen Organisation, die Gegenstand eines Angemessenheitsbeschlusses ist oder mit der die Union eine internationale Übereinkunft geschlossen hat, übermittelt werden. Sämtliche Informationsaustausche erfolgen über eine Netzanwendung für sicheren Datenaustausch (SIENA).

Als Reaktion auf neuere Entwicklungen wurden bei Europol Fachzentren eingerichtet. Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität wurde 2013 bei Europol eingerichtet.⁸¹⁴ Das Zentrum dient als EU-Informationsdrehscheibe für die Bekämpfung der Cyberkriminalität, leistet einen Beitrag zu schnelleren Reaktionen bei Online-Straftaten, dient der Entwicklung und dem Einsatz digitaler forensischer Fähigkeiten und liefert bewährte Vorgehensweisen für Ermittlungen gegen Cyberstraftaten. Das Zentrum befasst sich schwerpunktmäßig mit Cyberstraftaten, die

- von organisierten Gruppen zwecks Erzielung großer krimineller Gewinne begangen werden, wie Online-Betrug;
- dem Opfer erheblichen Schaden zufügen, wie sexuelle Ausbeutung von Kindern im Internet;
- kritische Infrastruktur- und Informationssysteme in der EU berühren.

Im Januar 2016 wurde das Europäische Zentrum zur Terrorismusbekämpfung (ECTC) eingerichtet, um die Mitgliedstaaten bei Ermittlungen in Bezug auf terroristische Straftaten zu unterstützen.

Es gleicht Echtzeitdaten mit bereits vorhandenen Daten von Europol ab, bringt schnell finanzielle Vorteile ans Licht und analysiert alle verfügbaren Untersuchungsergebnisse, um ein strukturiertes Bild eines terroristischen Netzwerks zu erstellen.⁸¹⁵

814 Siehe auch EDSB (2012), Stellungnahme des Datenschutzbeauftragten zu der Mitteilung der Europäischen Kommission an den Rat und das Europäische Parlament über die Errichtung eines Zentrums zur Bekämpfung der Cyberkriminalität, Brüssel, 29. Juni 2012.

815 Siehe die Europol [Website zum ECTC](#).

Das Europäische Zentrum zur Bekämpfung der Migrantenschleusung (EMSC) wurde im Februar 2016 im Anschluss an eine im November 2015 stattgefundene Tagung des Rates eingerichtet, um die Mitgliedstaaten bei der Identifizierung und Zerstörung von kriminellen Netzwerken im Bereich der Schleusung zu unterstützen. Es fungiert als Informationsdrehscheibe zur Unterstützung der Büros der Regionalen Taskforce der EU in Catania (Italien) und Piräus (Griechenland), die den nationalen Behörden in vielen Bereichen beistehen, darunter beim Austausch von Informationen, bei strafrechtlichen Ermittlungen und bei der strafrechtlichen Verfolgung von kriminellen Schleusernetzen.⁸¹⁶

Die für Europol geltenden Datenschutzvorschriften wurden verbessert und stützen sich auf die Grundsätze der Datenschutzverordnung für die EU-Organe⁸¹⁷ und entsprechen auch den Bestimmungen der Datenschutzrichtlinie für Polizei und Strafjustiz, des Modernisierten Übereinkommens Nr. 108 und der Polizei-Empfehlung.

Die Verarbeitung personenbezogener Daten in Bezug auf Opfer von Straftaten, Zeugen oder andere Personen, die Informationen über Straftaten liefern können, oder in Bezug auf Personen unter 18 Jahren ist erlaubt, wenn sie für die Verhütung oder Bekämpfung von Straftaten, die unter die Ziele von Europol fallen, unbedingt notwendig und verhältnismäßig ist.⁸¹⁸ Die Verarbeitung sensibler personenbezogener Daten ist verboten, es sein denn, dass sie für die Verhütung oder Bekämpfung von Straftaten, die unter die Ziele von Europol fallen, unbedingt notwendig und verhältnismäßig ist und dass diese Daten andere von Europol verarbeitete personenbezogene Daten ergänzen.⁸¹⁹ In beiden Fällen hat allein Europol Zugriff auf die entsprechenden Daten.⁸²⁰

Die Speicherung der Daten ist nur über eine erforderliche und verhältnismäßige Zeitspanne erlaubt und die fortgesetzte Speicherung unterliegt einer alle drei Jahre stattfindenden Prüfung, ohne die die Daten automatisch gelöscht werden.⁸²¹

816 Siehe die Europol [Website](#) zum EMSC.

817 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001.

818 Europol-Verordnung, Artikel 30 Absatz 1.

819 a.a.O., Artikel 30 Absatz 2.

820 a.a.O., Artikel 30 Absatz 3.

821 a.a.O., Artikel 31.

Unter bestimmten Voraussetzungen kann Europol personenbezogene Daten direkt an eine Unionseinrichtung oder an einen Drittstaat oder eine internationale Organisation übermitteln.⁸²² Verletzungen des Datenschutzes, die wahrscheinlich eine schwere Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen zur Folge haben, sind diesen unverzüglich mitzuteilen.⁸²³ Auf Ebene der Mitgliedstaaten wird eine nationale Kontrollbehörde zur Überwachung der Verarbeitung personenbezogener Daten durch Europol ernannt.⁸²⁴

Der EDSB ist zuständig für die Kontrolle und Sicherstellung des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Europol sowie für die Beratung von Europol und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten. Zu diesem Zweck fungiert der EDSB als Untersuchungs- und Beschwerdestelle und arbeitet eng mit den nationalen Kontrollbehörden zusammen.⁸²⁵ Der EDSB und die nationalen Kontrollbehörden treten im Rahmen des Beirats für die Zusammenarbeit, dem eine Beratungsfunktion zukommt, mindestens zweimal jährlich zusammen.⁸²⁶ Die Mitgliedstaaten sind gesetzlich zur Einrichtung einer Kontrollbehörde verpflichtet, die für die Überwachung der Zulässigkeit der Übermittlung personenbezogener Daten von den Mitgliedstaaten an Europol und des Abrufs personenbezogener Daten sowie jedweder Übermittlung dieser personenbezogenen Daten an Europol durch die Mitgliedstaaten zuständig ist.⁸²⁷ Überdies sind die Mitgliedstaaten dazu verpflichtet, sicherzustellen, dass die nationale Kontrollbehörde beim Vollzug ihrer Aufgaben und Pflichten gemäß der Europol-Verordnung völlig unabhängig handeln kann.⁸²⁸ Zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenkontrolle ihrer Tätigkeiten und der Sicherstellung der Integrität und Sicherheit der Daten führt Europol Protokolle oder Dokumentationen über ihre Datenverarbeitungstätigkeiten. Diese Protokolle enthalten Informationen über Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen in Bezug auf die Erhebung, Veränderung, Abfrage, Offenlegung, Kombination und Löschung personenbezogener Daten.⁸²⁹

822 a.a.O., Artikel 24 bzw. Artikel 25.

823 a.a.O., Artikel 35.

824 Europol-Verordnung, Artikel 42.

825 a.a.O., Artikel 43 und Artikel 44.

826 a.a.O., Artikel 45.

827 a.a.O., Artikel 42 Absatz 1.

828 a.a.O., Artikel 42 Absatz 1.

829 a.a.O., Artikel 40.

Rechtsbehelfe gegen Entscheidungen des EDSB können beim EuGH eingelegt werden.⁸³⁰ Jede Person, der wegen einer widerrechtlichen Datenverarbeitung ein Schaden entsteht, hat das Recht, entweder von Europol oder von dem verantwortlichen Mitgliedstaat Schadensersatz zu fordern, indem sie im ersten Fall beim EuGH oder im zweiten Fall bei dem zuständigen nationalen Gericht Klage erhebt.⁸³¹ Darüber hinaus können die Tätigkeiten von Europol durch einen speziellen Gemeinsamen parlamentarischen Kontrollausschuss kontrolliert werden, der sich aus den nationalen Parlamenten und dem Europäischen Parlament zusammensetzt.⁸³² Jede Person hat das Recht auf Auskunft über die seitens Europol über sie möglicherweise gespeicherten personenbezogenen Daten, sowie das Recht auf die Erwirkung ihrer Überprüfung, Korrektur oder Löschung. Diese Rechte können Ausnahmen und Einschränkungen unterliegen.

Eurojust

Eurojust wurde 2002 errichtet und ist eine Einrichtung der EU mit Sitz in Den Haag. Sie fördert die justizielle Zusammenarbeit bei Ermittlungen und Strafverfolgungsmaßnahmen im Zusammenhang mit schweren Straftaten, von denen mindestens zwei Mitgliedstaaten betroffen sind.⁸³³ Eurojust verfolgt folgende Ziele:

- Förderung und Verbesserung der Koordinierung von Ermittlungen und Strafverfolgungsmaßnahmen zwischen den zuständigen Behörden der Mitgliedstaaten;
- Erleichterung der Erledigung von Ersuchen und Entscheidungen im Bereich der justiziellen Zusammenarbeit.

Die Aufgaben von Eurojust werden von nationalen Mitgliedern wahrgenommen. Jeder Mitgliedstaat entsendet einen Richter oder Staatsanwalt zu Eurojust, die hinsichtlich ihres Status dem nationalen Recht ihres Mitgliedstaats

830 a.a.O., Artikel 48.

831 a.a.O., Artikel 50.

832 a.a.O., Artikel 51.

833 Rat der Europäischen Union (2002), Beschluss 2002/187/JI des Rates vom 28. Februar 2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität, ABl. L 63 vom 6.3.2002; Rat der Europäischen Union (2003), Beschluss 2003/659/JI des Rates vom 18. Juni 2003 zur Änderung des Beschlusses 2002/187/JI über die Errichtung von Eurojust zur Bekämpfung der schweren Kriminalität, ABl. L 245 vom 29.9.2003; Rat der Europäischen Union (2009), Beschluss 2009/426/JI des Rates vom 16. Dezember 2008 zur Stärkung von Eurojust und zur Änderung des Beschlusses 2002/187/JI über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität, ABl. L 138 vom 4.6.2009 (Eurojust-Beschlüsse).

unterliegen und mit den erforderlichen Kompetenzen ausgestattet sind, um die Aufgaben wahrzunehmen, die für die Förderung und Verbesserung der justiziellen Zusammenarbeit erforderlich sind. Darüber hinaus werden die nationalen Mitglieder bei der Durchführung spezieller Aufgaben von Eurojust als Kollegium tätig.

Eurojust darf personenbezogene Daten verarbeiten, sofern dies für das Erreichen ihrer Ziele erforderlich ist. Dies ist allerdings auf spezifische Informationen über Personen beschränkt, die im Verdacht stehen, eine Straftat begangen zu haben oder an einer Straftat beteiligt gewesen zu sein, oder die wegen einer Straftat verurteilt wurden, für die Eurojust zuständig ist. Eurojust darf auch bestimmte Daten über Zeugen oder Opfer von Straftaten verarbeiten, die in die Zuständigkeit von Eurojust fallen.⁸³⁴ In Ausnahmefällen darf Eurojust für begrenzte Zeit umfangreichere personenbezogene Daten über Tatumstände verarbeiten, wenn sie für die laufenden Ermittlungen unmittelbar von Belang sind. Innerhalb ihres Zuständigkeitsbereichs darf Eurojust mit anderen Organen, Einrichtungen und Agenturen der EU zusammenarbeiten und mit ihnen personenbezogene Daten austauschen. Eurojust darf auch mit Drittländern und Organisationen zusammenarbeiten und mit ihnen personenbezogene Daten austauschen.

Bezüglich des Datenschutzes muss Eurojust ein Datenschutzniveau gewährleisten, das zumindest den Grundsätzen des Modernisierten Übereinkommens Nr. 108 und dessen späteren Änderungen gleichwertig ist. Beim Datenaustausch sind besondere Vorschriften und Einschränkungen einzuhalten, die entweder in Vereinbarungen über die Zusammenarbeit oder in Arbeitsvereinbarungen gemäß den Eurojust-Beschlüssen und den Eurojust-Datenschutzvorschriften niedergelegt sind.⁸³⁵

Bei Eurojust wurde eine unabhängige gemeinsame Kontrollinstanz (GKI) eingerichtet, deren Aufgabe die Überwachung der von Eurojust vorgenommenen Verarbeitungen personenbezogener Daten ist. Sind Personen mit der Entscheidung von Eurojust über ein Ersuchen um Auskunft, Berichtigung, Sperrung oder Löschung personenbezogener Daten nicht zufrieden, können sie bei der GKI Beschwerde einlegen. Wenn Eurojust personenbezogene Daten

834 Konsolidierte Fassung des Beschlusses 2002/187/JI des Rates, geändert durch den Beschluss 2003/659/JI des Rates und den Beschluss 2009/426/JI des Rates, Artikel 15 Absatz 2.

835 Bestimmungen der Geschäftsordnung betreffend die Verarbeitung und den Schutz personenbezogener Daten bei Eurojust, ABl. C 68 vom 19.3.2005, S. 1.

rechtswidrig verarbeitet, haftet Eurojust nach dem innerstaatlichen Recht des Mitgliedstaats, in dem sie ihren Sitz hat, also der Niederlande, für den der betroffenen Person entstandenen Schaden.

Ausblick

Im Juli 2013 legte die Europäische Kommission einen Vorschlag für eine Verordnung zur Reform von Eurojust vor. Dieser Vorschlag wurde von einem Vorschlag zur Einrichtung einer Europäischen Staatsanwaltschaft begleitet (siehe unten). Diese Verordnung zielt auf die Modernisierung der Aufgaben und der Struktur von Eurojust ab, um diese an den Vertrag von Lissabon anzupassen. Darüber hinaus zielt die Reform auf eine klare Trennung der vom Eurojust-Kollegium durchgeführten operativen Aufgaben von Eurojust und ihren Verwaltungsaufgaben ab. Auf diese Weise können sich die Mitgliedstaaten in stärkerem Maße auf die operativen Aufgaben konzentrieren. Ein neuer Exekutivausschuss wird eingerichtet, der das Kollegium bei der Durchführung der Verwaltungsaufgaben unterstützt.⁸³⁶

Europäische Staatsanwaltschaft

Die Mitgliedstaaten verfügen über die ausschließliche Zuständigkeit für die strafrechtliche Verfolgung der Straftaten des Betrugs und der missbräuchlichen Verwendung des EU-Haushalts, die auch grenzüberschreitende Auswirkungen haben können. Die strafrechtliche Untersuchung und Verfolgung sowie die Anklageerhebung in Bezug auf die Täter solcher Straftaten wird insbesondere in Anbetracht der anhaltenden Wirtschaftskrise zunehmend wichtiger.⁸³⁷ Die Europäische Kommission unterbreitete einen Vorschlag für eine Verordnung über die Errichtung einer unabhängigen Europäischen Staatsanwaltschaft (EUSTA)⁸³⁸ zur Bekämpfung von gegen die finanziellen Interessen der EU gerichteten Straftaten. Die Errichtung der EUSTA erfolgt über das Verfahren der verstärkten Zusammenarbeit, wonach mindestens neun Mitgliedstaaten in einem Bereich innerhalb der EU-Strukturen eine verstärkte Zusammenarbeit ohne Beteiligung der übrigen EU-Länder begründen können.⁸³⁹ Belgien, Bulgarien,

836 Siehe die [Eurojust-Website](#) der Europäischen Kommission.

837 Siehe Europäische Kommission (2013), Vorschlag für eine Verordnung des Rates über die Errichtung der Europäischen Staatsanwaltschaft, COM(2013) 0534 final, Brüssel, 17. Juli 2013, S. 1 und die [EUSTA-Website](#) der Kommission.

838 Europäische Kommission (2013), Vorschlag für eine Verordnung des Rates über die Errichtung der Europäischen Staatsanwaltschaft, COM(2013) 0534 final, Brüssel, 17. Juli 2013.

839 Vertrag über die Arbeitsweise der EU, Artikel 86 Absatz 1 und Artikel 329 Absatz 1.

Kroatien, Zypern, die Tschechische Republik, Estland, Finnland, Frankreich, Deutschland, Griechenland, Lettland, Litauen, Luxemburg, Portugal, Rumänien, Slowenien, die Slowakei und Spanien sind der Verstärkten Zusammenarbeit beigetreten; Österreich und Italien haben ihren geplanten Beitritt zum Ausdruck gebracht.⁸⁴⁰

Die EUSTa wird für die Ermittlung und Verfolgung von Betrug und anderen Straftaten zuständig sein, die sich gegen die finanziellen Interessen der EU richten und dabei auf die wirksame Koordinierung der Ermittlungen und Strafverfolgungsmaßnahmen in den verschiedenen nationalen Rechtsordnungen und auf die Verbesserung des Ressourceneinsatzes und des Informationsaustauschs auf europäischer Ebene abzielen.⁸⁴¹

An der Spitze der EUSTa wird ein Europäischer Staatsanwalt stehen und in jedem Mitgliedstaat wird es mindestens einen Abgeordneten Europäischen Staatsanwalt geben, dem die Durchführung der Ermittlungen und Strafverfolgungsmaßnahmen in diesem Mitgliedstaat obliegt.

Der Vorschlag enthält starke Garantien zur Gewährleistung der im nationalen Recht, im EU-Recht und in der Charta der Grundrechte der EU festgesetzten Rechte der von den Ermittlungen der EUSTa betroffenen Personen. Für Ermittlungsmaßnahmen, die hauptsächlich die Grundrechte berühren, ist eine vorherige Genehmigung seitens eines nationalen Gerichts erforderlich.⁸⁴² Die Ermittlungen der EUSTa unterliegen einer gerichtlichen Kontrolle seitens der nationalen Gerichte.⁸⁴³

Auf die seitens der EUSTa durchgeführte Verarbeitung verwaltungstechnischer personenbezogener Daten wird die Datenschutzverordnung für die EU-Organe⁸⁴⁴ Anwendung finden. Für die Verarbeitung personenbezogener Daten im

840 Siehe Rat der Europäischen Union (2017), „*20 Mitgliedstaaten einigen sich über Einzelheiten bei der Errichtung der Europäischen Staatsanwaltschaft*“, Pressemitteilung, 8. Juni 2017.

841 Europäische Kommission (2013), Vorschlag für eine Verordnung des Rates über die Errichtung der Europäischen Staatsanwaltschaft, COM(2013) 0534 final, Brüssel, 17. Juli 2013, S. 1 und S. 51. Siehe die [EUSTa-Website](#) der Kommission.

842 Europäische Kommission (2013), Vorschlag für eine Verordnung des Rates über die Errichtung der Europäischen Staatsanwaltschaft, COM(2013) 0534 final, Brüssel, 17. Juli 2013, Artikel 26 Absatz 4.

843 a.a.O., Artikel 36.

844 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001.

Zusammenhang mit operativen Angelegenheiten wie Europol wird die EUSa eine eigene Datenschutzregelung bekommen, die der Datenschutzregelung für die Tätigkeiten von Europol und Eurojust ähnelt, da die Ausübung der Aufgaben der EUSa die Verarbeitung personenbezogener Daten mit Strafverfolgungsbehörden auf Ebene der Mitgliedstaaten umfassen wird. Folglich sind die Datenschutzvorschriften der EUSa nahezu identisch mit den Vorschriften der Datenschutzrichtlinie für Polizei und Strafjustiz. Nach Maßgabe des Vorschlags für die Errichtung der EUSa, muss die Verarbeitung personenbezogener Daten die Grundsätze der Rechtmäßigkeit, Fairness, Zweckbindung, Datenminimierung, Richtigkeit, Integrität und Vertraulichkeit einhalten. Wenn möglich muss die EUSa zwischen den personenbezogenen Daten der verschiedenen Arten von betroffenen Personen klar unterscheiden, wie zwischen den Daten von Personen, die aufgrund einer Straftat verurteilt sind, von Personen, die lediglich verdächtigt werden, von Opfern und von Zeugen. Sie muss sich auch um die Überprüfung der Qualität der personenbezogenen Daten bemühen und wenn möglich auf Tatsachen beruhende personenbezogene Daten von personenbezogenen Daten unterscheiden, die auf persönlichen Einschätzungen beruhen.

Der Vorschlag enthält Bestimmungen in Bezug auf die Rechte der betroffenen Personen und insbesondere über das Recht auf Information, auf Einsicht in ihre personenbezogenen Daten, auf Berichtigung, Löschung und Verarbeitungseinschränkung, und sieht vor, dass diese Rechte auch indirekt über den EDSB ausgeübt werden können. Er enthält auch die Grundsätze der Sicherheit der Verarbeitung und der Rechenschaftspflicht, die erfordern, dass die EUSa geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines den Verarbeitungsrisiken entsprechenden Sicherheitsniveaus umsetzt, sämtliche Verarbeitungstätigkeiten schriftlich festhält und in Fällen, in denen eine Verarbeitungsart wahrscheinlich ein hohes Risiko für die Rechte der Personen mit sich bringt (beispielsweise bei Verarbeitungen unter Einsatz neuer Technologien), vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführt. Schließlich sieht der Vorschlag die seitens des Kollegiums erfolgende Ernennung eines Datenschutzbeauftragten vor, der in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird und gewährleistet, dass die EUSa die geltenden Datenschutzvorschriften einhält.

8.3.2. Datenschutz in den gemeinsamen Informationssystemen auf EU-Ebene

Über den Datenaustausch zwischen Mitgliedstaaten und die Errichtung von Fachbehörden der EU für die Bekämpfung der grenzüberschreitenden Kriminalität wie Europol, Eurojust und die EUSTa hinaus wurden auf EU-Ebene mehrere gemeinsame Informationssysteme eingerichtet, um die Zusammenarbeit und den Informationsaustausch zwischen den zuständigen nationalen Behörden und der EU für spezifische Zwecke in den Bereichen Grenzschutz, Einwanderung und Asyl und Zollwesen zu ermöglichen und zu erleichtern. Da der Schengen-Raum zunächst über ein internationales Abkommen geschaffen wurde, das unabhängig vom EU-Recht Anwendung fand, entstand das Schengener Informationssystem (SIS) aus multilateralen Abkommen, die später dem EU-Recht unterstellt wurden. Das Visa-Informationssystem (VIS), Eurodac, Eurosur und das Zollinformationssystem (ZIS) wurden als Instrumente errichtet, die dem EU-Recht unterlagen.

Die Aufsicht über diese Systeme teilen sich die nationalen Aufsichtsbehörden und der EDSB. Zur Gewährleistung eines hohen Schutzniveaus arbeiten diese Behörden in Bezug auf die nachstehenden IT-Großsysteme im Rahmen von Koordinierungsgruppen für die Aufsicht (SCGs) zusammen: 1) Eurodac; 2) Visa-Informationssystem; 3) Schengener Informationssystem; 4) Zollinformationssystem und 5) Binnenmarkt-Informationssystem.⁸⁴⁵ Die SCGs treffen sich normalerweise zweimal jährlich unter der Leitung eines gewählten Vorsitzenden und erlassen Leitlinien, diskutieren über grenzüberschreitende Rechts-sachen oder nehmen gemeinsame Rahmen für Überwachungen an.

Die 2012 eingerichtete Europäische Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA)⁸⁴⁶ ist für das Betriebsmanagement des Schengener Informationssystems der zweiten Generation (SIS II), des Visa-Informationssystems (VIS) und von Eurodac zuständig. Hauptaufgabe von eu-LISA ist es, den effektiven, sicheren und kontinuierlichen Betrieb der Informationstechnologiesysteme zu gewährleisten. Weiter ist die Agentur dafür verantwortlich, mit den erforderlichen Maßnahmen für die Sicherheit der Systeme und die Sicherheit von Daten zu sorgen.

⁸⁴⁵ Siehe die [Website über die Koordination der Aufsicht](#) des Europäischen Datenschutzbeauftragten.

⁸⁴⁶ Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ABl. L 286 vom 1.11.2011.

Das Schengener Informationssystem

1985 traten mehrere Mitgliedstaaten der damaligen Europäischen Gemeinschaft dem Übereinkommen zwischen den Staaten der Benelux-Wirtschaftsunion, Deutschland und Frankreich über den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen (Schengener Übereinkommen) bei, mit dem ein Raum der Freizügigkeit geschaffen werden sollte, ohne behindernde Grenzkontrollen innerhalb des Schengen-Hoheitsgebiets.⁸⁴⁷ Als Gegengewicht zur Bedrohung der öffentlichen Sicherheit, die nach der Öffnung der Grenzen entstehen konnte, wurden schärfere Grenzkontrollen an den Außengrenzen des Schengen-Gebiets sowie eine enge Zusammenarbeit zwischen nationalen Polizei- und Justizbehörden eingerichtet.

Als Folge des Beitritts weiterer Staaten zum Schengener Übereinkommen wurde das Schengen-System schließlich mit dem Vertrag von Amsterdam vollständig in den EU-Rechtsrahmen überführt.⁸⁴⁸ Die Umsetzung dieser Entscheidung erfolgte 1999. Die neueste Version des Schengener Informationssystems, das so genannte SIS II, ging am 9. April 2013 in Betrieb. Es gilt nunmehr in den meisten EU-Mitgliedstaaten,⁸⁴⁹ sowie Island, Liechtenstein, Norwegen und der Schweiz.⁸⁵⁰ Auch Europol und Eurojust haben Zugriff auf SIS II.

SIS II besteht aus einer zentralen Unterstützungseinheit (C.SIS), einem nationalen Teil (N.SIS) in jedem Mitgliedstaat sowie einer Kommunikationsinfrastruktur zwischen der zentralen Unterstützungseinheit und den nationalen Teilen. Die C.SIS enthält bestimmte Daten zu Personen und Gegenständen, die von den Mitgliedstaaten eingegeben werden. Das SIS wird von nationalen Grenzschutzbehörden, Polizei, Zoll, Visa- und Justizbehörden im gesamten Schengen-Raum benutzt. In jedem Mitgliedstaat ist eine nationale Kopie der C.SIS in Betrieb,

847 Übereinkommen zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen, ABl. L 239 vom 22.9.2000.

848 Europäische Gemeinschaften (1997), Vertrag von Amsterdam zur Änderung des Vertrags über die Europäische Union, die Verträge zur Gründung der Europäischen Gemeinschaften sowie einiger damit zusammenhängender Rechtsakte, ABl. C 340 vom 10.22.1997.

849 Kroatien, Zypern und Irland bereiten sich auf den Beitritt zu SIS II vor, gehören diesem aber noch nicht an. Siehe die Informationen zum Schengener Informationssystem auf der [Website der Generaldirektion Migration und Inneres der Europäischen Kommission](#).

850 Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 381 vom 28.12.2006, und Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Errichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 205 vom 7.8.2007.

auch bezeichnet als nationale Teile des Schengener Informationssystems (N.SIS), die laufend aktualisiert werden und damit auch die C.SIS auf den neuesten Stand bringen. Es gibt verschiedene Arten von Alarm/Warnungen im SIS:

- die Person ist nicht befugt, in das Schengen-Hoheitsgebiet einzureisen oder sich dort aufzuhalten, oder
- die Person oder der Gegenstand werden von Justiz- oder Strafverfolgungsbehörden gesucht (z. B. Europäischer Haftbefehl, Antrag auf verdeckte Kontrolle), oder
- die Person wurde als vermisst gemeldet, oder
- Waren wie Banknoten, Autos, Lieferwagen, Feuerwaffen und Identitätsdokumente wurden als gestohlen oder verloren gemeldet.

Im Falle einer Warnung müssen von den SIRENE-Büros Folgemaßnahmen veranlasst werden. SIS II weist neue Funktionalitäten auf: Es können jetzt beispielsweise biometrische Daten wie Fingerabdrücke und Fotos eingegeben werden; es gibt neue Alarmkategorien wie gestohlene Boote, Flugzeuge, Container oder Zahlungsmittel; es gibt verschärfte Ausschreibungen für Personen und Gegenstände und Kopien Europäischer Haftbefehle von Personen, die zur Festnahme, Übergabe oder Auslieferung gesucht werden.

SIS II gründet auf zwei einander ergänzenden Rechtsakten: dem SIS II-Beschluss⁸⁵¹ und der SIS II-Verordnung.⁸⁵² Zum Erlass des Beschlusses und der Verordnung verwendete der EU-Gesetzgeber unterschiedliche Rechtsgrundlagen. Der Beschluss regelt die Verwendung von SIS II zu Zwecken der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (die frühere dritte Säule der EU). Die Verordnung findet auf Ausschreibungsverfahren statt, die unter Visa-, Asyl-, Einwanderungs- und sonstige Maßnahmen im Zusammenhang mit dem freien Personenverkehr fallen (die frühere erste Säule). Die Ausschreibungsverfahren für jede Säule mussten durch gesonderte Rechtsakte geregelt werden, da die beiden Rechtsakte vor dem Vertrag von Lissabon und der Abschaffung der Säulenstruktur erlassen wurden.

851 Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 205 vom 7.8.2007.

852 Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 381 vom 28.12.2006.

Beide Rechtsakte enthalten Vorschriften zum Datenschutz. Der SIS II-Beschluss verbietet die Verarbeitung sensibler Daten.⁸⁵³ Die Verarbeitung personenbezogener Daten unterliegt dem Anwendungsbereich des Modernisierten Übereinkommens Nr. 108.⁸⁵⁴ Darüber hinaus haben die Personen das Recht auf Auskunft über die sie betreffenden und im SIS II gespeicherten personenbezogenen Daten.⁸⁵⁵

Die SIS II-Verordnung regelt die Bedingungen und Verfahren zur Eingabe und Verarbeitung von Ausschreibungen in Bezug auf Einreise- oder Aufenthaltsverweigerungen von Nicht-EU-Bürgern. Sie enthält auch Vorschriften für den Austausch von Zusatzinformationen und ergänzenden Daten zum Zwecke der Einreise oder des Aufenthalts in einem Mitgliedstaat.⁸⁵⁶ Diese Verordnung enthält auch Vorschriften zum Datenschutz. Sensible Datenkategorien im Sinne von Artikel 9 Absatz 1 der DSGVO dürfen nicht verarbeitet werden.⁸⁵⁷ Die SIS II-Verordnung enthält auch bestimmte Rechte für die betroffenen Personen:

- das Recht auf Auskunft über personenbezogene Daten zur betroffenen Person;⁸⁵⁸
- das Recht auf Berichtigung sachlich unrichtiger Daten;⁸⁵⁹
- das Recht auf Löschung unrechtmäßig gespeicherter Daten;⁸⁶⁰ und
- das Recht auf Information über Ausschreibungen in Bezug auf die betroffene Person. Diese Information wird schriftlich zusammen mit einer Abschrift der oder unter Angabe der der Ausschreibung zugrunde liegenden innerstaatlichen Entscheidung übermittelt.⁸⁶¹

Das Recht auf Information findet keine Anwendung, wenn 1) die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden und die Information

853 SIS II-Beschluss, Artikel 56; SIS II-Verordnung, Artikel 40.

854 SIS II-Beschluss, Artikel 57.

855 SIS II-Beschluss, Artikel 58; SIS II-Verordnung, Artikel 41.

856 SIS II-Beschluss, Artikel 2.

857 SIS II-Verordnung, Artikel 40.

858 *a.a.O.*, Artikel 41 Absatz 1.

859 *a.a.O.*, Artikel 41 Absatz 5.

860 *a.a.O.*, Artikel 41 Absatz 5.

861 *a.a.O.*, Artikel 42 Absatz 1.

unmöglich ist oder unverhältnismäßigen Aufwand erfordern würde, 2) die betroffene Person bereits über die Information verfügt oder 3) wenn das nationale Recht unter anderem auf Grundlage des Schutzes der nationalen Sicherheit oder der Verhütung von Straftaten eine Einschränkung vorsieht.⁸⁶²

Sowohl gemäß des SIS II-Beschlusses als auch gemäß der SIS II-Verordnung können die Auskunftsrechte der Personen in Bezug auf SIS II in jedem Mitgliedstaat ausgeübt werden und werden nach dem Recht des betreffenden Mitgliedstaats behandelt.⁸⁶³

Beispiel: In der Rechtssache *Dalea gegen Frankreich*⁸⁶⁴ wurde dem Beschwerdeführer ein Visum für Frankreich verweigert, weil die französischen Behörden dem Schengener Informationssystem gemeldet hatten, es solle ihm die Einreise verweigert werden. Der Beschwerdeführer beantragte ohne Erfolg zunächst bei der französischen Datenschutzkommission und dann beim Staatsrat Auskunft über die Daten sowie deren Berichtigung oder Löschung. Nach Auffassung des EGMR war die Meldung des Beschwerdeführers an das Schengener Informationssystem rechtmäßig und diente dem rechtmäßigen Ziel des Schutzes der nationalen Sicherheit. Da der Beschwerdeführer nicht nachgewiesen hatte, wie er tatsächlich unter der verweigerten Einreise in den Schengen-Raum gelitten hatte, und da ausreichende Vorkehrungen zu seinem Schutz vor willkürlichen Entscheidungen bestanden, war der Eingriff in sein Recht auf Achtung des Privatlebens verhältnismäßig gewesen. Die Beschwerde des Beschwerdeführers unter Artikel 8 wurde daher für unzulässig erklärt.

Die zuständige nationale Kontrollinstanz in jedem Mitgliedstaat überwacht den innerstaatlichen N.SIS. Die nationale Kontrollinstanz gewährleistet, dass die Datenverarbeitungsvorgänge im innerstaatlichen N.SIS mindestens alle vier Jahre überprüft werden.⁸⁶⁵ Die nationalen Kontrollinstanzen und der EDSB arbeiten zusammen und gewährleisten eine koordinierte Überwachung des N.SIS, während der EDSB für die Überwachung der C.SIS zuständig ist. Aus Gründen der Transparenz wird dem Europäischen Parlament, dem Rat und eu-LISA alle zwei Jahre ein gemeinsamer Tätigkeitsbericht übermittelt. Zur Gewährleistung der Koordinierung der Aufsicht über SIS wurde die Koordinierungsgruppe für die Aufsicht über SIS II (SCG SIS II)

⁸⁶² a.a.O., Artikel 42 Absatz 2.

⁸⁶³ SIS II-Verordnung, Artikel 41 Absatz 1 und SIS II-Beschluss, Artikel 58.

⁸⁶⁴ EGMR, *Dalea / Frankreich*, Nr. 964/07, 2. Februar 2010.

⁸⁶⁵ SIS II-Beschluss, Artikel 60 Absatz 2.

eingerrichtet, die zweimal jährlich zusammentritt. Diese Gruppe besteht aus dem EDSB und Vertretern der nationalen Kontrollinstanzen der Mitgliedstaaten, die SIS II umgesetzt haben, sowie der nationalen Kontrollinstanzen von Island, Liechtenstein, Norwegen und der Schweiz, da das SIS für sie als Schengen-Mitglieder ebenfalls Anwendung findet.⁸⁶⁶ Zypern, Kroatien und Irland nehmen noch nicht am SIS II teil und sind daher in der SCG lediglich als Beobachter vertreten. Im Rahmen der SCG arbeiten der EDSB und die nationalen Kontrollinstanzen durch den Austausch von Informationen, die gegenseitige Unterstützung bei der Durchführung von Prüfungen und Inspektionen, die Ausarbeitung harmonisierter Vorschläge im Hinblick auf gemeinsame Lösungen für etwaige Probleme und die Förderung der Sensibilisierung für die Datenschutzrechte aktiv zusammen.⁸⁶⁷ Die SIS II SCG erlässt auch Leitlinien zur Unterstützung der betroffenen Personen. Ein Beispiel ist der Leitfaden zur Unterstützung der betroffenen Personen bei der Ausübung ihrer Auskunftsrechte.⁸⁶⁸

Ausblick

2016 führte die Europäische Kommission eine Evaluierung des SIS durch⁸⁶⁹, die gezeigt hat, dass es nationale Mechanismen dafür gibt, dass die betroffenen Personen Auskunft über die Daten erhalten, die über sie im SIS II gespeichert sind, und dass sie im Fall von unrichtigen Daten die Berichtigung oder Löschung dieser Daten erwirken oder Schadensersatz erlangen können. Zur Verbesserung der Leistungsfähigkeit und Wirksamkeit des SIS unterbreitete die Europäische Kommission Vorschläge für drei Verordnungen:

- eine Verordnung über die Einrichtung, den Betrieb und die Nutzung des SIS im Bereich der Grenzkontrollen, die die SIS II-Verordnung außer Kraft setzen wird;
- eine Verordnung über die Einrichtung, den Betrieb und die Nutzung des SIS im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, die unter anderem den SIS II-Beschluss außer Kraft setzen wird;
- eine Verordnung über die Nutzung des SIS zur Rückführung illegal-bleibender Drittstaatsangehöriger.

866 Siehe die [Website über das Schengener Informationssystem](#) des Europäischen Datenschutzbeauftragten.

867 SIS II-Verordnung, Artikel 46 und SIS II-Beschluss, Artikel 62.

868 Siehe SIS II SCG, *The Schengen Information System. A guide for exercising the right of access*, abrufbar auf der Website des EDSB.

869 Bericht der Kommission an das Europäische Parlament und den Rat über die Evaluierung des Schengener Informationssystems der zweiten Generation (SIS II) nach den Artikeln 24 Absatz 5, 43 Absatz 3 und 50 Absatz 5 der Verordnung (EG) Nr. 1987/2006 in Verbindung mit Artikel 59 Absatz 3 und Artikel 66 Absatz 5 des Beschlusses 2007/533/JI, COM(2016) 880 final.

Wichtig ist, dass die Vorschläge die Verarbeitung anderer Kategorien biometrischer Daten erlauben – zusätzlich zu Lichtbildern und Fingerabdrücken, die bereits in der gegenwärtigen SIS II-Regelung enthalten sind. Auch Gesichtsbilder, Handballenabdrücke und DNA-Profile werden in der SIS-Datenbank gespeichert. Während die SIS II-Verordnung und der SIS II-Beschluss die Möglichkeit vorsahen, die Identität einer Person über Fingerabdrücke zu ermitteln, machen die Vorschläge diese Ermittlung darüber hinaus obligatorisch, sofern die Identität der Person auf keine andere Art bestimmt werden kann. Sobald dies technisch möglich ist, werden Gesichtsbilder, Lichtbilder und Handballenabdrücke zur Durchsuchung des Systems und zur Identifizierung von Personen eingesetzt. Die neuen Vorschriften zu den biometrischen Kennzeichen stellen besondere Risiken für die Rechte der Personen dar. In seiner Stellungnahme zu den Vorschlägen der Kommission⁸⁷⁰ wies der EDSB darauf hin, dass biometrische Daten in hohem Maße schutzwürdig sind und ihre Eingabe in eine so groß angelegte Datenbank auf einer auf klare Fakten gestützten Beurteilung der Erfordernisse ihrer Aufnahme in das SIS beruhen sollte. Anders ausgedrückt sollte das Erfordernis der Verarbeitung der neuen Kennzeichen nachgewiesen werden. Der EDSB war auch der Auffassung, dass noch näher zu klären wäre, welche Arten von Informationen in das DNA-Profil aufgenommen werden können. Da das DNA-Profil sensible Informationen enthalten kann (das augenfälligste Beispiel wären Informationen zu gesundheitlichen Aspekten), sollten die im SIS gespeicherten Informationen „nur das Mindestmaß an Informationen enthalten [...], das für eine Identifizierung der Vermissten unbedingt erforderlich ist, und Angaben zur Gesundheit, zur rassischen Herkunft und alle anderen sensiblen Informationen ausdrücklich ausgenommen werden.“⁸⁷¹ Die Vorschläge führen jedoch zusätzliche Garantien ein, um die Erhebung und weitere Verarbeitung von Daten auf das absolut notwendige und in operativer Hinsicht erforderliche Maß zu begrenzen und den Zugriff auf diese personenbezogenen Daten auf Personen zu beschränken, die sie verarbeiten müssen.⁸⁷² Überdies ermächtigen diese Vorschläge eu-LISA zur regelmäßigen Erstellung von Datenqualitätsberichten und zu deren Übermittlung an die Mitgliedstaaten, um Ausschreibungen regelmäßig zu überprüfen und die Datenqualität zu gewährleisten.⁸⁷³

870 EDSB (2017), Stellungnahme des EDSB zur neuen Rechtsgrundlage für das Schengener Informationssystem, Stellungnahme 7/2017, 2. Mai 2017.

871 *a.a.O.*, Absatz 22.

872 Europäische Kommission (2016), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung der Verordnung (EU) Nr. 515/2014 und zur Aufhebung der Verordnung (EG) Nr. 1986/2006, des Beschlusses 2007/533/JI des Rates und des Beschlusses 2010/261/EU der Kommission, COM (2016) 883 final, Brüssel, 21. Dezember 2016.

873 *a.a.O.*, S. 15.

Das Visa-Informationssystem

Das Visa-Informationssystem (VIS), das ebenfalls von eu-LISA betrieben wird, wurde zur Unterstützung der Durchführung einer gemeinsamen Visa-Politik der EU entwickelt.⁸⁷⁴ Mithilfe des VIS können Schengen-Staaten Daten über Visabewerber über ein komplett zentralisiertes System austauschen, das die Konsulate und Botschaften der Schengen-Staaten in Drittländern mit den Grenzübergangsstellen an den Außengrenzen aller Schengen-Staaten verbindet. Das VIS verarbeitet Daten über Anträge auf Visa für einen kurzfristigen Aufenthalt beim Besuch im oder der Durchreise durch den Schengen-Raum. Das VIS gibt den Grenzbehörden die Möglichkeit, anhand biometrischer Kennzeichen und insbesondere Fingerabdrücken zu überprüfen, ob die Person, die das Visum vorlegt, dessen rechtmäßiger Inhaber ist, und Personen ohne Dokumente oder mit gefälschten Dokumenten zu identifizieren.

Die Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) regelt die Bedingungen und Verfahren für die Übermittlung personenbezogener Daten über Anträge auf Erteilung eines Visums für einen kurzfristigen Aufenthalt. Sie überwacht auch die über die Anträge getroffenen Entscheidungen, einschließlich der Entscheidung zur Annullierung, zur Aufhebung oder zur Verlängerung des Visums.⁸⁷⁵ Die VIS-Verordnung umfasst in erster Linie Daten über den Antragsteller, dessen Visa, Fotos, Fingerabdrücke, Verknüpfungen zu früheren Anträgen, und die Antragsdatensätze der ihn begleitenden Personen oder Daten über die Personen, die ihn eingeladen haben.⁸⁷⁶ Der Zugriff auf das VIS für Zwecke der Eingabe, Änderung oder Löschung von Daten ist ausschließlich auf die Visabehörden beschränkt, während ein Zugriff zum Zweck der Datenabfrage für Visabehörden und Behörden, die für Kontrollen an den Grenzübergangsstellen an den Außengrenzen, Einwanderungskontrollen und Asyl zuständig sind, vorgesehen ist.

874 Rat der Europäischen Union (2004), Entscheidung 2004/512/EG des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS), ABl. L 213 vom 15.6.2004; Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt, ABl. L 218 vom 13.8.2008 (VIS-Verordnung); Rat der Europäischen Union (2008), Beschluss 2008/633/JI vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008.

875 VIS-Verordnung, Artikel 1.

876 Artikel 5 der Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl. L 218 vom 13.8.2008.

Unter bestimmten Voraussetzungen können die zuständigen nationalen Polizeibehörden sowie Europol zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten Daten aus dem VIS abfragen.⁸⁷⁷ Da das VIS als Instrument zur Unterstützung der Durchführung der gemeinsamen Visumpolitik konzipiert wurde, würde dessen Umwandlung in ein Strafverfolgungsinstrument den Grundsatz der Zweckbindung verletzen, der – wie in [Abschnitt 3.2](#) erläutert – die ausschließliche Verarbeitung personenbezogener Daten für festgelegte, eindeutige und rechtmäßige Zwecke erfordert, und dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Aus diesem Grund wird den nationalen Strafverfolgungsbehörden und Europol kein routinemäßiger Zugriff auf die VIS-Datenbank gewährt. Sie erhalten nur im Einzelfall und unter Gewährleistung strenger Garantien Zugriff. Die Bedingungen und Garantien für den Zugang zum VIS und für Datenabfragen seitens dieser Behörden wurden im Beschluss 2008/633/JI des Rates geregelt.⁸⁷⁸

Darüber hinaus sieht die VIS-Verordnung Rechte der betroffenen Personen vor. Diese beinhalten:

- Das Recht, seitens des zuständigen Mitgliedstaats über die Identität und die Kontaktangaben des für die Verarbeitung personenbezogener Daten in diesem Mitgliedstaat zuständigen Verantwortlichen, die Zwecke der Datenverarbeitung im Rahmen des VIS, die Kategorien der Personen, an die die Daten übermittelt werden können (Empfänger) und die Aufbewahrungsfrist der Daten informiert zu werden. Darüber hinaus müssen die Visumantragsteller darüber informiert werden, dass die Erhebung ihrer personenbezogenen Daten im VIS für die Prüfung ihres Antrags vorgeschrieben ist. Die Mitgliedstaaten müssen sie überdies über das Bestehen ihres Auskunftsrechts bezüglich ihrer Daten informieren und über das Recht zur Beantragung ihrer Berichtigung oder Löschung sowie über die Verfahren zur Ausübung dieser Rechte.⁸⁷⁹
- Das Recht auf Auskunft über die im VIS gespeicherten und sie betreffenden personenbezogenen Daten.⁸⁸⁰

877 Rat der Europäischen Union (2008); Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008.

878 a.a.O.

879 VIS-Verordnung, Artikel 37.

880 a.a.O., Artikel 38 Absatz 1.

- Das Recht auf Berichtigung unrichtiger Daten.⁸⁸¹
- Das Recht auf Löschung unrechtmäßig gespeicherter Daten.⁸⁸²

Zur Gewährleistung der Kontrolle des VIS wurde die Koordinierungsgruppe für die Aufsicht über das VIS (VIS SCG) eingerichtet. Diese besteht aus Vertretern des EDSB und der nationalen Kontrollstellen und trifft sich zweimal jährlich. Diese Gruppe umfasst die Vertreter der 28 EU-Mitgliedstaaten und die Vertreter Islands, Liechtensteins, Norwegens und der Schweiz.

Eurodac

Eurodac steht für europäische Daktyloskopie. Es handelt sich um ein zentralisiertes System mit Fingerabdruckdaten von Drittstaatsangehörigen und Staatenlosen, die in einem der EU-Mitgliedstaaten Asyl beantragen.⁸⁸³ Das System ist seit der im Januar 2003 erfolgten Annahme der Verordnung (EG) Nr. 2725/2000 in Betrieb, deren Neufassung 2015 Anwendung fand. Der Hauptzweck des Systems besteht darin, bei der Bestimmung des Mitgliedstaats zu helfen, der gemäß der Verordnung (EG) Nr. 604/2013 für die Prüfung eines bestimmten Asylantrags zuständig ist. Die genannte Verordnung legt die Kriterien und Verfahren zur Bestimmung des Mitgliedstaats fest, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist

881 *a.a.O.*, Artikel 38 Absatz 2.

882 *a.a.O.*, Artikel 38 Absatz 2.

883 Siehe die [Eurodac-Website](#) des Europäischen Datenschutzbeauftragten; Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl. L 316 vom 15.12.2000; Verordnung (EG) Nr. 407/2002 des Rates vom 28. Februar 2002 zur Festlegung von Durchführungsbestimmungen zur Verordnung (EG) Nr. 2725/2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl. L 62 vom 5.3.2002 (Eurodac-Verordnungen); Verordnung (EG) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europol auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ABl. L 180 vom 29.6.2013, S. 1 (Neufassung der Eurodac-Verordnung).

(Dublin III-Verordnung).⁸⁸⁴ Personenbezogene Daten in Eurodac dienen in erster Linie der Erleichterung der Anwendung der Dublin III-Verordnung.⁸⁸⁵

Die nationalen Strafverfolgungsbehörden und Europol können Fingerabdrücke im Zusammenhang mit strafrechtlichen Ermittlungen zum alleinigen Zwecke der Verhütung, Aufdeckung oder Ermittlung von terroristischen Straftaten oder anderen schweren Straftaten mit den in Eurodac enthaltenen Fingerabdrücken abgleichen. Da Eurodac als Instrument zur Unterstützung der Umsetzung der Asylpolitik der EU und nicht als Strafvollstreckungsinstrument konzipiert wurde, haben Strafverfolgungsbehörden nur in bestimmten Fällen und unter strengen Voraussetzungen Zugriff auf die Datenbank.⁸⁸⁶ Auf die Weiterverwendung der Daten zu Strafverfolgungszwecken findet die Datenschutzrichtlinie für Polizei und Strafjustiz Anwendung, während Daten, die hauptsächlich zum Zweck der Erleichterung der Anwendung der Dublin III-Verordnung verwendet werden, nach Maßgabe der DSGVO geschützt sind. Die Weiterübermittlung von seitens eines Mitgliedstaats oder Europol nach Maßgabe der Neufassung der Eurodac-Verordnung erhaltenen personenbezogenen Daten an einen Drittstaat, eine internationale Organisation oder eine private Stelle innerhalb oder außerhalb der Union ist verboten.⁸⁸⁷

Eurodac umfasst eine von eu-LISA betriebene Zentraleinheit für die Speicherung und den Abgleich von Fingerabdrücken und ein System für die elektronische Datenübermittlung zwischen den Mitgliedstaaten und der zentralen Datenbank. Die Mitgliedstaaten nehmen von jeder Person über 14 Jahren, die in ihrem Hoheitsgebiet Asyl beantragt, und von jedem Drittstaatsangehörigen oder Staatenlosen über 14 Jahren, der bei einem illegalen Übertritt ihrer Außengrenze aufgegriffen wird, Fingerabdrücke ab und übermitteln sie. Die Mitgliedstaaten dürfen auch Fingerabdrücke von Drittstaatsangehörigen oder Staatenlosen nehmen und übermitteln, die sich ohne Genehmigung in ihrem Hoheitsgebiet aufhalten.

884 Verordnung (EU) Nr. 604/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist, ABl. L 180 vom 29.6.2013 (Dublin III-Verordnung).

885 Neufassung der Eurodac-Verordnung, ABl. L 180 vom 29.6.2013, S. 1, Artikel 1 Absatz 1.

886 a.a.O., Artikel 1 Absatz 2.

887 a.a.O., Artikel 35.

Obgleich jeder Mitgliedstaat Eurodac abfragen und um Abgleiche mit Fingerabdrucksdaten ersuchen kann, ist nur der Mitgliedstaat, der die Fingerabdrücke erhoben und an die Zentraleinheit übermittelt hat, dazu berechtigt, die Daten durch Berichtigung oder Ergänzung zu verändern oder sie zu löschen.⁸⁸⁸ Zur Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit fertigt die eu-LISA über alle Datenverarbeitungsvorgänge Aufzeichnungen an.⁸⁸⁹ Die nationalen Kontrollstellen unterstützen und beraten die betroffenen Personen bei der Wahrnehmung ihrer Rechte.⁸⁹⁰ Die Erhebung und Übermittlung von Fingerabdruckdaten unterliegt der gerichtlichen Überprüfung seitens der nationalen Gerichte.⁸⁹¹ Verarbeitungsvorgänge der Zentraleinheit, die in Bezug auf Eurodac von eu-LISA verwaltet wird, unterliegen der Datenschutzverordnung für die EU-Organe⁸⁹² und der Kontrolle durch den EDSB.⁸⁹³ Sollte einer Person durch eine rechtswidrige Verarbeitung oder durch eine andere Handlung, die der Eurodac-Verordnung zuwiderläuft, ein Schaden entstanden sein, so hat sie das Recht, von dem für den Schaden verantwortlichen Mitgliedstaat Schadenersatz zu verlangen.⁸⁹⁴ Diesbezüglich ist jedoch hervorzuheben, dass es sich bei Asylbewerbern um eine besonders verletzbare Gruppe von Menschen handelt, die oftmals lange und gefährliche Reisen durchgeführt haben. Aufgrund ihrer Verletzlichkeit und der prekären Lage, in der sie sich während der Prüfung ihres Asylantrags häufig befinden, kann sich die Ausübung ihrer Rechte einschließlich des Rechts auf Schadenersatz als schwierig erweisen.

Um Eurodac zu Strafverfolgungszwecken verwenden zu können, müssen die Mitgliedstaaten die zugangsberechtigten Behörden benennen, sowie die Behörden, die überprüfen, ob die Abgleichsanträge rechtmäßig sind.⁸⁹⁵ Nationale Behörden und Europol erhalten nur unter sehr strengen Voraussetzungen Zugriff auf die Fingerabdruckdaten von Eurodac. Erst nachdem

888 a.a.O., Artikel 27.

889 a.a.O., Artikel 28.

890 a.a.O., Artikel 29.

891 a.a.O., Artikel 29.

892 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001.

893 Neufassung der Eurodac-Verordnung, ABl. L 180 vom 29.6.2013, S. 1, Artikel 31.

894 a.a.O., Artikel 37.

895 Roots, L. (2015), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination“, *Baltic Journal of European Studies Tallinn University of Technology*, Vol. 5, Nr. 2, S. 108–129.

die abfragende Behörde die Daten mit den Daten in anderen verfügbaren Informationssystemen wie nationalen Fingerabdruckdatenbanken und dem VIS abgeglichen hat, reicht die antragstellende Behörde einen begründeten Antrag in elektronischer Form ein. Damit der Abgleich verhältnismäßig ist, muss ein überwiegendes öffentliches Sicherheitsinteresse bestehen. Der Abgleich muss wahrhaft erforderlich sein, sich auf einen Einzelfall beziehen und es müssen hinreichende Gründe zu der Annahme vorliegen, dass der Abgleich wesentlich zur Verhütung, Aufdeckung oder Ermittlung einer der in Rede stehenden Straftaten beitragen wird, insbesondere wenn der begründete Verdacht besteht, dass der Verdächtige, der Täter oder das Opfer einer terroristischen Straftat oder sonstiger schwerer Straftaten einer Personenkategorie zugeordnet werden kann, die der Erhebung von Fingerabdrücken im Rahmen des Eurodac-Systems unterliegt. Der Abgleich ist ausschließlich auf Fingerabdruckdaten beschränkt. Europol muss auch die Zustimmung des Mitgliedstaats einholen, der die Fingerabdruckdaten erfasst hat.

In Eurodac gespeicherte personenbezogene Daten über Asylbewerber werden ab dem Datum der Abnahme der Fingerabdrücke zehn Jahre aufbewahrt, sofern die betroffene Person nicht die Staatsbürgerschaft eines EU-Mitgliedstaats erwirbt. In diesem Fall sind die Daten unverzüglich zu löschen. Daten über Ausländer, die beim unerlaubten Übertritt über die Außengrenze aufgegriffen werden, werden 18 Monate gespeichert. Diese Daten sind unverzüglich zu löschen, wenn die betroffene Person eine Aufenthaltsgenehmigung erhält, das EU-Hoheitsgebiet verlässt oder die Staatsangehörigkeit eines Mitgliedstaats erwirbt. Die Daten der Personen, denen Asyl gewährt wurde, bleiben über einen Zeitraum von drei Jahren für den Abgleich im Rahmen der Verhütung, Aufdeckung oder Ermittlung von terroristischen Straftaten oder anderen schweren Straftaten verfügbar.

Neben allen EU-Mitgliedstaaten setzen auch Island, Norwegen, Liechtenstein und die Schweiz Eurodac auf der Grundlage internationaler Abkommen ein.

Zur Gewährleistung der Überwachung von Eurodac wurde die Koordinierungsgruppe für die Aufsicht über Eurodac (Eurodac SCG) eingerichtet. Diese besteht aus Vertretern des EDSB und der nationalen Kontrollstellen und trifft sich zweimal jährlich. Diese Gruppe umfasst die Vertreter der 28 EU-Mitgliedstaaten und die Vertreter Islands, Liechtensteins, Norwegens und der Schweiz.⁸⁹⁶

⁸⁹⁶ Siehe die [Eurodac-Website](#) des Europäischen Datenschutzbeauftragten.

Ausblick

Im Mai 2016 veröffentlichte die Kommission einen Vorschlag für einen neuen Entwurf der Eurodac-Verordnung als Teil einer Reform zur Verbesserung der Funktionsweise des Gemeinsamen Europäischen Asylsystems (GEAS).⁸⁹⁷ Die vorgeschlagene Neufassung ist wichtig, da sie den Anwendungsbereich der ursprünglichen Eurodac-Datenbank erheblich ausweiten wird. Anfänglich wurde Eurodac zur Unterstützung der Umsetzung des GEAS errichtet und stellte Fingerabdruckdaten zur Bestimmung des für die Prüfung eines in der EU gestellten Asylantrags zuständigen Mitgliedstaats bereit. Die vorgeschlagene Neufassung wird den Anwendungsbereich der Datenbank ausweiten, um die Rückführung irregulärer Migranten zu erleichtern.⁸⁹⁸ Die nationalen Behörden werden die Datenbank zur Identifizierung von Drittstaatsangehörigen abfragen können, die sich irregulär in der EU aufhalten oder irregulär in die EU eingereist sind, um den diesbezüglichen Beweis zu erhalten und die Mitgliedstaaten bei der Rückführung dieser Personen zu unterstützen. Während die gegenwärtige Rechtsregelung lediglich die Erfassung und Speicherung von Fingerabdrücken erfordert, führt der Vorschlag darüber hinaus die Erfassung von Gesichtsbildern der Personen vor,⁸⁹⁹ bei denen es sich um eine andere Art biometrischer Daten handelt. Der Vorschlag würde auch das Mindestalter der Kinder, deren biometrische Daten erfasst werden können, von 14 Jahren in der Verordnung aus dem Jahr 2013 auf sechs Jahre verringern⁹⁰⁰. Der ausgeweitete Anwendungsbereich des Vorschlags bedeutet, dass mehr Personen in die Datenbank aufgenommen werden

897 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „Eurodac“ für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der [Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist], für die Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europol auf den Abgleich mit Eurodac-Daten (Neufassung), COM(2016) 272 final, 4. Mai 2016.

898 Siehe die Begründung des Vorschlags, S. 3.

899 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „Eurodac“ für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der [Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist], für die Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europol auf den Abgleich mit Eurodac-Daten (Neufassung), COM(2016) 272 final, 4. Mai 2016, Artikel 2 Absatz 1.

900 a.a.O., Artikel 2 Absatz 2.

können und er demnach für eine größere Anzahl von Personen einen Eingriff in die Rechte auf Privatsphäre und Datenschutz darstellen wird. Zum Ausgleich dieses Eingriffs bemühen sich der Vorschlag und die seitens des LIBE-Ausschusses des Europäischen Parlaments vorgeschlagenen Änderungsanträge⁹⁰¹ um die Verschärfung der Datenschutzaufgaben. Zum Zeitpunkt der Abfassung des vorliegenden Handbuchs wurde im Parlament und im Rat noch über den Vorschlag diskutiert.

Eurosur

Mit dem Europäischen Grenzüberwachungssystem (Eurosur)⁹⁰² soll die Kontrolle an den Außengrenzen des Schengen-Raums durch die Aufdeckung, Verhütung und Bekämpfung von illegaler Einwanderung und grenzüberschreitender Kriminalität verstärkt werden. Es dient der Verstärkung des Informationsaustauschs und der operativen Zusammenarbeit zwischen nationalen Koordinierungszentren und Frontex, der EU-Agentur, die für die Entwicklung und Anwendung des neuen Konzepts der integrierten Grenzverwaltung zuständig ist.⁹⁰³ Zu seinen allgemeinen Zielsetzungen gehört:

- die Verringerung der Zahl illegaler Migranten, die unentdeckt in die EU kommen;
- die Verringerung der Zahl der Todesfälle bei illegalen Migranten durch verstärkte Rettung des Lebens auf See;

901 Europäisches Parlament, [Bericht](#) über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der [Verordnung (EU) Nr. 604/2013] zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist, für die Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europol auf den Abgleich mit Eurodac-Daten (Neufassung), PE 597.620v03-00, 9. Juni 2017.

902 Verordnung (EG) Nr. 1052/2013 des Europäischen Parlaments und des Rates vom 22. Oktober 2013 zur Errichtung eines Europäischen Grenzüberwachungssystems (Eurosur), ABl. L 295 vom 6.11.2013.

903 Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates vom 14. September 2016 über die Europäische Grenz- und Küstenwache und zur Änderung der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Verordnung (EG) Nr. 863/2007 des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 2007/2004 des Rates und der Entscheidung des Rates 2005/267/EG (ABl. L 251 vom 16.9.2016).

- Verbesserung der inneren Sicherheit der EU insgesamt durch einen Beitrag zur Prävention grenzüberschreitender Kriminalität.⁹⁰⁴

Eurosur nahm seine Tätigkeit in allen Mitgliedstaaten mit Außengrenzen am 2. Dezember 2013 auf und in den anderen Mitgliedstaaten am 1. Dezember 2014. Die Verordnung gilt für die Überwachung der Land-, See- und Luftaußengrenzen der Mitgliedstaaten. Der Austausch und die Verarbeitung personenbezogener Daten ist bei Eurosur sehr beschränkt, da die Mitgliedstaaten und Frontex lediglich Schiffsidentifizierungsnummern austauschen dürfen. Eurosur tauscht operative Informationen wie den Standort von Patrouillen und Störfällen aus, und in der Regel dürfen die ausgetauschten Informationen keine personenbezogenen Daten enthalten.⁹⁰⁵ In den Ausnahmefällen, in denen im Rahmen von Eurosur personenbezogene Daten ausgetauscht werden, sieht die Verordnung vor, dass der allgemeine EU-Rechtsrahmen für den Datenschutz vollständig Anwendung findet.⁹⁰⁶

Demnach gewährleistet Eurosur das Recht auf Datenschutz, indem es besagt, dass der Austausch personenbezogener Daten mit den in der Datenschutzrichtlinie für Polizei und Strafjustiz und der DSGVO festgesetzten Kriterien und Garantien übereinstimmen muss.⁹⁰⁷

Zollinformationssystem

Ein weiteres wichtiges gemeinsames Informationssystem auf EU-Ebene ist das Zollinformationssystem (ZIS).⁹⁰⁸ Im Zuge der Errichtung des Binnenmarktes wur-

904 Siehe ferner: Europäische Kommission (2008), Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Prüfung der Schaffung eines Europäischen Grenzkontrollsystems (Eurosur), COM(2008) 68 final, Brüssel, 13. Februar 2008; Europäische Kommission (2011), Folgenabschätzung zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Europäischen Grenzüberwachungssystems (Eurosur), Arbeitsunterlage der Kommissionsdienststellen, SEC(2011) 1536 final, Brüssel, 12. Dezember 2011, S. 18.

905 Europäische Kommission, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29. November 2013.

906 Verordnung (EU) Nr. 1052/2013, Erwägungsgrund 13 und Artikel 13.

907 a.a.O., Erwägungsgrund 13 und Artikel 13.

908 Rat der Europäischen Union (1995), Rechtsakt des Rates vom 26. Juli 1995 über die Fertigstellung des Übereinkommens über den Einsatz der Informationstechnologie im Zollbereich, ABl. C 316 vom 27.11.1995, geändert durch Rat der Europäischen Union (2009), Verordnung (EG) Nr. 515/97 des Rates vom 13. März 1997 über die gegenseitige Amtshilfe zwischen Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und der Agrarregelung, Beschluss 2009/917/JI des Rates vom 30. November 2009 über den Einsatz der Informationstechnologie im Zollbereich, ABl. L 323 vom 10.12.2009 (ZIS-Beschluss).

den alle Kontrollen und Formalitäten im Zusammenhang mit dem Warenverkehr im EU-Hoheitsgebiet abgeschafft, woraus sich ein gesteigertes Betrugsrisiko ergab. Als Gegengewicht zu diesem Risiko wurde die Zusammenarbeit zwischen den Zollverwaltungen der Mitgliedstaaten intensiviert. Zweck des CIS ist es, die Mitgliedstaaten bei der Verhinderung, Ermittlung oder Verfolgung von schweren Zuwiderhandlungen gegen die innerstaatlichen und die EU-Rechtsvorschriften in den Bereichen Zoll und Landwirtschaft zu unterstützen. Das ZIS wurde durch zwei Rechtsakte errichtet, deren Erlass auf verschiedenen Rechtsgrundlagen gründete: Die Verordnung (EG) Nr. 515/97 des Rates betrifft die Zusammenarbeit zwischen den verschiedenen nationalen Verwaltungsbehörden zur Betrugsbekämpfung im Rahmen der Zollunion und der gemeinsamen Agrarpolitik, während der Beschluss 2009/917/JI des Rates auf die Verhinderung, Ermittlung und Verfolgung von schweren Zuwiderhandlungen gegen die Zollgesetze abzielt. Dies bedeutet, dass das ZIS nicht nur die Strafverfolgung betrifft.

Die im ZIS gespeicherten Informationen enthalten personenbezogene Daten mit Bezug auf Waren, Transportmittel, Unternehmen, Personen, zurückgehaltene, beschlagnahmte oder eingezogene Waren und Barmittel. Die Datenkategorien, die verarbeitet werden können, sind klar festgelegt und umfassen die Namen, die Staatsangehörigkeit, das Geschlecht, den Geburtsort und das Geburtsdatum der betroffenen Personen, die Gründe für die Aufnahme ihrer Daten in das System und das amtliche Kennzeichen des Transportmittels.⁹⁰⁹ Diese Daten dürfen nur zum Zwecke der Feststellung und Unterrichtung oder zur Durchführung besonderer Kontrollen oder für strategische oder operative Analysen von Personen verwendet werden, die des Verstoßes gegen Zollbestimmungen verdächtig werden.

Zugriff auf das ZIS haben die nationalen Zoll-, Steuer-, Landwirtschafts-, öffentlichen Gesundheits- und Polizeibehörden sowie Europol und Eurojust.

Bei der Verarbeitung personenbezogener Daten sind die entsprechenden Bestimmungen in der Verordnung (EG) Nr. 515/97 und im Beschluss 2009/917/JI des Rates sowie die Bestimmungen der DSGVO, der Datenschutzverordnung für die EU-Organe, des Modernisierten Übereinkommens Nr. 108 und der Polizei-Empfehlung einzuhalten. Mit der Verordnung (EG) Nr. 45/2001 ist der EDSB zuständig für die Kontrolle der Einhaltung des ZIS. Er beruft mindestens einmal pro Jahr ein Treffen mit allen nationalen Datenschutzaufsichtsbehörden ein, die zuständig für ZIS-bezogene Aufsichtsfragen sind.

909 Siehe ZIS-Beschluss, Artikel 4.

Interoperabilität zwischen den Informationssystemen der EU

Die Migrationssteuerung, das integrierte Grenzmanagement der EU-Außengrenzen und die Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität stellen große Herausforderungen dar und sind in einer globalisierten Welt zu zunehmend komplexeren Themen geworden. In den vergangenen Jahren arbeitete die EU an einem neuen umfassenden Ansatz zum Schutz und zur Aufrechterhaltung der Sicherheit ohne Gefährdung der Werte und Grundfreiheiten der EU. In diesem Zusammenhang ist ein wirksamer Informationsaustausch zwischen den nationalen Strafverfolgungsbehörden und zwischen den Mitgliedstaaten und den entsprechenden EU-Agenturen von entscheidender Bedeutung.⁹¹⁰ Die bestehenden Informationssysteme der EU für das Grenzmanagement und die innere Sicherheit verfügen über ihre jeweiligen Ziele, institutionellen Strukturen, betroffenen Personen und Nutzer. Die EU arbeitet daran, Mängel in den Funktionsweisen einer zersplitterten EU-Datenverwaltung durch die Analyse des Interoperabilitätspotentials zwischen den verschiedenen Informationssystemen wie SIS II, VIS und Eurodac zu beseitigen.⁹¹¹ Hauptziel ist es, sicherzustellen, dass den zuständigen Polizei-, Zoll- und Justizbehörden die regelmäßig die erforderlichen Informationen zur Durchführung ihrer Aufgaben bereitstehen, und gleichzeitig ein Gleichgewicht in Bezug auf die Rechte auf Privatsphäre, Datenschutz und andere Grundrechte beibehalten wird.

910 Europäische Kommission (2016), Mitteilung der Kommission an das Europäische Parlament und den Rat: Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit, COM(2016) 205 final, Brüssel, 6. April 2016; Europäische Kommission (2016), Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat: Mehr Sicherheit in einer von Mobilität geprägten Welt: Besserer Informationsaustausch bei der Terrorismusbekämpfung und ein stärkerer Schutz der Außengrenzen, COM(2016) 602 final, Brüssel, 14. September 2016; Europäische Kommission (2016), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger, COM(2016) 881 final, Brüssel, 21. Dezember 2016. Siehe auch Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament und den Rat: Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Siebter Fortschrittsbericht, COM(2017) 261 final, Brüssel, 16. Mai 2017.

911 Rat der Europäischen Union (2005), Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, ABl. C 53 vom 3.3.2005; Europäische Kommission (2010), Mitteilung der Kommission an das Europäische Parlament und den Rat: Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht, COM(2010) 385 final; Europäische Kommission (2016), Mitteilung der Kommission an das Europäische Parlament und den Rat: Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit, COM(2016) 205 final, Brüssel, 6. April 2016; Europäische Kommission (2016), Beschluss der Kommission vom 17. Juni 2016 zur Einsetzung der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität, ABl. C 257 vom 15.7.2016.

Unter Interoperabilität versteht man „die Fähigkeit von Informationssystemen, Daten auszutauschen und die gemeinsame Nutzung von Informationen zu ermöglichen“.⁹¹² Dieser Austausch darf die durch die DSGVO, die Datenschutzrichtlinie für Polizei und Strafjustiz, die Charta der Grundrechte der EU und alle sonstigen einschlägigen Vorschriften garantierten und notwendigerweise strengen Zugangs- und Verwendungsbestimmungen nicht gefährden. Keine integrierte Lösung für die Datenverarbeitung darf die Grundsätze der Zweckbindung, des Datenschutzes durch Technik oder des Datenschutzes durch datenschutzfreundliche Voreinstellungen beeinträchtigen.⁹¹³

Zusätzlich zur Verbesserung der Funktionsweisen der drei Hauptinformationssysteme SIS II, VIS und Eurodac hat die Kommission die Einrichtung eines vierten zentralen Grenzmanagementsystems für Drittstaatsangehörige vorgeschlagen. Dabei handelt es sich um das Einreise-/Ausreisensystem (EES),⁹¹⁴ dessen Umsetzung bis 2020 geplant ist.⁹¹⁵ Überdies hat die Kommission einen Vorschlag über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS)⁹¹⁶ veröffentlicht, das Informationen über Personen erfasst, die ohne Visum in die EU einreisen, um Vorabkontrollen in Bezug auf illegale Einreise und Sicherheit durchführen zu können.

912 Europäische Kommission (2016), Mitteilung der Kommission an das Europäische Parlament und den Rat: Solidere und intelligendere Informationssysteme für das Grenzmanagement und mehr Sicherheit, COM(2016) 205 final, 6. April 2016, S. 14.

913 a.a.O., S. 4–5.

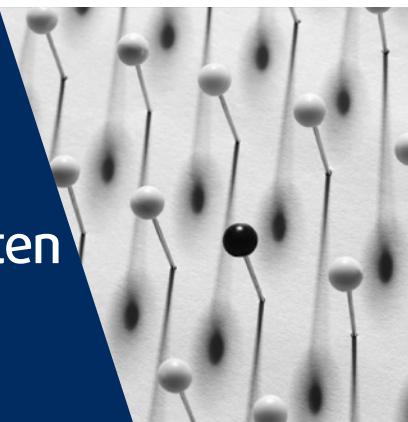
914 Europäische Kommission (2016), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Einreise-/Ausreisensystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung der Verordnung (EG) Nr. 767/2008 und der Verordnung (EU) Nr. 1077/2011, COM(2016) 194 final.

915 Europäische Kommission (2016), Mitteilung der Kommission an das Europäische Parlament und den Rat: Solidere und intelligendere Informationssysteme für das Grenzmanagement und mehr Sicherheit, COM(2016) 205 final, 6. April 2016, S. 5.

916 Europäische Kommission (2016), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/794 und (EU) 2016/1624, COM(2016) 731 final.

9

Besondere Arten von Daten und ihre entsprechenden Datenschutzvorschriften



EU	Behandelte Themen	Europarat
DSGVO Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie 2002/58/EG)	Elektronische Kommunikation	Modernisiertes Übereinkommen Nr. 108 Empfehlung betreffend Telekommunikationsdienste
DSGVO, Artikel 89	Beschäftigtenkontext	Modernisiertes Übereinkommen Nr. 108 Empfehlung für den Beschäftigtenkontext EGMR, <i>Copland / Vereinigtes Königreich</i> , Nr. 62617/00, 2007
DSGVO, Artikel 9 Absatz 2 Buchstabe h und i	Medizinische Daten	Modernisiertes Übereinkommen Nr. 108 Empfehlung betreffend medizinische Daten EGMR, <i>Z / Finnland</i> , Nr. 22009/93, 1997
Verordnung über klinische Prüfungen	Klinische Prüfungen	
DSGVO, Artikel 6 Absatz 4, Artikel 89	Statistiken	Modernisiertes Übereinkommen Nr. 108 Empfehlung betreffend statistische Daten

EU	Behandelte Themen	Europarat
Verordnung (EG) Nr. 223/2009 über europäische Statistiken EuGH, C-524/06, <i>Huber / Bundesrepublik Deutschland</i> [GK], 2008	Amtliche Statistiken	Modernisiertes Übereinkommen Nr. 108 Empfehlung betreffend statistische Daten
Richtlinie 2014/65/EU über Märkte für Finanzinstrumente Verordnung (EU) Nr. 648/2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister Verordnung (EG) Nr. 1060/2009 über Ratingagenturen Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt	Finanzdaten	Modernisiertes Übereinkommen Nr. 108 Empfehlung 90(19) für Zahlungszwecke und andere verwandte Operationen EGMR, <i>Michaud / Frankreich</i> , Nr. 12323/11, 2012

Mehrfach wurden auf europäischer Ebene spezifische Rechtsakte angenommen, mit denen die allgemeinen Vorschriften des Modernisierten Übereinkommens Nr. 108 oder der DSGVO in detaillierterer Form für spezielle Situationen umgesetzt wurden.

9.1. Elektronische Kommunikation

Kernpunkte

- Spezifische Vorschriften für den Datenschutz im Bereich Telekommunikation unter besonderer Berücksichtigung von Telefondiensten finden sich in der Empfehlung des Europarates aus dem Jahr 1995.
- Die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung von Kommunikationsdiensten auf EU-Ebene ist in der Datenschutzrichtlinie für elektronische Kommunikation geregelt.
- Die Vertraulichkeit der elektronischen Kommunikation bezieht sich nicht nur auf den Inhalt einer Kommunikation, sondern auch auf Metadaten, also Informationen darüber, wer mit wem, wann und wie lange kommuniziert hat, und auf Ortsdaten, also Informationen darüber, von wo aus Daten kommuniziert wurden.

Kommunikationsdienste verfügen über ein größeres Potenzial für unberechtigte Eingriffe in die persönliche Sphäre der Nutzer, da sie leistungsfähige technische Möglichkeiten für das Abhören und Überwachen der über solche Netze durchgeführten Kommunikationen bieten. Daher wurden besondere Datenschutzbestimmungen für notwendig erachtet, um die besonderen Risiken für die Nutzer von Kommunikationsdiensten anzugehen.

1995 gab der **Europarat** eine Empfehlung zum Schutz personenbezogener Daten im Bereich der Fernmeldedienste, namentlich im Hinblick auf die Telefondienste, heraus.⁹¹⁷ Nach dieser Empfehlung sollten die Zwecke der Erhebung und Verarbeitung personenbezogener Daten im Bereich der Fernmeldedienste beschränkt sein auf: den Anschluss eines Nutzers an das Netz, die Bereitstellung des betreffenden Fernmeldedienstes, die Abrechnung, die Überprüfung, die Gewährleistung eines optimalen technischen Betriebs und den Ausbau von Netz und Diensten.

Besondere Aufmerksamkeit galt ferner der Nutzung von Kommunikationsnetzen für die Versendung von Direktwerbenachrichten. Generell dürfen Direktwerbenachrichten nicht an einen Teilnehmer gesandt werden, der deren Empfang ausdrücklich abgelehnt hat. Anrufautomaten für die Übermittlung zuvor aufgezeichneter Werbenachrichten dürfen nur zum Einsatz kommen, wenn ein Teilnehmer dem ausdrücklich zugestimmt hat. Spezifischere Regeln für diesen Bereich sind im innerstaatlichen Recht festzulegen.

Im EU-Recht wurde nach einem ersten Versuch im Jahr 1997 die Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) 2002 angenommen und 2009 mit dem Ziel geändert, die Bestimmungen der früheren Datenschutzrichtlinie zu ergänzen und auf den Telekommunikationssektor zuzuschneiden.⁹¹⁸

917 Europarat, Ministerkomitee (1995), Empfehlung Rec(95)4 an die Mitgliedstaaten zum Schutz personenbezogener Daten im Bereich der Fernmeldedienste, namentlich im Hinblick auf die Telefondienste; 7. Februar 1995.

918 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und die Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden, ABl. L 337 vom 9.12.2004.

Die Anwendung der Datenschutzrichtlinie für elektronische Kommunikation ist auf Kommunikationsdienste in öffentlichen elektronischen Netzen beschränkt.

In der Datenschutzrichtlinie für elektronische Kommunikation wird zwischen drei Hauptkategorien von Daten unterschieden, die im Verlauf einer Kommunikation generiert werden:

- die Daten, die den Inhalt der während der Kommunikation übermittelten Nachrichten ausmachen; diese Daten unterliegen absoluter Vertraulichkeit;
- die Daten, die für die Herstellung und Aufrechterhaltung der Kommunikation erforderlich sind, so genannte Metadaten, die in der Richtlinie als „Verkehrsdaten“ bezeichnet sind, wie Informationen über die Kommunikationspartner, Zeitpunkt und Dauer der Kommunikation;
- in der Kategorie der Metadaten gibt es Daten, die sich spezifisch auf den Standort des Kommunikationsgeräts beziehen, so genannte Ortungsdaten; diese Daten sind gleichzeitig auch Daten über den Standort der Nutzer der Kommunikationsgeräte, insbesondere wenn es sich dabei um Nutzer mobiler Kommunikationsgeräte handelt.

Verkehrsdaten dürfen vom Diensteanbieter nur für Abrechnungszwecke und für die technische Bereitstellung des Dienstes verarbeitet werden. Mit Einwilligung der betroffenen Person dürfen diese Daten jedoch an andere Verantwortliche weitergegeben werden, die weitere Mehrwertdienste anbieten, wie z. B. die Angabe der dem Standort des Nutzers nächsten U-Bahnstation oder Apotheke oder auch die Wettervorhersage für diesen Standort.

Anderer Zugriff auf Daten über Kommunikation in elektronischen Netzwerken muss gemäß Artikel 15 der ePrivacy-Richtlinie den Anforderungen an einen rechtmäßigen Eingriff in das Recht auf Datenschutz genügen, wie es in Artikel 8 Absatz 2 EMRK ausgeführt ist und in Artikel 8 und 52 der Charta der Grundrechte der EU bekräftigt wurde. Solche Zugriffe können etwa für strafrechtliche Ermittlungen erfolgen.

Die Änderungen der Datenschutzrichtlinie für elektronische Kommunikation von 2009 führten Folgendes ein:⁹¹⁹

- Die für den Versand von E-Mails zu Direktwerbezwecken geltenden Einschränkungen wurden auf SMS- und MMS-Dienste und ähnliche Anwendungen ausgedehnt; Werbe-E-Mails sind nur nach vorheriger Einwilligung zulässig. Ohne eine solche Einwilligung dürfen Werbe-E-Mails nur an Bestandskunden gesandt werden, wenn diese ihre E-Mail-Adresse angegeben haben und keinen Widerspruch erheben.
- Die Mitgliedstaaten wurden dazu verpflichtet, Rechtsbehelfe bei Verstößen gegen das Verbot unerbetener Nachrichten vorzusehen.⁹²⁰
- Das Setzen von Cookies, einer Software, die Handlungen eines Computernutzers überwacht und aufzeichnet, ist ohne Einwilligung des Computernutzers nicht länger erlaubt. Im einzelstaatlichen Recht sollte im Detail geregelt werden, wie eine Einwilligung zum Ausdruck gebracht und eingeholt werden sollte, um ausreichenden Schutz zu bieten.⁹²¹

Kommt es aufgrund eines unbefugten Zugriffs, des Verlusts oder der Zerstörung von Daten zu einem Verstoß gegen die Datenschutzvorschriften, ist die zuständige Aufsichtsbehörde unverzüglich zu benachrichtigen. Die Teilnehmer müssen darüber informiert werden, wenn ein möglicher Schaden für sie auf einen Verstoß gegen die Datenschutzvorschriften zurückgeht.⁹²²

919 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. L 241 vom 18.12.2009.

920 Siehe geänderte Richtlinie, Artikel 13.

921 Siehe a.a.O., Artikel 5; siehe ferner Artikel-29-Datenschutzgruppe (2012), *Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht*, WP 194, Brüssel, 7. Juni 2012

922 Siehe auch Artikel-29-Datenschutzgruppe (2011), *Arbeitsdokument 1/2011 über die EU-Regeln für Verstöße gegen die Datenschutzvorschriften mit Empfehlungen für zukünftige Politikentwicklungen*, WP 184, Brüssel, 5. April 2011.

Nach der Richtlinie über die Vorratsspeicherung von Daten⁹²³ waren Anbieter von Kommunikationsdiensten zur Speicherung von Metadaten verpflichtet. Diese Richtlinie wurde jedoch vom EuGH für ungültig erklärt (für weitere Einzelheiten siehe [Abschnitt 8.3](#)).

Ausblick

Im Januar 2017 nahm die Europäische Kommission einen neuen Vorschlag für eine ePrivacy-Verordnung an, die die alte ePrivacy-Richtlinie ersetzen soll. Ziel würde auch weiterhin der Schutz von „Grundrechten und Grundfreiheiten natürlicher und juristischer Personen bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste [...] [sein] und [...] insbesondere [...] [der Schutz der] Rechte auf Achtung des Privatlebens und der Kommunikation und [...] [der] Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“, unter gleichzeitiger Gewährleistung des freien Verkehrs elektronischer Kommunikationsdaten und elektronischer Kommunikationsdienste in der Union.⁹²⁴ Während die DSGVO in erster Linie Artikel 8 der Charta der Grundrechte der EU betrifft, will die vorgeschlagene Verordnung Artikel 7 der Charta im Sekundärrecht der EU verankern.

Die Verordnung würde die Bestimmungen der früheren Richtlinie an neue Technologien und die Marktwirklichkeit anpassen und zusammen mit der DSGVO einen umfassenden und einheitlichen Rahmen bilden. Somit wäre die ePrivacy-Verordnung *lex specialis* zur DSGVO und würde für elektronische Kommunikationsdaten gelten, die personenbezogene Daten darstellen. Die neue Verordnung umfasst die Verarbeitung von „elektronischen Kommunikationsdaten“ einschließlich elektronischer Kommunikationsinhalte und Metadaten, bei denen es sich nicht zwingenderweise um personenbezogene Daten handeln muss. Der räumliche Anwendungsbereich ist auf die EU beschränkt, schließt jedoch die außerhalb der EU erfolgende Verarbeitung von in der EU erhobenen Daten ein, und erstreckt sich auch auf Anbieter von Over-the-Top-Kommunikationsdiensten. Bei diesen handelt es sich um Diensteanbieter, die Inhalte, Dienste oder Anwendungen ohne die direkte Beteiligung

923 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.4.2006.

924 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, Artikel 1.

eines Netzbetreibers oder Internetdiensteanbieters über das Internet anbieten. Beispiele solcher Anbieter sind Skype (Sprach- und Videoanrufe), WhatsApp (Nachrichtenübermittlung), Google (Suche), Spotify (Musik) oder Netflix (Videoinhalte). Auf die neue Verordnung würden die Durchsetzungsmechanismen der DSGVO Anwendung finden.

Die Annahme der ePrivacy-Verordnung ist vor dem 25. Mai 2018 geplant, wenn die DSGVO in allen 28 Mitgliedstaaten Anwendung finden wird. Dies hängt jedoch von der Zustimmung des Europäischen Parlaments und des Rates ab.⁹²⁵

9.2. Beschäftigtendaten

Kernpunkte

- Spezifische Vorschriften für den Datenschutz im Beschäftigtenkontext finden sich in der Empfehlung des Europarates für den Beschäftigtenkontext.
- In der DSGVO werden Beschäftigtendaten konkret nur im Zusammenhang mit der Verarbeitung sensibler Daten erwähnt.
- Die Gültigkeit der Einwilligung, die freiwillig erteilt worden sein muss, als Rechtsgrundlage für die Verarbeitung der Daten über Arbeitnehmer kann angesichts des wirtschaftlichen Ungleichgewichts zwischen Arbeitgeber und Arbeitnehmern fragwürdig sein. Eine sorgfältige Prüfung der Umstände, unter denen die Einwilligung gegeben wurde, ist erforderlich.

Die Verarbeitung von Daten im Beschäftigtenkontext unterliegt den allgemeinen Rechtsvorschriften der EU zum Schutz personenbezogener Daten. Gleichwohl befasst sich eine Verordnung⁹²⁶ (unter anderem) speziell mit dem Schutz der Verarbeitung personenbezogener Daten durch die europäischen Organe im Beschäftigtenkontext. In der DSGVO wird in Artikel 9 Absatz 2 speziell auf Beschäftigungsverhältnisse eingegangen, und besagt, dass personenbezogene Daten im Rahmen der Ausübung der aus dem Arbeitsrecht erwachsenden Rechte und der Erfüllung der diesbezüglichen Pflichten des Verantwortlichen oder der betroffenen Person verarbeitet werden können.

⁹²⁵ Für weitere Informationen siehe Europäische Kommission (2017), „*Vorschlag der Kommission: noch besserer Schutz der Privatsphäre für die gesamte elektronische Kommunikation und moderne Datenschutzvorschriften für die EU-Organen*“, Pressemitteilung, 10. Januar 2017.

⁹²⁶ Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001.

Der DSGVO zufolge sollte dem Beschäftigten ermöglicht werden, die Daten, in deren Verarbeitung/Speicherung er freiwillig einwilligt und die Zwecke, für die die ihn betreffenden Daten gespeichert werden, eindeutig zu erkennen. Bevor die Beschäftigten ihre Einwilligung geben können, sollten sie auch über ihre Rechte und über die Speicherdauer der Daten unterrichtet werden. Sollte eine Verletzung des Schutzes personenbezogener Daten eintreten, die voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, benachrichtigt der Arbeitgeber den Beschäftigten über diese Verletzung. Artikel 88 der Verordnung erlaubt den Mitgliedstaaten die Festsetzung spezifischerer Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten der Beschäftigten in Bezug auf ihre personenbezogenen Daten im Beschäftigtenkontext.

Beispiel: In der Rechtssache *Worten*⁹²⁷ enthielten die Daten Aufzeichnungen über die Arbeitszeiten, die die täglichen Arbeits- und Ruhezeiten umfassten, bei denen es sich um personenbezogene Daten handelt. Die nationalen Rechtsvorschriften können einen Arbeitgeber dazu verpflichten, die Aufzeichnungen über die Arbeitszeiten der für die Überwachung der Arbeitsbedingungen zuständigen nationalen Behörde zur Verfügung zu stellen. Dies würde einen unverzüglichen Zugang zu den entsprechenden personenbezogenen Daten erlauben. Der Zugang zu den personenbezogenen Daten ist jedoch erforderlich, um der zuständigen Behörde die Überwachung der Regelungen über die Arbeitsbedingungen zu ermöglichen.⁹²⁸

Was den **Europarat** anbelangt, so wurde die Empfehlung des Europarates für den Beschäftigtenkontext 1989 veröffentlicht und 2015 überarbeitet.⁹²⁹ Die Empfehlung erstreckt sich auf die Verarbeitung personenbezogener Daten zu Beschäftigungszwecken im privaten und im öffentlichen Sektor. Die Verarbeitung muss bestimmte Grundsätze und Auflagen einhalten, darunter den Grundsatz der Transparenz und die Anhörung der Arbeitnehmervertreter, bevor Kontrollsysteme am Arbeitsplatz angebracht werden. Die Empfehlung sieht auch vor, dass die Arbeitgeber anstelle die Internetnutzung seitens der Beschäftigten zu überwachen, vorbeugende Maßnahmen wie beispielsweise Filter anwenden sollten.

927 EuGH, C-342/12, *Worten – Equipamentos para o Lar SA / Autoridade para as Condições de Trabalho (ACT)*, 30. Mai 2013, Randnr. 19.

928 a.a.O., Randnr. 43.

929 Europarat, Ministerkomitee (2015), Empfehlung Rec(2015)5 an die Mitgliedstaaten über die Verarbeitung personenbezogener Daten im Beschäftigtenkontext, April 2015.

Ein Überblick über die im Beschäftigtenkontext am häufigsten auftretenden Datenschutzprobleme findet sich in einer Stellungnahme der Artikel-29-Datenschutzgruppe.⁹³⁰ Die Datenschutzgruppe untersuchte die Bedeutung der Einwilligung als Rechtsgrundlage für die Verarbeitung von Daten von Beschäftigten.⁹³¹ Sie stellte fest, dass das wirtschaftliche Ungleichgewicht zwischen dem Arbeitgeber, der die Einwilligung verlangt, und dem Beschäftigten, der die Einwilligung gibt, oft Anlass zu Zweifeln gibt, ob die Einwilligung tatsächlich freiwillig gegeben wurde. Es sind daher bei der Beurteilung der Gültigkeit einer Einwilligung im Beschäftigtenkontext genau die Umstände zu betrachten, unter denen die Einwilligung als Rechtsgrundlage für die Verarbeitung herangezogen wird.

Ein in einem heutigen Arbeitsumfeld typisches und weit verbreitetes Datenschutzproblem ist das Ausmaß der rechtmäßigen Überwachung der elektronischen Kommunikation eines Beschäftigten an seinem Arbeitsplatz. Es wird häufig behauptet, dieses Problem ließe sich leicht durch ein Verbot der privaten Nutzung von Kommunikationseinrichtungen bei der Arbeit lösen. Ein solches allgemeines Verbot könnte sich jedoch als unverhältnismäßig und unrealistisch erweisen. Die Urteile des EGMR in den Rechtssachen *Copland gegen Vereinigtes Königreich* und *Bărbulescu gegen Rumänien* sind in diesem Zusammenhang besonders interessant.

Beispiel: In der Rechtssache *Copland gegen Vereinigtes Königreich*⁹³² war die Nutzung von Telefon, E-Mail und Internet durch eine College-Angestellte heimlich überwacht worden, um festzustellen, ob sie die Einrichtungen des Colleges übermäßig für private Zwecke nutzte. Der EGMR entschied, dass Telefongespräche aus dem Büro von der Definition Privatleben und Korrespondenz erfasst sind. Solche Anrufe und E-Mails, die vom Arbeitsplatz aus getätigt bzw. versendet werden, sowie Informationen aus der Überwachung der Internetnutzung für private Zwecke seien daher durch Artikel 8 EMRK geschützt. Im Falle der Beschwerdeführerin gab es keine Vorschriften, die besagten, unter welchen Umständen Arbeitgeber die Nutzung von Telefon, E-Mail und Internet durch Angestellte überwachen

930 Artikel-29-Datenschutzgruppe (2017), *Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz*, WP 249, Brüssel, 8. Juni 2017.

931 Artikel-29-Datenschutzgruppe (2005), Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114, Brüssel, 25. November 2005.

932 EGMR, *Copland / Vereinigtes Königreich*, Nr. 62617/00, 3. April 2007.

dürfen. Daher war der Eingriff nicht im Gesetz vorgesehen. Der Gerichtshof befand, dass eine Verletzung von Artikel 8 EMRK vorlag.

Beispiel: In der Rechtssache *Bărbulescu gegen Rumänien*⁹³³ ging es um einen rumänischen Vertriebsingenieur, dem wegen privater Chats über einen Messenger-Dienst gekündigt worden war. Sein Arbeitgeber überwachte seine Kommunikation. Die Aufzeichnungen, aus denen Nachrichten rein privater Natur hervorgingen, wurden im Zuge des Verfahrens vor dem innerstaatlichen Gericht vorgelegt. Der EGMR befand, dass Artikel 8 Anwendung finde und ließ die Frage offen, ob – und wenn ja, in welchem Ausmaß – die restriktiven Regelungen des Arbeitgebers den Beschwerdeführer in einer vernünftigen Erwartung auf Privatsphäre beließen, war jedoch der Ansicht, dass die Anweisungen eines Arbeitgebers das private soziale Leben am Arbeitsplatz nicht auf null reduzieren könnten.

In Bezug auf die materielle Rechtslage müsse den Vertragsstaaten ein großer Ermessensspielraum eingeräumt werden für die Beurteilung der Notwendigkeit zur Festsetzung eines Rechtsrahmens für die Voraussetzungen, unter denen ein Arbeitgeber die in elektronischer oder sonstiger Form erfolgende nicht berufliche Kommunikation seiner Arbeitnehmer am Arbeitsplatz regeln könne. Gleichwohl müssten die innerstaatlichen Behörden gewährleisten, dass die seitens eines Arbeitgebers erfolgende Einführung von Maßnahmen zur Überwachung der Korrespondenz und sonstigen Kommunikation unabhängig vom Umfang und von der Dauer dieser Maßnahmen von angemessenen und hinreichenden Garantien gegen Missbrauch begleitet ist. Verhältnismäßigkeit und Verfahrensgarantien gegen Willkür seien von entscheidender Bedeutung und der EGMR ermittelte eine Reihe von diesbezüglich maßgeblichen Faktoren. Dazu zählten beispielsweise der Umfang der Überwachung seitens des Arbeitgebers und das Ausmaß des Eindringens in die Privatsphäre des Arbeitnehmers, die Folgen für den Arbeitnehmer und ob angemessene Garantien gegen Willkür bereitgestellt wurden. Darüber hinaus müssten die innerstaatlichen Behörden sicherstellen, dass ein Arbeitnehmer, dessen Kommunikation überwacht wurde, Zugang zu einem Rechtsbehelf vor einem gerichtlichen Spruchkörper hat, der dafür zuständig ist, zumindest der Sache nach zu entscheiden, inwiefern die dargelegten Kriterien eingehalten wurden und ob die umstrittenen Maßnahmen rechtmäßig waren.

933 EGMR, *Bărbulescu / Rumänien* [GK], Nr. 61496/08, 5. September 2017, Randnr. 121.

Der EGMR stellte in dieser Rechtssache eine Verletzung von Artikel 8 fest, da die innerstaatlichen Behörden keinen angemessenen Schutz des Rechts des Beschwerdeführers auf Achtung seines Privatlebens und seiner Korrespondenz gewährt hatten und folglich verabsäumten, einen fairen Ausgleich zwischen den auf dem Spiel stehenden Interessen zu treffen.

Gemäß der Empfehlung für den Beschäftigtenkontext des Europarates sollten personenbezogene Daten, die für Beschäftigungszwecke erhoben werden, beim betreffenden Beschäftigten direkt erhoben werden.

Personenbezogene Daten, die bei der Einstellung erhoben werden, müssen sich auf die Informationen beschränken, die für die Bewertung der Eignung von Bewerbern und ihres Karrierepotenzials erforderlich sind.

In der Empfehlung werden auch ausdrücklich wertende Daten im Zusammenhang mit einer Beurteilung der Leistung oder des Potenzials eines bestimmten Beschäftigten erwähnt. Solche wertenden Daten müssen auf einer fairen und ehrlichen Bewertung gründen und dürfen nicht beleidigend formuliert sein. Dies erfordern die Grundsätze der Datenverarbeitung nach Treu und Glauben und der Richtigkeit der Daten.

Ein Sonderaspekt des Datenschutzes in der Beziehung zwischen Arbeitgeber und Arbeitnehmer ist die Funktion des Arbeitnehmervertreters. Solche Vertreter dürfen personenbezogene Daten von Beschäftigten nur insofern erhalten, als sie sie benötigen, um die Interessen der Beschäftigten zu vertreten oder sofern diese Daten zur Erfüllung oder Überwachung der in Kollektivvereinbarungen enthaltenen Verpflichtungen erforderlich sind.

Sensible personenbezogene Daten, die zu Beschäftigungszwecken erhoben werden, dürfen nur in besonderen Fällen und gemäß den im innerstaatlichen Recht niedergelegten Garantien verarbeitet werden. Arbeitgeber dürfen Beschäftigte oder Bewerber nach ihrem Gesundheitszustand nur dann befragen und sie ärztlich nur dann untersuchen lassen, wenn dies erforderlich ist, um ihre Eignung für den Arbeitsplatz festzustellen, Anforderungen der Präventivmedizin gerecht zu werden, die lebenswichtige Interessen der betroffenen Person oder anderer Beschäftigten und Personen zu schützen, Sozialleistungen zu gewähren oder gerichtliche Anfragen zu beantworten. Gesundheitsdaten dürfen nur bei dem betreffenden Beschäftigten selbst erhoben werden,

nicht bei anderen Quellen, es sei denn, es wurde eine ausdrückliche Einwilligung in Kenntnis der Sachlage erteilt oder es ist im innerstaatlichen Recht so vorgesehen.

Die Empfehlung für den Beschäftigtenkontext besagt, dass Beschäftigte über den Zweck der Verarbeitung ihrer personenbezogenen Daten, die Art der erhobenen personenbezogenen Daten, die Stellen, an die die Daten regelmäßig weitergegeben werden, und den Zweck und die Rechtsgrundlage einer solchen Offenlegung unterrichtet werden sollten. Auf elektronische Kommunikation darf am Arbeitsplatz ausschließlich aus Gründen der Sicherheit oder aus anderen rechtmäßigen Gründen zugriffen werden und ist nur erlaubt, wenn die Beschäftigten vorab darüber unterrichtet wurden, dass der Arbeitgeber Zugang zu dieser Art der Kommunikation haben kann.

Beschäftigten ist das Recht auf Auskunft über ihre Beschäftigtendaten sowie das Recht auf deren Berichtigung oder Löschung einzuräumen. Werden Beurteilungen verarbeitet, müssen Beschäftigte außerdem das Recht haben, die Beurteilung anzufechten. Diese Rechte können jedoch für Zwecke interner Untersuchungen vorübergehend eingeschränkt werden. Wird einem Beschäftigten die Auskunft über personenbezogene Beschäftigtendaten, deren Berichtigung oder Löschung verweigert, muss das innerstaatliche Recht angemessene Maßnahmen für eine Anfechtung dieser Verweigerung vorsehen.

9.3. Gesundheitsdaten

Kernpunkte

- Gesundheitsdaten sind sensible Daten und genießen daher besonderen Schutz.

Personenbezogene Daten über den Gesundheitszustand der betroffenen Person werden in Artikel 9 Absatz 1 der DSGVO und in Artikel 6 des Modernisierten Übereinkommens Nr. 108 als sensible Daten eingestuft. Folglich unterliegen Gesundheitsdaten bei der Datenverarbeitung strengeren Vorschriften als nicht-sensible Daten. Die DSGVO verbietet die Verarbeitung von „personenbezogenen Gesundheitsdaten“ (worunter „alle Daten [...] [zu verstehen sind], die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person

hervorgehen“)⁹³⁴, genetischen Daten und biometrischen Daten, es sei denn, diese Verarbeitung ist gemäß Artikel 9 Absatz 2 erlaubt. Beide Arten von Daten wurden der Liste der „besonderen Datenkategorien“ hinzugefügt.⁹³⁵

Beispiel: In der Rechtssache *Z gegen Finnland*⁹³⁶ hatte der frühere Ehemann der Beschwerdeführerin, der HIV-positiv war, eine Reihe von Sexualstraftaten begangen. Er wurde später wegen Totschlags verurteilt, weil er seine Opfer wissentlich dem Risiko einer HIV-Infektion ausgesetzt hatte. Das innerstaatliche Gericht ordnete an, dass das vollständige Urteil und alle Unterlagen zum Fall zehn Jahre der Geheimhaltung unterliegen sollten, obwohl die Beschwerdeführerin einen längeren Geheimhaltungszeitraum beantragt hatte. Das Berufungsgericht wies diese Anträge zurück, und sein Urteil enthielt die vollen Namen sowohl der Beschwerdeführerin als auch ihres ehemaligen Ehemanns. Der EGMR stellte fest, dass der Eingriff nicht als in einer demokratischen Gesellschaft notwendig betrachtet wurde, weil der Schutz medizinischer Daten von grundlegender Bedeutung für die Wahrnehmung des Rechts auf Achtung des Privat- und Familienlebens ist, insbesondere, wenn es um Informationen über HIV-Infektionen geht, da diese Erkrankung in vielen Kulturen stigmatisiert ist. Der Gerichtshof befand daher, dass die Gewährung des Zugangs zu dem Urteil des Berufungsgerichts, in dem die Identität und der Gesundheitszustand der Beschwerdeführerin beschrieben wurde, bereits zehn Jahre nach Ergehen des Urteils, eine Verletzung von Artikel 8 EMRK sei.

Im **EU-Recht** lässt Artikel 9 Absatz 2 Buchstabe h DSGVO eine Verarbeitung medizinischer Daten zu, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Versorgung oder Behandlung im Gesundheitsbereich oder der Verwaltung von Leistungen der Gesundheitsfürsorge erforderlich ist. Eine Verarbeitung ist jedoch nur dann zulässig, wenn sie durch ärztliches Personal, das dem Berufsgeheimnis unterliegt, oder durch eine andere Person, die einer gleichwertigen Pflicht unterliegt, vorgenommen wird.⁹³⁷

934 DSGVO, Erwägungsgrund 35.

935 a.a.O., Artikel 9 Absatz 1.

936 EGMR, *Z / Finnland*, Nr. 22009/93, 25. Februar 1997, Randnrn. 94 und 112; siehe auch EGMR, *M.S. / Schweden*, Nr. 20837/92, 27. August 1997; EGMR, *L.L. / Frankreich*, Nr. 7508/02, 10. Oktober 2006; EGMR, *I / Finnland*, Nr. 20511/03, 17. Juli 2008; EGMR, *K.H. und andere / Slowakei*, Nr. 32881/04, 28. April 2009; EGMR, *Szuluk / Vereinigtes Königreich*, Nr. 36936/05, 2. Juni 2009.

937 Siehe ferner EGMR, *Biriuk / Litauen*, Nr. 23373/03, 25. November 2008.

Im **Recht des Europarates** wendet die Empfehlung des Europarates betreffend den Schutz medizinischer Daten aus dem Jahr 1997 die Grundsätze des Übereinkommens Nr. 108 im Detail auf die Datenverarbeitung im medizinischen Bereich an.⁹³⁸ Im Hinblick auf die rechtmäßigen Zwecke der Verarbeitung medizinischer Daten, die notwendigen Geheimhaltungspflichten für Personen, die medizinische Daten verwenden, und die Rechte der betroffenen Personen auf Transparenz und Auskunft, Berichtigung und Löschung, stimmen die vorgeschlagenen Vorschriften mit der DSGVO überein. Medizinische Daten, die rechtmäßig von Angehörigen der Gesundheitsberufe verarbeitet werden, dürfen außerdem nicht an Strafverfolgungsbehörden weitergegeben werden, es sei denn, „es liegen ausreichende Garantien vor, die eine Weitergabe, die nicht mit der Achtung des [...] Privatlebens in Einklang steht, wie sie in Artikel 8 EMRK garantiert wird, verhindern“.⁹³⁹ Die nationalen Rechtsvorschriften müssen zudem „hinreichend präzise formuliert sein und einen angemessenen Rechtsschutz gegen Willkür gewähren“.⁹⁴⁰

Darüber hinaus enthält die Empfehlung betreffend den Schutz medizinischer Daten besondere Bestimmungen bezüglich der medizinischen Daten ungeborener Kinder und Behinderter sowie der Verarbeitung genetischer Daten. Die wissenschaftliche Forschung wird ausdrücklich als Grund dafür anerkannt, dass Daten länger aufbewahrt werden, als sie eigentlich benötigt werden, auch wenn hierfür in der Regel eine Anonymisierung verlangt wird. Artikel 12 der Empfehlung betreffend den Schutz medizinischer Daten enthält detaillierte Vorschriften für den Fall, dass Forscher personenbezogene Daten benötigen und anonymisierte Daten nicht ausreichen.

Ein geeignetes Mittel, um den Bedürfnissen der Wissenschaft entgegenzukommen und gleichzeitig die Interessen der betroffenen Patienten zu schützen, könnte die Pseudonymisierung sein. Nähere Erläuterungen zum Konzept der Pseudonymisierung im Zusammenhang mit dem Datenschutz finden sich in [Abschnitt 2.1.1](#).

938 Europarat, Ministerkomitee (1997), Empfehlung Rec(97)5 an die Mitgliedstaaten betreffend den Schutz medizinischer Daten, 13. Februar 1997. Diese Empfehlung befindet sich in Überarbeitung.

939 EGMR, *Avilkina und andere / Russland*, Nr. 1585/09, 6. Juni 2013, Randnr. 53. Siehe auch EGMR, *Biriuk / Lithuania*, Nr. 23373/03, 25 November 2008.

940 EGMR, *L.H. / Lettland*, Nr. 52019/07, 29. April 2014, Randnr. 59.

Die Empfehlung des Europarates aus dem Jahr 2016 über Daten aus Gentests findet auch auf die Datenverarbeitung im Medizinbereich Anwendung.⁹⁴¹ Diese Empfehlung ist für den Bereich der elektronischen Gesundheitsdienste von großer Bedeutung, in dem die Informations- und Kommunikationstechnologien zur Unterstützung der medizinischen Betreuung eingesetzt werden. Ein Beispiel ist die Übermittlung der Ergebnisse eines Mutter- oder Vaterschaftstests eines Patienten von einem Erbringer von Gesundheitsleistungen an einen anderen. Diese Empfehlung zielt auf den Schutz der Rechte von Personen ab, deren personenbezogene Daten zu Versicherungszwecken verarbeitet werden, um diese gegen Risiken im Zusammenhang mit der Gesundheit, der körperlichen Unversehrtheit, dem Alter oder dem Tod zu versichern. Versicherer müssen die Verarbeitung gesundheitsbezogener Daten rechtfertigen und die Verarbeitung sollte in Bezug auf die Art und die Bedeutung des in Betracht gezogenen Risikos verhältnismäßig sein. Die Verarbeitung dieser Art von Daten hängt von der Einwilligung der betroffenen Person ab. Versicherer sollten auch Schutzmaßnahmen für die Speicherung gesundheitsbezogener Daten eingerichtet haben.

Klinische Prüfungen, die die Bewertung der Wirkungen neuer Arzneimittel auf Patienten in dokumentierten Forschungsumgebungen beinhalten, haben beträchtliche datenschutzrechtliche Auswirkungen. Klinische Prüfungen mit Humanarzneimitteln sind durch die Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG (Verordnung über klinische Prüfungen) geregelt.⁹⁴² Zu den Hauptbestandteilen der Verordnung über klinische Prüfungen zählen:

- ein vereinfachtes Antragsverfahren über das EU-Portal;⁹⁴³
- Fristen für die Bewertung des Antrags für klinische Prüfungen;⁹⁴⁴

941 Europarat, Ministerkomitee (2016), Recommendation Rec(2016)8 to Member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, 26. Oktober 2016.

942 Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG (Verordnung über klinische Prüfungen), ABl. L 158 vom 27.5.2014.

943 Verordnung über klinische Prüfungen, Artikel 5 Absatz 1.

944 a.a.O., Artikel 5 Absatz 2-5.

- eine Ethik-Kommission als Bestandteil der Bewertung gemäß dem Recht des Mitgliedstaats (und gemäß dem europäischen Recht zur Festsetzung der betreffenden Fristen),⁹⁴⁵ und
- verbesserte Transparenz der klinischen Prüfungen und ihrer Ergebnisse.⁹⁴⁶

Die DSGVO präzisiert, dass für die Zwecke der Einwilligung in die Teilnahme an wissenschaftlichen Forschungstätigkeiten im Rahmen klinischer Prüfungen die Verordnung (EU) Nr. 536/2014 gilt.⁹⁴⁷

Bezüglich der Verarbeitung personenbezogener Daten im Gesundheitssektor stehen auf EU-Ebene noch viele weitere Gesetzesvorschläge und andere Initiativen an.⁹⁴⁸

Elektronische Patientenakten

Elektronische Patientenakten sind definiert als „umfassende medizinische Aufzeichnungen oder ähnliche Unterlagen über den bisherigen und gegenwärtigen körperlichen und geistigen Gesundheitszustand einer Person, die in elektronischer Form vorliegen und unmittelbar zur medizinischen Behandlung und anderen damit eng verbundenen Zwecken zur Verfügung stehen“.⁹⁴⁹ Elektronische Patientenakten sind elektronische Versionen der Krankengeschichte von Patienten und können klinische Daten über diese Personen wie die frühere Krankengeschichte, Probleme und Befunde, Medikationen und Heilverfahren sowie Untersuchungs- und Laborergebnisse und -berichte enthalten. Diese elektronischen Dateien, bei denen es sich um ganze Akten oder lediglich um Auszüge oder Zusammenfassungen handeln kann, sind für den Allgemeinmediziner, den Apotheker und anderes Gesundheitspersonal zugänglich. Das Gesamtkonzept „eHealth“ bezieht sich auch auf diese Patientenakten.

945 a.a.O., Artikel 2 Absatz 2 Buchstabe 11.

946 a.a.O., Artikel 9 Absatz 1 und Erwägungsgrund 67.

947 DSGVO, Erwägungsgründe 156 und 161.

948 EDSB (2013), Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission über den „eGesundheit Aktionsplan 2012-2020 – Innovative Gesundheitsfürsorge für das 21. Jahrhundert“, Brüssel, 27. März 2013.

949 *Empfehlung der Kommission vom 2. Juli 2008 zur grenzübergreifenden Interoperabilität elektronischer Patientendatenysteme*, Punkt 3 Buchstabe c.

Beispiel: Herr A hat einen Versicherungsvertrag mit dem Unternehmen B, dem Versicherer, abgeschlossen. Letzterer erfasst einige gesundheitsbezogene Informationen von A, wie anhaltende Gesundheitsprobleme oder Krankheiten. Der Versicherer sollte die gesundheitsbezogenen personenbezogenen Daten von A getrennt von anderen Daten speichern. Der Versicherer muss die gesundheitsbezogenen personenbezogenen Daten auch getrennt von anderen personenbezogenen Daten speichern. Dies bedeutet, dass nur der mit A befasste Sachbearbeiter Zugang zu den gesundheitsbezogenen Daten von A haben wird.

Gleichwohl werfen elektronische Patientenakten einige Datenschutzthemen auf, die deren Zugriffsrechte, ordnungsgemäße Speicherung und das Auskunftsrecht der betroffenen Person betreffen.

Zusätzlich zu der Empfehlung zu den elektronischen Patientenakten veröffentlichte die Europäische Kommission am 10. April 2014 ein Grünbuch über Mobile-Health-Dienste (mHealth), da sie der Ansicht war, dass mHealth ein sich entwickelnder und schnell wachsender Bereich ist, der das Potenzial hat, die Gesundheitswesen zu verändern und deren Effizienz und Qualität zu steigern. Der Begriff umfasst medizinische Verfahren und Praktiken der öffentlichen Gesundheitsfürsorge, die durch Mobilgeräte wie Mobiltelefone, Patientenüberwachungsgeräte, persönliche digitale Assistenten und andere drahtlos angebundene Geräte unterstützt werden, sowie Anwendungen (beispielsweise Gesundheits-Apps), die mit medizinischen Geräten oder mit Sensoren vernetzt werden können.⁹⁵⁰ Das Grünbuch gibt einen Überblick über die Risiken, die die Entwicklung von mHealth für den Schutz personenbezogener Daten mit sich bringen könnte und sieht vor, dass diese Entwicklung angesichts des sensiblen Charakters von Gesundheitsdaten besondere und geeignete Sicherheitsvorkehrungen für Patientendaten wie Verschlüsselung und angemessene Mechanismen zur Authentifizierung der Patienten umfassen sollte, um die Sicherheitsrisiken zu mindern. Die Vorschriften für den Schutz personenbezogener Daten müssen unbedingt eingehalten werden, damit Vertrauen in mHealth-Lösungen entsteht. Dazu gehören die Pflicht zur Unterrichtung der betroffenen Person, die Sicherheit der Daten und der Grundsatz der rechtmäßigen Verarbeitung personenbezogener Daten.⁹⁵¹ Zu diesem Zweck hat die Branche Verhaltensregeln entworfen, die auf Beiträgen einer breiten

950 Europäische Kommission (2014), *Grünbuch über Mobile-Health-Dienste („mHealth“)*, COM(2014) 219 final, Brüssel, 10. April 2014.

951 *a.a.O.*, S. 8.

Palette von Interessenvertretern beruhen, darunter Experten der Bereiche Datenschutz, Selbst- und Koregulierung, IKT und Gesundheitswesen.⁹⁵² Zum Zeitpunkt der Abfassung des Handbuchs wurde der Entwurf der Verhaltensregeln der Artikel-29-Datenschutzgruppe zur Stellungnahme unterbreitet und seine offizielle Genehmigung steht noch aus.

9.4. Datenverarbeitung für Forschungszwecke und statistische Zwecke

Kernpunkte

- Für statistische, wissenschaftliche oder historische Forschungszwecke erhobene Daten dürfen nicht für andere Zwecke verwendet werden.
- Daten, die rechtmäßig für einen anderen Zweck erhoben wurden, dürfen für statistische, wissenschaftliche oder historische Forschungszwecke weiterverwendet werden, sofern geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen bestehen. Erfolgt zu diesem Zweck, Anonymisierung oder Pseudonymisierung der Daten vor deren Übermittlung an Dritte, kann dies solche Garantien bereitstellen.

Das **EU-Recht** erlaubt die Verarbeitung von Daten für statistische und wissenschaftliche oder historische Forschungszwecke, sofern geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen bestehen. Dazu kann die Pseudonymisierung gehören.⁹⁵³ Das EU-Recht oder das nationale Recht kann bestimmte Ausnahmen von den Rechten der betroffenen Personen vorsehen, sofern diese Rechte voraussichtlich die Verwirklichung des rechtmäßigen Zwecks der Forschung unmöglich machen oder ernsthaft beeinträchtigen.⁹⁵⁴ Es können Ausnahmen vom Auskunftsrecht der betroffenen Person, vom Recht auf Berichtigung, vom Recht auf Einschränkung der Verarbeitung und vom Widerspruchsrecht eingeführt werden.

Auch wenn Daten, die rechtmäßig von einem Verantwortlichen für einen bestimmten Zweck erhoben wurden, von diesem Verantwortlichen für eigene

⁹⁵² *Draft Code of Conduct on privacy for mobile health applications*, 7. Juni 2016.

⁹⁵³ DSGVO, Artikel 89 Absatz 1.

⁹⁵⁴ a.a.O., Artikel 89 Absatz 2.

statistische, wissenschaftliche oder historische Forschungszwecke weiterverwendet werden dürfen, müssten die Daten vor einer Übermittlung an Dritte für statistische, wissenschaftliche oder historische Forschungszwecke je nach Kontext anonymisiert oder Maßnahmen zur Pseudonymisierung unterzogen werden, sofern die betroffene Person nicht eingewilligt hat oder dies in einem nationalen Gesetz ausdrücklich vorgesehen ist. Im Gegensatz zu anonymen Daten bleiben Daten, die einer Pseudonymisierung unterzogen wurden, der DSGVO unterworfen.⁹⁵⁵

Die DSGVO gewährt der Forschung folglich eine Sonderbehandlung hinsichtlich der allgemeinen Datenschutzvorschriften, um die Weiterentwicklung der Forschung nicht einzuschränken und dem Ziel der Verwirklichung eines europäischen Forschungsraums gemäß Artikel 179 AEUV Rechnung. Sie sieht eine weite Auslegung der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken vor, die die Verarbeitung für die technologische Entwicklung und Beweisführung, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließt. Sie erkennt auch an, dass es wichtig ist, die Daten für Forschungszwecke in Registern zu sammeln, und dass es schwierig sein kann, den späteren Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der Daten vollständig anzugeben.⁹⁵⁶ Daher erlaubt die DSGVO die zu diesen Zwecken erfolgende Verarbeitung von Daten ohne Einwilligung der betroffenen Person, sofern die entsprechenden Garantien bereitgestellt werden.

Ein wichtiges Beispiel für die Verwendung von Daten zu statistischen Zwecken sind amtliche Statistiken, die von den statistischen Ämtern der Mitgliedstaaten und der EU auf der Grundlage innerstaatlicher und europäischer Rechtsvorschriften über amtliche Statistiken erstellt werden. Diese Rechtsvorschriften besagen, dass Bürger und Unternehmen in der Regel verpflichtet sind, Daten an die entsprechenden Statistikbehörden weiterzugeben. In den statistischen Ämtern tätige Bedienstete an besondere berufliche Geheimhaltungsverpflichtungen gebunden, die ordnungsgemäß einzuhalten sind, da sie für ein hohes Maß an Vertrauen der Bürger wesentlich sind, das vorhanden sein muss, wenn Daten Statistikbehörden zur Verfügung gestellt werden sollen.⁹⁵⁷

⁹⁵⁵ *a.a.O.*, Erwägungsgrund 26.

⁹⁵⁶ *a.a.O.*, Erwägungsgrund 33, 157 und 159.

⁹⁵⁷ *a.a.O.*, Artikel 90.

Die Verordnung (EG) Nr. 223/2009 über europäische Statistiken (Europäische Statistikverordnung) enthält grundlegende Vorschriften über den Datenschutz im Zusammenhang mit amtlichen Statistiken und kann daher auch für auf nationaler Ebene festgesetzte Vorschriften über amtliche Statistiken als relevant angesehen werden.⁹⁵⁸ Diese Verordnung behält den Grundsatz bei, wonach amtliche statistische Erfassung einer hinreichend klaren Rechtsgrundlage bedürfen.⁹⁵⁹

Beispiel: In der Rechtssache *Huber gegen Bundesrepublik Deutschland*⁹⁶⁰ beschwerte sich ein in Deutschland niedergelassener österreichischer Geschäftsmann darüber, dass die seitens der deutschen Behörden auch zu statistischen Zwecken erfolgende Erhebung und Aufbewahrung personenbezogener Daten von Ausländern in einem zentralen Register („AZR“) seine Rechte gemäß der Datenschutzrichtlinie verletze. In Anbetracht der Tatsache, dass die Richtlinie 95/46 auf die Gewährleistung eines gleichwertigen Datenschutzniveaus in allen Mitgliedstaaten abzielt, befand der EuGH, dass der Begriff der Erforderlichkeit im Sinne von Artikel 7 Buchstabe e in den einzelnen Mitgliedstaaten keinen variablen Inhalt haben kann. Es handelt sich somit um einen autonomen Begriff des Gemeinschaftsrechts, der so auszulegen ist, dass er in vollem Umfang dem Ziel der Richtlinie 95/46 entspricht. Der EuGH stellte fest, dass lediglich anonyme Informationen zu statistischen Zwecken erforderlich sein sollten und entschied, dass das deutsche Register mit dem Erforderlichkeitsgebot von Artikel 7 Buchstabe e nicht vereinbar sei.

958 Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates vom 11. März 2009 über europäische Statistiken und zur Aufhebung der Verordnung (EG, Euratom) Nr. 1101/2008 des Europäischen Parlaments und des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften, der Verordnung (EG) Nr. 322/97 des Rates über die Gemeinschaftsstatistiken und des Beschlusses 89/382/EWG, Euratom des Rates zur Einsetzung eines Ausschusses für das Statistische Programm der Europäischen Gemeinschaften, ABl. L 87 vom 31.3.2009, in der durch die Verordnung (EU) Nr. 2015/759 des Europäischen Parlaments und des Rates vom 29. April 2015 zur Änderung der Verordnung (EG) Nr. 223/2009 über europäische Statistiken geänderten Form, ABl. L 123 vom 19.5.2015.

959 Dieser Grundsatz wird im *Verhaltenskodex von Eurostat* näher ausgeführt, der gemäß Artikel 11 der Europäischen Statistikverordnung ethische Orientierung für die Erstellung amtlicher Statistiken einschließlich der besonnenen Verwendung personenbezogener Daten bieten soll.

960 EuGH, C-524/06, *Heinz Huber / Bundesrepublik Deutschland* [GK], 16. Dezember 2008, siehe insbesondere Randnr. 68.

Im **Recht des Europarates** kann eine Weiterverarbeitung von Daten für statistische, wissenschaftliche oder historische Forschungszwecke erfolgen, sofern dies im öffentlichen Interesse geschieht und geeigneten Garantien unterliegt.⁹⁶¹ Die Rechte der betroffenen Personen können bei der Datenverarbeitung für statistische Zwecke ebenfalls eingeschränkt werden, sofern kein erkennbares Risiko in Bezug auf eine Verletzung ihrer Rechte und Freiheiten besteht.⁹⁶²

Die 1997 herausgegebene Empfehlung betreffend statistische Daten deckt die Leistung statistischer Tätigkeiten im öffentlichen und im privaten Sektor ab.⁹⁶³

Daten, die von einem Verantwortlichen zu statistischen Zwecken erhoben wurden, dürfen nicht für andere Zwecke verwendet werden. Daten, die nicht für statistische Zwecke erhoben wurden, stehen für eine weitere Verwendung in Statistiken zur Verfügung. Die Empfehlung betreffend statistische Daten erlaubt auch die Weitergabe von Daten an Dritte, sofern dies nur zu statistischen Zwecken erfolgt. In derartigen Fällen sollten die Beteiligten den genauen Umfang der rechtmäßigen Weiterverwendung für Statistiken vereinbaren und schriftlich festlegen. Da dies die Einwilligung – sofern erforderlich – der betroffenen Person jedoch nicht ersetzen kann, müssen im innerstaatlichen Recht geeignete Garantien vorgesehen sein, um das Risiko des Missbrauchs personenbezogener Daten möglichst klein zu halten, beispielsweise die Verpflichtung zur Anonymisierung oder Pseudonymisierung der Daten vor der Offenlegung.

Für Personen, die von Berufs wegen statistische Forschung betreiben, muss nach innerstaatlichem Recht eine besondere berufliche Geheimhaltungspflicht gelten – wie es in der Regel auch bei statistischen Ämtern der Fall ist. Diese muss auch für Interviewer und andere Personen, die personenbezogene Daten erheben, gelten, wenn sie Daten bei betroffenen oder anderen Personen erheben.

Ist eine statistische Erhebung unter Verwendung personenbezogener Daten vom Gesetz nicht zugelassen, kann es sein, dass die betroffenen Personen in die Verwendung ihrer Daten einwilligen müssen, damit sie rechtmäßig ist, oder sie zumindest die Möglichkeit haben müssen, ihr zu widersprechen. Werden

961 Modernisiertes Übereinkommen Nr. 108, Artikel 5 Absatz 4 Buchstabe b.

962 *a.a.O.*, Artikel 11 Absatz 2.

963 Europarat, Ministerkomitee (1997), Empfehlung Rec(97)18 an die Mitgliedstaaten betreffend den Schutz personenbezogener Daten, die zu statistischen Zwecken erhoben und verarbeitet werden, 30. September 1997.

personenbezogene Daten von Interviewern für statistische Zwecke erhoben, sind die befragten Personen klar und deutlich darüber aufzuklären, ob die Bereitstellung der Daten im innerstaatlichen Recht vorgeschrieben ist.

Kann eine statistische Erhebung nicht mit Daten anonymer Personen durchgeführt werden und werden personenbezogene Daten benötigt, sind die zu diesem Zweck erhobenen Daten schnellstmöglich zu anonymisieren. Die Ergebnisse der statistischen Erhebung dürfen zumindest keine Identifizierung von betroffenen Personen ermöglichen, es sei denn, dies würde eindeutig kein Risiko bedeuten.

Nach Abschluss der Auswertung der Statistiken sollten die verwendeten personenbezogenen Daten entweder gelöscht oder anonymisiert werden. In diesen Fällen wird in der Empfehlung betreffend statistische Daten darauf hingewiesen, dass Identifizierungsdaten getrennt von anderen personenbezogenen Daten zu speichern sind. Das bedeutet beispielsweise, dass entweder der Entschlüsselungscode oder die Liste mit den identifizierenden Synonymen getrennt von den anderen Daten aufbewahrt werden muss.

9.5. Finanzdaten

Kernpunkte

- Finanzdaten werden zwar nicht als sensible Daten im Sinne des Modernisierten Übereinkommens Nr. 108 oder der DSGVO betrachtet, doch sind bei ihrer Verarbeitung besondere Garantien für Richtigkeit und Datensicherheit erforderlich.
- Insbesondere elektronische Zahlungssysteme benötigen eingebauten Datenschutz, d. h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.
- Besondere Datenschutzprobleme können in diesem Bereich aus der Notwendigkeit resultieren, über geeignete Mechanismen für die Authentifizierung zu verfügen.

Beispiel: In der Rechtssache *Michaud gegen Frankreich*⁹⁶⁴ focht der Beschwerdeführer, ein französischer Anwalt, seine nach französischem Recht bestehende Verpflichtung zur Berichterstattung über Verdachtsmomente in Bezug auf mögliche Geldwäscheaktivitäten seiner Mandanten an. Nach Auffassung des EGMR stelle die Forderung an Anwälte, den Verwaltungsbehörden Informationen über eine Person zu geben, in deren Besitz sie im Zuge berufsbedingter Gespräche gelangt sind, einen Eingriff in das Recht des Anwalts auf Achtung seines Privatlebens und seiner Korrespondenz unter Artikel 8 EMRK dar, da die Definition auch Tätigkeiten beruflicher Art abdecke. Der Eingriff sei jedoch im Gesetz vorgesehen gewesen und habe ein rechtmäßiges Ziel verfolgt, nämlich die Aufrechterhaltung der Ordnung und die Verhütung von Straftaten. Da Anwälte nur unter sehr begrenzten Umständen zur Meldung von verdächtigen Tätigkeiten verpflichtet seien, hielt der EGMR diese Verpflichtung für verhältnismäßig. Er befand, dass keine Verletzung von Artikel 8 vorlag.

Beispiel: In der *Rechtssache M.N. und andere gegen San Marino*⁹⁶⁵ ging der Beschwerdeführer, ein italienischer Staatsangehöriger, eine Treuhandvereinbarung mit einer Gesellschaft ein, gegen die Ermittlungen geführt wurden. Dies bedeutete, dass die Gesellschaft der Durchsuchung und Beschlagnahme von Kopien (elektronischer) Dokumentation unterlag. Der Beschwerdeführer reichte eine Beschwerde beim Gericht von San Marino ein, da er behauptete, dass zwischen ihm und den mutmaßlichen Straftaten kein Zusammenhang bestehe. Das Gericht erklärte die Beschwerde jedoch für unzulässig, da der Beschwerdeführer keine „interessierte Person“ sei. Der EGMR befand, dass der Beschwerdeführer im Hinblick auf den Rechtsschutz gegenüber einer „interessierten Person“ wesentlich benachteiligt war, da seine Daten nach wie vor den Durchsuchungs- und Beschlagnahmemaßnahmen unterlagen. Folglich stellte der Gerichtshof fest, dass eine Verletzung von Artikel 8 EMRK stattgefunden hat.

Beispiel: In der Rechtssache *G.S.B. gegen Schweiz*⁹⁶⁶ wurden Details über das Bankkonto des Beschwerdeführers auf Grundlage des zwischen der Schweiz und den Vereinigten Staaten geschlossenen Abkommens über

964 EGMR, *Michaud / Frankreich*, Nr. 12323/11, 6. Dezember 2012. Siehe auch EGMR, *Niemietz / Deutschland*, Nr. 13710/88, 16. Dezember 1992, Randnr. 29, und EGMR, *Halford / Vereinigtes Königreich*, Nr. 20605/92, 25. Juni 1997, Randnr. 42.

965 EGMR, *M.N. und andere / San Marino*, Nr. 28005/12, 7. Juli 2015.

966 EGMR, *G.S.B. / Schweiz*, Nr. 28601/11 22. Dezember 2015.

die Verwaltungszusammenarbeit an die US-Steuerbehörden übermittelt. Der EGMR befand, dass die Übermittlung nicht unter Verletzung gegen Artikel 8 EMRK stattgefunden habe, da der Eingriff in das Recht des Beschwerdeführers auf Privatsphäre gesetzlich vorgesehen war, ein legitimes Ziel verfolgte und zum betreffenden öffentlichen Interesse verhältnismäßig war.

In seiner Empfehlung Rec(90)19 stellte der **Europarat** die Anwendung des allgemeinen Datenschutzregelwerks (wie im Übereinkommen Nr. 108 enthalten) auf den Zahlungsverkehr dar.⁹⁶⁷ In dieser Empfehlung wird der Anwendungsbereich der rechtmäßigen Erhebung und Verwendung von Daten im Bereich des Zahlungsverkehrs, insbesondere Kartenzahlungen, erläutert. Sie gibt den nationalen Gesetzgebern detaillierte Empfehlungen über die Regeln für die Weitergabe von Zahlungsdaten an Dritte, über die Fristen für die Datenspeicherung, über Transparenz, Datensicherheit und grenzüberschreitenden Datenfluss sowie über die Aufsicht und Rechtsbehelfe. Der Europarat hat auch eine Stellungnahme zur Übermittlung von Steuerdaten ausgearbeitet,⁹⁶⁸ die Empfehlungen und Aspekte enthält, die es beim Umgang mit der Übermittlung von Steuerdaten zu berücksichtigen gilt.

Der EGMR erlaubt die Übermittlung von Finanzdaten und insbesondere der Details über das Bankkonto einer Person gemäß Artikel 8 EMRK, sofern sie gesetzlich vorgesehen ist, ein legitimes Ziel verfolgt und zum betreffenden öffentlichen Interesse verhältnismäßig ist.⁹⁶⁹

Nach **EU-Recht** müssen elektronische Zahlungssysteme, die die Verarbeitung personenbezogener Daten beinhalten, die Bestimmungen der DSGVO einhalten. Daher müssen diese Systeme Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sicherstellen. Datenschutz durch Technikgestaltung verpflichtet den Verantwortlichen zum Treffen geeigneter technischer und organisatorischer Maßnahmen zur Umsetzung der Datenschutzgrundsätze. Datenschutz durch datenschutzfreundliche Voreinstellungen bedeutet, dass der Verantwortliche sicherstellen muss, dass nur

967 Europarat, Ministerkomitee (1990), Empfehlung Nr. R(90)19 über den Schutz personenbezogener Daten, die für Zahlungen und damit zusammenhängende Vorgänge verwendet werden, 13. September 1990.

968 Europarat, Beratender Ausschuss für das Übereinkommen 108 (2014), Opinion on the implication for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes, 4. Juni 2014.

969 EGMR, *G.S.B. / Schweiz*, Nr. 28601/11, 22. Dezember 2015.

personenbezogene Daten, die für einen bestimmten Zweck erforderlich sind, durch Voreinstellung verarbeitet werden können (siehe [Abschnitt 4.4](#)). Was Finanzdaten betrifft, so befand der EuGH, dass übermittelte Steuerdaten personenbezogene Daten darstellen können.⁹⁷⁰ Die Artikel-29-Datenschutzgruppe gab diesbezügliche Leitlinien für die Mitgliedstaaten heraus, die Kriterien für die Gewährleistung der Einhaltung der Datenschutzvorschriften beim automatischen Austausch personenbezogener Daten zu Steuerzwecken enthalten.⁹⁷¹ Darüber hinaus wurde eine Reihe von Rechtsinstrumenten zur Regulierung der Finanzmärkte und der Tätigkeiten von Kreditinstituten und Wertpapierfirmen erlassen.⁹⁷² Weitere Rechtsinstrumente unterstützen den Kampf gegen Insider-Geschäfte und Marktmanipulation.⁹⁷³ Nachstehend die Hauptbereiche, die sich auf den Datenschutz auswirken:

- Aufbewahrung von Aufzeichnungen über finanzielle Transaktionen;
- Weitergabe personenbezogener Daten an Drittländer;
- Aufzeichnung von Telefongesprächen oder elektronischer Kommunikation einschließlich der Befugnis der zuständigen Behörden, die Vorlage von Aufzeichnungen über Telefon- und Datenverkehr zu verlangen;
- Offenlegung personenbezogener Informationen einschließlich der Veröffentlichung von Sanktionen;
- Aufsichts- und Untersuchungsbefugnisse der zuständigen Behörden einschließlich Vor-Ort-Kontrollen und Betreten von Privaträumen zwecks Beschlagnahme von Unterlagen;

970 EuGH, C-201/14, *Smaranda Bara und andere / Casa Națională de Asigurări de Sănătate und andere*, 1. Oktober 2015, Randnr. 29.

971 Artikel-29-Datenschutzgruppe (2015), Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes, 14/EN WP 230.

972 Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU, ABl. L 173 vom 12.6.2014; Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012, ABl. L 173 vom 12.6.2014; Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG, ABl. L 176 vom 27.6.2013.

973 Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission, ABl. L 173 vom 12.6.2014.

- Regelungen für die Meldung von Verstößen, also für Whistleblowing; und
- Zusammenarbeit zwischen zuständigen Behörden der Mitgliedstaaten und der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA).

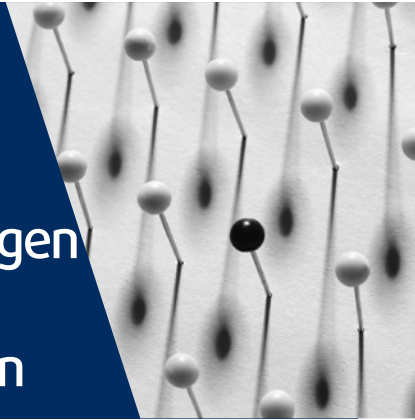
In diesen Bereichen gibt es noch andere Themen, an denen gearbeitet wird; dazu gehören die Erhebung von Daten über die finanzielle Situation betroffener Personen⁹⁷⁴ oder grenzüberschreitende Zahlungen per Banküberweisung, bei denen unausweichlich personenbezogene Daten übertragen werden.⁹⁷⁵

974 Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen, ABl. L 302 vom 17.11.2009, zuletzt geändert durch die Richtlinie 2014/51/EU des Europäischen Parlaments und des Rates vom 16. April 2014 zur Änderung der Richtlinien 2003/71/EG und 2009/138/EG und der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 im Hinblick auf die Befugnisse der Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung) und der Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), ABl. L 153 vom 22.5.2014; Verordnung (EU) Nr. 462/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 zur Änderung der Verordnung (EG) Nr. 1060/2009 über Ratingagenturen, ABl. L 146 vom 31.5.2013.

975 Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG und zur Aufhebung der Richtlinie 97/5/EG, ABl. L 319 vom 5.12.2007, geändert durch Richtlinie 2009/111/EG des Europäischen Parlaments und des Rates vom 16. September 2009 zur Änderung der Richtlinien 2006/48/EG, 2006/49/EG und 2007/64/EG hinsichtlich Zentralorganisationen zugeordneter Banken, bestimmter Eigenmittelbestandteile, Großkredite, Aufsichtsregelungen und Krisenmanagement, ABl. L 302 vom 17.11.2009.

10

Moderne Herausforderungen beim Schutz personenbezogener Daten



Das digitale Zeitalter oder das Zeitalter der Informationstechnologie zeichnet sich durch die massive Nutzung von Computern, dem Internet und digitalen Technologien aus. Es geht mit der Erhebung und Verarbeitung riesiger Datenmengen einher, zu denen auch personenbezogene Daten zählen. Die Erhebung und Verarbeitung personenbezogener Daten in einer globalisierten Wirtschaft bedeutet, dass der grenzüberschreitende Datenverkehr zunimmt. Aus einer solchen Verarbeitung können sich für das Alltagsleben bedeutende und sichtbare Vorteile ergeben: Suchmaschinen erleichtern den Zugang zu beachtlichen Mengen an Informationen und Wissen, soziale Netzwerke ermöglichen den Menschen auf der ganzen Welt, miteinander zu kommunizieren, ihre Meinungen zu äußern und sich für soziale, ökologische und politische Angelegenheiten einzusetzen, während Unternehmen und Verbraucher von wirksamen und leistungsfähigen Marketingtechniken profitieren, die die Wirtschaft ankurbeln. Die Technologie und die Verarbeitung personenbezogener Daten sind aber auch unentbehrliche Werkzeuge für staatliche Behörden bei der Bekämpfung von Kriminalität und Terrorismus. Ebenso kann die Massendatenverarbeitung, die in der Erhebung, Speicherung und Analyse großer Mengen an Informationen zur Ermittlung von Gesetzmäßigkeiten und zur Vorhersage von Verhaltensweisen besteht, „für die Gesellschaft eine Quelle von erheblichem Wert darstellen, die die Produktivität, die Leistung des öffentlichen Sektors und die soziale Beteiligung verbessert“.⁹⁷⁶

⁹⁷⁶ Europarat, Beratender Ausschuss für das Übereinkommen 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Straßburg, 23. Januar 2017.

Trotz seiner zahlreichen Vorteile stellt das digitale Zeitalter auch Herausforderungen für die Privatsphäre und den Datenschutz dar, da riesige Mengen personenbezogener Daten auf zunehmend vielschichtigere und undurchsichtigere Arten erhoben und verarbeitet werden. Der technologische Fortschritt hat zur Entwicklung massiver Datenbestände geführt, die leicht abgeglichen und weiter analysiert werden können, um nach Gesetzmäßigkeiten zu suchen oder Entscheidungen auf Grundlage von Algorithmen anzunehmen, was beispiellose Erkenntnisse über das menschliche Verhalten und das Privatleben bieten kann.⁹⁷⁷

Neue Technologien sind leistungsstark und können besonders gefährlich sein, wenn sie in die falschen Hände geraten. Staatliche Behörden, die unter dem Einsatz dieser Technologien Massenüberwachungstätigkeiten durchführen, sind nur ein Beispiel für die bedeutenden Auswirkungen, die diese Technologien auf die Rechte der Personen haben können. 2013 lösten die Enthüllungen von Edward Snowden über den seitens der Nachrichtendienste einiger Staaten erfolgenden Betrieb von großangelegten Internet- und Telefonüberwachungsprogrammen erhebliche Bedenken über die Gefahren aus, die Überwachungstätigkeiten für die Privatsphäre, die demokratische Staatsführung und die Freiheit der Meinungsäußerung zur Folge haben. Massenüberwachung und Technologien, die die globalisierte Speicherung und Verarbeitung personenbezogener Daten und den Massenzugang zu Daten ermöglichen, können den Wesensgehalt des Rechts auf Privatsphäre verletzen.⁹⁷⁸ Darüber hinaus können sie sich negativ auf die politische Kultur und abschreckend auf Demokratie, Kreativität und Innovation auswirken.⁹⁷⁹ Allein die Angst davor, dass der Staat das Verhalten und die Tätigkeiten der Bürger ständig verfolgen und analysieren könnte, kann diese davor abschrecken, ihre Meinungen zu bestimmten Angelegenheiten zu äußern, und zu Misstrauen und Vorsicht führen.⁹⁸⁰ Diese Herausforderungen haben eine Reihe von Behörden, Forschungszentren und Organisationen der Zivilgesellschaft zur Untersuchung der potenziellen Auswirkungen der neuen Technologien auf die Gesellschaft veranlasst. 2015 leitete

977 Europäisches Parlament (2017), *Entschließung zu den Folgen von Massendaten für die Grundrechte: Privatsphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung* (P8_TA-PROV(2017)0076, Straßburg, 14. März 2017.

978 Siehe UN, Generalversammlung, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Ben Emmerson, A/69/397, 23. September 2014, Absatz 59. Siehe auch EGMR, *Factsheet on Mass surveillance*, Juli 2017.

979 EDSB (2015), *Bewältigung der Herausforderungen in Verbindung mit Big Data*, Stellungnahme 7/2015, Brüssel, 19. November 2015.

980 Siehe insbesondere EuGH, Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014, Randnr. 37.

der Europäische Datenschutzbeauftragte mehrere Initiativen in die Wege, die auf die Beurteilung der Auswirkungen der Big Data und des Internets der Dinge auf die Ethik abzielten. Insbesondere richtete er einen Ethik-Beirat ein, mit dem Ziel, „eine offene und von Sachkenntnis geprägte Diskussion [anzuregen], dank derer die EU die Vorteile erkennen kann, die die Technologie für Gesellschaft und Wirtschaft mit sich bringt, und gleichzeitig die Rechte und Freiheiten natürlicher Personen stärkt, insbesondere ihr Recht auf Privatsphäre und Datenschutz.“⁹⁸¹

Die Verarbeitung personenbezogener Daten ist auch ein leistungsstarkes Werkzeug in den Händen von Unternehmen. Heutzutage kann sie detaillierte Informationen über die Gesundheit oder die finanzielle Lage einer Person offenbaren, die Unternehmen dann nutzen, um für die Einzelnen wichtige Entscheidungen zu treffen wie in Bezug auf ihren Krankenversicherungsbeitrag oder ihre Kreditwürdigkeit. Datenverarbeitungstechniken können sich auch auf demokratische Prozesse auswirken, wenn sie von Politikern oder Unternehmen zur Beeinflussung von Wahlen eingesetzt werden, wie beispielsweise durch das „Mikrotargeting“ der Kommunikation der Wähler. Anders ausgedrückt kann die Privatsphäre, die ursprünglich als Recht auf den Schutz von Personen vor ungerechtfertigten Eingriffen seitens Behörden betrachtet wurde, im modernen Zeitalter auch durch die Befugnisse privater Akteure bedroht sein. Dies wirft Fragen in Bezug auf den Einsatz von Technologie und Vorhersagenanalyse bei Entscheidungen auf, die sich auf das Alltagsleben der Einzelnen auswirken und verstärkt die Notwendigkeit, zu gewährleisten, dass sich jede Verarbeitung personenbezogener Daten an die Grundrechte hält.

Datenschutz ist untrennbar mit technologischem, gesellschaftlichem und politischem Wandel verbunden. Die Ausarbeitung einer umfassenden Liste künftiger Herausforderungen würde sich demnach als unmöglich erweisen. Dieses Kapitel befasst sich mit ausgewählten Bereichen im Zusammenhang mit Big Data, sozialen Netzwerken im Internet und dem digitalen Binnenmarkt der EU. Aus Sicht des Datenschutzes stellt es keine erschöpfende Beurteilung dieser Bereiche dar, sondern hebt vielmehr die Vielzahl der möglichen Interaktionen zwischen neuen oder geänderten menschlichen Tätigkeiten und dem Datenschutz hervor.

⁹⁸¹ Beschluss des Europäischen Datenschutzbeauftragten vom 3. Dezember 2015 über die Einsetzung eines externen Beirats für die ethische Dimension des Datenschutzes („Ethik-Beirat“), 3. Dezember 2015, Erwägungsgrund 5.

10.1. Big Data, Algorithmen und künstliche Intelligenz

Kernpunkte

- Bahnbrechende Innovationen in der IKT prägen eine neue Lebensweise, in der soziale Beziehungen, das Wirtschaftsleben und öffentliche Dienstleistungen digital miteinander verbunden sind und dadurch eine zunehmend große Datenmenge erzeugen, zu der auch zahlreiche personenbezogene Daten gehören.
- Regierungen, Unternehmen und Bürger arbeiten immer häufiger in einer daten-gesteuerten Wirtschaft, in der die Daten selbst zu wertvollen Vermögenswerten geworden sind.
- Der Begriff „Big Data“ bezieht sich sowohl auf die Daten als auch auf deren Analyse.
- Mittels Massendatenanalyse verarbeitete personenbezogene Daten fallen unter die Gesetzgebung der EU und des Europarates.
- Ausnahmen von den Datenschutzvorschriften und Datenschutzrechten sind auf ausgewählte Rechte und besondere Situationen begrenzt, in denen sich die Durchsetzung eines Rechts als unmöglich erweisen würde oder für die Verantwortlichen mit unverhältnismäßig hohem Aufwand verbunden wäre.
- Eine vollständig automatisierte Entscheidungsfindung ist außer in bestimmten Fällen grundsätzlich verboten.
- Kenntnis und Kontrolle seitens der Personen sind für die Gewährleistung der Durchsetzung der Rechte von entscheidender Bedeutung.

In unserer zunehmend digitalisierten Welt hinterlässt jede Tätigkeit eine digitale Spur, die erfasst, verarbeitet und ausgewertet oder analysiert werden kann. Mit neuen Informations- und Kommunikationstechnologien werden immer mehr Daten erhoben und aufgezeichnet.⁹⁸² Bis vor kurzem war keine Technologie dazu in der Lage, diese Datenmasse auszuwerten oder nützliche Schlüsse daraus zu ziehen. Die Daten waren für eine Auswertung schlichtweg zu zahlreich und für die Ermittlung von Trends und Gewohnheiten zu komplex, zu schlecht strukturiert und zu schnelllebig.

⁹⁸² Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – „Für eine florierende datengesteuerte Wirtschaft“, COM(2014) 442 final, Brüssel, 2. Juli 2014.

10.1.1. Definition der Begriffe „Big Data“, „Algorithmen“ und „künstliche Intelligenz“

Big Data

Der Begriff „Big Data“ ist ein Modewort, das sich je nach Kontext auf mehrere Konzepte beziehen kann. Für gewöhnlich umfasst er „das wachsende technologische Vermögen zur Erhebung, Verarbeitung und Entnahme neuer und voraussagender Erkenntnisse aus der großen Menge, der Schnelligkeit und der Vielfalt der Daten“.⁹⁸³ Der Begriff „Big Data“ bezieht sich demnach sowohl auf die Daten selbst als auch auf die Datenanalyse.

Die **Quellen** der Daten sind unterschiedlicher Art und umfassen Personen und deren personenbezogene Daten, Maschinen oder Sensoren, klimatische Informationen, Satellitenbilder, Digitalfotos und Videos oder GPS-Signale. Bei einem Großteil der Daten und Informationen handelt es sich jedoch um personenbezogene Daten wie Namen, Fotos, E-Mail-Adressen, Kontodaten, Daten in Bezug auf die GPS-Ortung, Beiträge in sozialen Netzen, medizinische Informationen oder IP-Adressen von Computern.⁹⁸⁴

Der Begriff „Big Data“ bezieht sich auch auf die **Verarbeitung**, Analyse und Auswertung der Datenmassen und verfügbaren Informationen, um nützliche Informationen zum Zwecke der Analyse von Big Data zu erhalten. Das bedeutet, dass die erhobenen Daten und Informationen für andere als die ursprünglich beabsichtigten Zwecke verwendet werden können, wie z. B. für statistische Trends oder maßgeschneiderte Dienstleistungen wie Werbung. Sofern die Technologien zur Erhebung, Verarbeitung und Auswertung von Big Data vorhanden sind, können jedwede Informationen kombiniert und neu ausgewertet werden: Finanztransaktionen, Kreditwürdigkeit, medizinische Behandlung, privater Konsum, berufliche Tätigkeit, Standort- und Streckenverfolgung,

983 Europarat, Beratender Ausschuss für das Übereinkommen Nr. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. Januar 2017, S. 2; Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – „Für eine florierende datengesteuerte Wirtschaft“, COM(2014) 442 final, Brüssel, 2. Juli 2014, S. 4; Internationale Fernmeldeunion (2015), Empfehlung Y.3600. Big Data – Cloud computing based requirements and capabilities.

984 EU-Kommission, Factsheet „Die EU-Datenschutzreform und Big Data“; Europarat, Beratender Ausschuss für das Übereinkommen Nr. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. Januar 2017, S. 2.

Internetnutzung, elektronische Karten und Smartphones, Video- oder Kommunikationsüberwachung. Die Analyse von Big Data bringt eine neue quantitative Dimension der Daten mit sich, die ausgewertet und in Echtzeit genutzt werden kann, zum Beispiel, um den Verbrauchern maßgeschneiderte Dienstleistungen anzubieten.

Algorithmen und künstliche Intelligenz

Künstliche Intelligenz (KI) bezieht sich auf die Intelligenz von Maschinen, die als „intelligente Agenten“ handeln. Als intelligenter Agent können bestimmte Geräte mit der Unterstützung von Software ihre Umgebung wahrnehmen und nach Maßgabe von Algorithmen Maßnahmen ergreifen. Der Begriff KI findet Anwendung, wenn eine Maschine „kognitive“ Funktionen wie Lernen und Problemlösung imitiert, die normalerweise mit natürlichen Personen in Zusammenhang gebracht werden würden.⁹⁸⁵ Zur Imitation der Entscheidungsfindung verwenden moderne Technologien und Softwareprogramme Algorithmen, die Geräte zur „automatisierten Entscheidungsfindung“ verwenden. Ein Algorithmus lässt sich am besten als schrittweises Verfahren für die Berechnung, Datenverarbeitung, Auswertung und automatisierte Argumentation und Entscheidungsfindung beschreiben.

Ebenso wie die Analyse von Big Data, erfordert KI und die von ihr erzeugte automatisierte Entscheidungsfindung die Sammlung und Verarbeitung großer Datenmengen. Diese Daten können vom Gerät selbst (Bremswärme, Kraftstoff, usw.) oder von dessen Umgebung stammen. Beim Profiling handelt es sich beispielsweise um ein Verfahren, das auf der automatisierten Entscheidungsfindung nach Maßgabe vorher festgelegter Gesetzmäßigkeiten oder Faktoren beruht.

Beispiel: Profiling und gezielte Werbung

Ein auf Big Data basierendes Profiling umfasst die Suche nach Gesetzmäßigkeiten, die „Eigenschaften eines Persönlichkeitstyps“ widerspiegeln, wie beispielsweise im Falle von Online-Kaufhäusern, die auf Grundlage der von den zuvor in den Einkaufswagen eines Kunden gelegten Produkte gesammelten Informationen Produkte anbieten, die „Ihnen

⁹⁸⁵ Stuart Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach* (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, S. 27, 32–58, 968–972; Stuart Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach* (2nd ed.), 2009, Upper Saddle River, New Jersey: Prentice Hall, S. 2.

ebenfalls gefallen könnten“. Je mehr Daten vorliegen, umso eindeutiger ist das Mosaik. Das Smartphone ist beispielsweise ein leistungsstarker Fragebogen, den die Einzelnen mit jeder Verwendung bewusst oder unbewusst vervollständigen.

Die moderne Psychographie (Wissenschaft der Erforschung von Persönlichkeiten) verwendet die OCEAN-Methode zur Bestimmung der Charaktertypen, mit denen sie es zu tun hat. Die „*Big Five*“ – Charakterdimensionen beziehen sich auf die Offenheit (wie offen die Person gegenüber Neuheiten ist), die Gewissenhaftigkeit (wie ähnlich die Person einem Perfektionisten ist), die Extraversion (wie gesellig die Person ist), die Verträglichkeit (wie verträglich die Person ist) und den Neurotizismus (wie verletzlich die Person ist). Diese Informationen erstellen ein Profil der besagten Person, ihrer Bedürfnisse und Ängste, ihrer Verhaltensmuster, usw. und werden dann durch weitere Informationen über die Person vervollständigt, die von allen verfügbaren Quellen erworben werden, darunter Datenvermittler, soziale Netzwerke (die unter Beiträge gesetzten „*Likes*“ und die eingestellten Fotos), online angehörte Musik oder GPS- und Trackingdaten.

Die durch Techniken der Massendatenanalyse erschaffene Menge an Profilen wird im Anschluss daran miteinander verglichen, um ähnliche Gesetzmäßigkeiten zu identifizieren und Persönlichkeitsgruppen zu konstruieren. Die Informationen über das Verhalten und die Einstellung bestimmter Persönlichkeiten werden folglich umgekehrt. Mit dem Zugang zu und der Verwendung von Big Data wird der Persönlichkeitstest umgekehrt und die Informationen über das Verhalten und die Einstellung zur Beschreibung der Persönlichkeit des Einzelnen verwendet. Durch den Besitz der kombinierten Informationen über die „*Likes*“ in sozialen Netzwerken, Trackingdaten, angehörte Musik oder angesehene Filme, kann ein klares Bild der Persönlichkeit einer Person entstehen, das Unternehmen die Übermittlung von maßgeschneiderter Werbung und/oder Informationen in Abhängigkeit von der „Persönlichkeit“ der betreffenden Person ermöglicht. Darüber hinaus können diese Informationen in Echtzeit verarbeitet werden.⁹⁸⁶

986 Verarbeitungstechniken und neue Softwareprogramme werten in Echtzeit die Informationen darüber aus, was einer Person gefällt, was sie sich beim Online-Einkauf ansieht oder einem Online-Einkaufswagen hinzufügt, und können „Produkte“ vorschlagen, die auf Grundlage der eingeholten Informationen interessant sein könnten.

10.1.2. Abwägung der Vorteile und Risiken von Big Data

Moderne Verarbeitungstechniken können große Datenmengen bewältigen, schnell neue Daten importieren, durch eine kurze Reaktionszeit die Echtzeit-Verarbeitung der Informationen gewährleisten (selbst im Falle komplexer Anfragen), die Möglichkeit mehrerer und gleichzeitiger Anfragen vorsehen und verschiedene Arten von Informationen (Fotos, Texte oder Zahlen) analysieren. Diese technologischen Innovationen ermöglichen die Strukturierung, Verarbeitung und Auswertung großer Mengen an Daten und Informationen in Echtzeit.⁹⁸⁷ Durch den exponentiellen Anstieg der Menge der verfügbaren und analysierten Daten können nunmehr Ergebnisse erzielt werden, die im Rahmen einer Analyse in kleinerem Umfang unmöglich wären. Big Data hat bei der Entwicklung eines neuen Geschäftsfelds geholfen, in dem sich für Unternehmen wie Verbraucher neue Dienstleistungen herausbilden können. Der Wert der personenbezogenen Daten von EU-Bürgern hat das Potenzial, bis 2020 auf nahezu 1 Billion Euro pro Jahr anzusteigen.⁹⁸⁸ Daher kann Big Data neue **Chancen** bieten, die sich aus ihrer Auswertung für neue soziale, wirtschaftliche oder wissenschaftliche Erkenntnisse ergeben, die einzelnen Personen ebenso zugutekommen wie Unternehmen und Regierungen.⁹⁸⁹

Durch Big Data können Gesetzmäßigkeiten zwischen verschiedenen Datenquellen und Datensätzen aufgedeckt werden, wodurch neue Erkenntnisse in Bereichen wie Wissenschaft und Medizin gewonnen werden können. Dies ist beispielsweise in Bereichen wie Gesundheit, Lebensmittelsicherheit, intelligente

987 Die Entwicklung von Software für die Verarbeitung von Massendaten befindet sich noch in einer frühen Phase. Gleichwohl wurden in jüngster Zeit insbesondere Analyseprogramme für die Echtzeit-Analyse von Massendaten und Masseninformationen in Bezug auf die Tätigkeiten von Personen entwickelt. Die Möglichkeit der strukturierten Analyse und Verarbeitung von Massendaten hat neue Mittel für Profiling und gezielte Werbung geliefert. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – „Für eine florierende datengesteuerte Wirtschaft“, COM(2014) 442 final, Brüssel, 2. Juli 2014; EU-Kommission, Factsheet „Die EU-Datenschutzreform und Big Data“ und Europarat, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. Januar 2017, S. 2.

988 EU-Kommission, Factsheet „Die EU-Datenschutzreform und Big Data“.

989 Internationale Konferenz der Datenschutzbeauftragten (2014) Entschließung zu Big Data und Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – „Für eine florierende datengesteuerte Wirtschaft“, COM(2014) 442 final, Brüssel, 2. Juli 2014, S. 2; EU-Kommission, Factsheet „Die EU-Datenschutzreform und Big Data“ und Europarat, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. Januar 2017, S. 1.

Transportsysteme, Energieeffizienz oder Stadtplanung der Fall. Diese Echtzeit-Analyse der Informationen kann zur Verbesserung der eingesetzten Systeme verwendet werden. Im Bereich der Forschung können durch die Kombination großer Datenmengen und statistischer Auswertungen neue Erkenntnisse gewonnen werden, was speziell für Wissenszweige gilt, in denen eine große Menge an Daten bislang nur manuell ausgewertet wurde. Auf der Grundlage von Vergleichen mit der Menge an verfügbaren Informationen können neue Behandlungsmethoden entwickelt werden, die auf die einzelnen Patienten zugeschnitten sind. Unternehmen hoffen, dass sie durch die Analyse von Big Data einen Wettbewerbsvorteil erhalten, potenzielle Einsparungen erzielen und durch einen direkten und individualisierten Kundendienst neue Geschäftsbereiche schaffen können. Regierungsbehörden erhoffen sich davon Verbesserungen im Bereich der Strafverfolgung. Die Strategie der Kommission für einen digitalen Binnenmarkt für Europa erkennt an, dass datengestützte Technologien, Dienstleistungen und Big Data potenziell als Katalysator für wirtschaftliches Wachstum, Innovation und Digitalisierung in der EU wirken können.⁹⁹⁰

Big Data birgt jedoch auch **Risiken**, die im Allgemeinen mit ihren drei Eigenschaften Menge, Geschwindigkeit und Vielfalt der verarbeiteten Daten verknüpft sind. Die Menge bezieht sich auf den Umfang der verarbeiteten Daten, die Vielfalt auf die Anzahl und die Verschiedenheit der Datenarten und die Geschwindigkeit auf das Tempo der Datenverarbeitung. Bestimmte Bedenken in Bezug auf den Datenschutz kommen insbesondere dann auf, wenn die Analyse von Big Data bei großen Datensätzen angewandt wird, um neue und vorausschauende Erkenntnisse für Entscheidungsfindungszwecke betreffend Einzelner und/oder Gruppen zu gewinnen.⁹⁹¹ Die mit Big Data verbundenen Risiken für den Datenschutz und die Privatsphäre wurden in Stellungnahmen

990 Europäisches Parlament, Entschließung vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatsphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)).

991 Europarat, Beratender Ausschuss für das Übereinkommen Nr. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. Januar 2017, S. 2.

des EDSB und der Artikel-29-Datenschutzgruppe, in Entschlüssen des Europäischen Parlaments und in Berichten des Europarates hervorgehoben.⁹⁹²

Diese Risiken können die falsche Handhabung von Massendaten seitens derjenigen beinhalten, die Zugang zu der Informationsmenge haben, was durch Manipulation, Diskriminierung oder Unterdrückung von Einzelnen oder bestimmten gesellschaftlichen Gruppen erfolgen kann.⁹⁹³ Wo große Mengen an personenbezogenen Daten oder Informationen über das Verhalten der Einzelnen erhoben, verarbeitet und ausgewertet werden, kann deren Verwertung zu bedeutenden Verletzungen der Grundrechte und Freiheiten führen, die über das Recht auf Privatsphäre hinausgehen. Die genaue Messung des Ausmaßes der Beeinträchtigung der Privatsphäre und der personenbezogenen Daten ist nicht möglich. Das Europäische Parlament erkannte, dass es noch keine Methode gibt, mit der die Auswirkungen von Big Data einer faktengestützten Bewertung unterzogen werden können, dass es jedoch Anzeichen dafür gibt, dass die Massendatenanalyse beträchtliche horizontale Auswirkungen auf den gesamten öffentlichen und privaten Sektor haben kann.⁹⁹⁴

Die DSGVO enthält das Recht, keiner automatisierten Entscheidungsfindung – einschließlich Profiling – unterworfen zu werden.⁹⁹⁵ Die Frage nach dem Datenschutz stellt sich, wenn die Ausübung des Widerspruchsrechts das Eingreifen einer Person erfordert, die den betroffenen Personen die Darlegung ihres eigenen Standpunkts und die Anfechtung der Entscheidung ermöglicht.⁹⁹⁶ Dies kann zu Problemen bei der Sicherstellung eines angemessenen Schutzniveaus für betroffene Personen führen. Sofern beispielsweise das Eingreifen einer Person nicht möglich ist oder die Algorithmen zu komplex und die beteiligte Datenmenge zu groß ist, um den Personen Gründe für

992 Siehe beispielsweise EDSB (2015), *Bewältigung der Herausforderungen in Verbindung mit Big Data*, Stellungnahme 7/2015, 19. November 2015; EDSB (2016), *Kohärente Durchsetzung von Grundrechten im Zeitalter von Big Data*, Stellungnahme 8/2016, 23. September 2016; Europäisches Parlament (2016), Entschließung zu den Folgen von Massendaten für die Grundrechte: Privatsphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung, P8_TA(2017)0076, Straßburg, 14. März 2017; Europarat, Beratender Ausschuss für das Übereinkommen Nr. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Straßburg, 23. Januar 2017.

993 Internationale Konferenz der Datenschutzbeauftragten (2014) Entschließung zu Big Data.

994 Europäisches Parlament, Entschließung vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatsphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)).

995 DSGVO, Artikel 22.

996 a.a.O., Artikel 22 Absatz 3.

bestimmte Entscheidungen zu liefern und/oder diese vorab zu unterrichten, um ihre Einwilligung zu erhalten. Ein Beispiel für den Einsatz von KI und automatisierter Entscheidungsfindung sind die jüngsten Entwicklungen im Bereich von Hypothekenanträgen oder Personaleinstellungsverfahren. Anträge/Bewerbungen werden aufgrund der Tatsache abgewiesen oder abgelehnt, dass die Antragsteller/Bewerber vorgegebene Parameter oder Faktoren nicht erfüllen.

10.1.3. Probleme im Zusammenhang mit dem Datenschutz

Was den Datenschutz anbelangt, so betreffen die Hauptprobleme einerseits die Menge und die Vielfalt der verarbeiteten Daten und andererseits die Verarbeitung und deren Ergebnisse. Die Einführung von komplexen Algorithmen und Softwareprogrammen zur Umwandlung von Big Data in eine Quelle für Entscheidungsfindungszwecke beeinträchtigt insbesondere Einzelne und Gruppen, und dies besonders in Fällen von Profiling oder Kennzeichnung, und wirft in letzter Zeit viele Fragen in Bezug auf den Datenschutz auf.⁹⁹⁷

Die Identifizierung von Verantwortlichen und Auftragsverarbeitern und deren Haftung

Big Data und KI werfen mehrere Fragen in Bezug auf die Identifizierung und die Haftung von Verantwortlichen und Auftragsverarbeitern auf: Wer ist im Falle der Erhebung und Verarbeitung einer solch großen Datenmenge der Besitzer der Daten? Wer ist im Falle der Verarbeitung durch Intelligenzgeräte und Softwareprogramme der Verantwortliche? Welche genauen Zuständigkeiten hat jeder Akteur bei der Verarbeitung? Und für welche Zwecke dürfen Big Data verwendet werden?

Die Haftungsfrage im Zusammenhang mit KI wird noch herausfordernder werden, wenn ein Gerät mit künstlicher Intelligenz eine Entscheidung trifft, die auf der von ihm selbst entwickelten Datenverarbeitung beruht. Die DSGVO sieht eine Haftung des Verantwortlichen und des Auftragsverarbeiters vor. Die unrechtmäßige Verarbeitung personenbezogener Daten löst die Haftung des

⁹⁹⁷ Europarat, Beratender Ausschuss für das Übereinkommen Nr. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. Januar 2017, S. 2.

Verantwortlichen und des Auftragsverarbeiters aus.⁹⁹⁸ Künstliche Intelligenz und automatisierte Entscheidungsfindung werfen Fragen darüber auf, wer für Verletzungen der Privatsphäre der betroffenen Personen haftet, wenn die Komplexität und Menge der verarbeiteten Daten nicht mit Sicherheit zugeordnet werden kann. Wenn KI und Algorithmen als Produkte betrachtet werden, entstehen Probleme zwischen der persönlichen Haftung, die in der DSGVO geregelt ist, und der Produkthaftung, die darin nicht geregelt ist.⁹⁹⁹ Dies würde beispielsweise Haftungsvorschriften erfordern, die die Lücke zwischen persönlicher Haftung und Produkthaftung für Robotik und KI einschließlich automatisierter Entscheidungsfindung füllen.¹⁰⁰⁰

Auswirkungen auf die Datenschutzgrundsätze

Die Beschaffenheit, die Analyse und die Verwendung der oben beschriebenen Big Data stellen die Anwendung einiger traditioneller und elementarer Grundsätze des europäischen Datenschutzrechtes in Frage.¹⁰⁰¹ Dies betrifft insbesondere die Grundsätze der Rechtmäßigkeit, der Datenminimierung, der Zweckbindung und der Transparenz.

Der Grundsatz der Datenminimierung erfordert, dass die personenbezogenen Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind. Das Geschäftsmodell der Big Data kann jedoch als Widerspruch zur Datenminimierung betrachtet werden, da es immer mehr Daten zu oftmals nicht festgelegten Zwecken erfordert.

Selbiges gilt für den Grundsatz der Zweckbindung, der erfordert, dass die Daten für festgelegte, Zwecke verarbeitet werden und nicht für Zwecke verwendet werden dürfen, die mit dem ursprünglichen Erhebungszweck unvereinbar sind, es sei denn, eine solche Verarbeitung beruht auf einer

998 DSGVO, Artikel 77–79 und Artikel 82.

999 Europäisches Parlament, *European Civil Law Rules in Robotics*, Generaldirektion Interne Politikbereiche, (Oktober 2016), S. 14.

1000 Rede von Roberto Viola auf dem Medienseminar zum europäischen Robotikrecht im Europäischen Parlament. (REDE 16.2.2017); Europäisches Parlament [Veröffentlichung](#) zu dem an die Kommission gerichteten Ersuchen um einen Vorschlag für Bestimmungen zur zivilrechtlichen Haftung für Robotik und KI.

1001 Europarat, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Straßburg, 23. Januar 2017.

Rechtsgrundlage wie beispielsweise der Einwilligung der betroffenen Person (siehe [Abschnitt 4.1.1](#)).

Schließlich stellt Big Data auch den Grundsatz der Richtigkeit der Daten in Frage, da Massendatenanwendungen danach streben, Daten aus vielen Quellen zu erheben, ohne die Möglichkeit zu haben, die Richtigkeit der erhobenen Daten zu prüfen und/oder aufrechtzuerhalten.¹⁰⁰²

Besondere Vorschriften und Rechte

Grundsätzlich fallen mittels Massendatenanalyse verarbeitete personenbezogene Daten in den Anwendungsbereich der Datenschutzvorschriften fallen. **Das Rechts des Europarates und das EU-Recht** haben für bestimmte Fälle im Zusammenhang mit algorithmischer komplexer Datenverarbeitung jedoch besondere Vorschriften oder Ausnahmen eingefügt.

Im Recht des Europarates garantiert das Modernisierte Übereinkommen 108 der betroffenen Person neue Rechte, um ihr in der Zeit von Big Data eine effektivere Kontrolle über ihre personenbezogenen Daten zu ermöglichen. Ein Beispiel hierfür sind etwa Artikel 9 Absatz 1 Buchstaben a, c und d des Modernisierten Übereinkommens. Sie beinhalten das Recht, nicht einer Entscheidung zu unterliegen, die die betroffene Person ernsthaft beeinträchtigt und ausschließlich auf automatisierter Datenverarbeitung basiert, ohne dass die Person ihren Standpunkt darlegen konnte; das Recht, auf Anfrage Kenntnis über die Begründung zu erlangen, die der Datenverarbeitung zugrunde liegt, wenn die Ergebnisse solcher Datenverarbeitung auf die Person angewandt werden; sowie das Recht, Widerspruch zu erheben. Andere Bestimmungen des Modernisierten Übereinkommens 108, insbesondere zu Transparenz und zusätzliche Verpflichtungen, sind ergänzende Elemente des Schutzmechanismus, der mit dem Modernisierten Übereinkommen 108 geschaffen wurde, um digitalen Herausforderungen zu begegnen.

Im EU-Recht muss außer in den in Artikel 23 DSGVO aufgelisteten Fällen **Transparenz** für jede Verarbeitung personenbezogener Daten gewährleistet sein. Dies ist besonders wichtig im Zusammenhang mit Internetdiensten und anderen komplexen automatisierten Datenverarbeitungen wie der Verwendung von

¹⁰⁰² EDSB (2016), *Kohärente Durchsetzung von Grundrechten im Zeitalter von Big Data*, Stellungnahme 8/2016, 23. September 2016, S. 8.

Algorithmen zur Entscheidungsfindung. Hier müssen Datenverarbeitungssysteme so gestaltet sein, dass betroffene Personen wirklich verstehen, was mit ihren Daten geschieht. Zur Gewährleistung einer fairen und transparenten Verarbeitung verpflichtet die DSGVO den Verantwortlichen, der betroffenen Person aussagekräftige Informationen über die in der automatisierten Entscheidungsfindung angewandte Logik, einschließlich Profiling, bereitzustellen.¹⁰⁰³ In seiner Empfehlung zum Schutz und zur Förderung des Rechts auf freie Meinungsäußerung und des Rechts auf Privatleben im Zusammenhang mit der Netzneutralität empfahl das Ministerkomitee des Europarates, dass Internetdiensteanbieter „den Nutzern eindeutige, vollständige und öffentlich zugängliche Informationen über die Praktiken zur Steuerung des Internetverkehrs bereitstellen, die den Zugang der Nutzer zu und die Verwendung von Daten, Anwendungen oder Diensten beeinträchtigen könnten“.¹⁰⁰⁴ Seitens der zuständigen Behörden in allen Mitgliedstaaten erstellte Berichte über die Praktiken zur Steuerung des Internetverkehrs sollten auf offene und transparente Weise ausgearbeitet und der Öffentlichkeit unentgeltlich bereitgestellt werden.¹⁰⁰⁵

Die Verantwortlichen müssen die betroffenen Personen sowohl wenn die Daten bei ihnen erhoben wurden als auch wenn diese nicht bei ihnen erhoben wurden nicht nur über spezifische Informationen über die erhobenen Daten und die geplante Verarbeitung **unterrichten** (siehe [Abschnitt 6.1.1](#)), sondern gegebenenfalls auch über das Bestehen automatisierter Entscheidungsfindungsverfahren, und ihnen „aussagekräftige Informationen über die angewandte Logik“,¹⁰⁰⁶ die Zielsetzungen und die potenziellen Auswirkungen dieser Verfahren bereitstellen. Die DSGVO verdeutlicht überdies (nur in Fällen, in denen die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden), dass der Verantwortliche nicht zur Bereitstellung dieser Informationen an die betroffene Person verpflichtet ist, wenn „die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde“.¹⁰⁰⁷ Wie die Artikel-29-Datenschutzgruppe in ihren *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* jedoch betont, sollte die Komplexität der

1003 DSGVO, Artikel 13 Absatz 2 Buchstabe f.

1004 Europarat, Ministerkomitee (2016), Recommendation CM/Rec(2016)1 of the Committee of Ministers to the Member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, 13. Januar 2016, Absatz 5.1.

1005 a.a.O., Absatz 5.2.

1006 DSGVO, Artikel 13 Absatz 2 Buchstabe f und Artikel 14 Absatz 2 Buchstabe g.

1007 a.a.O., Artikel 14 Absatz 5 Buchstabe b.

Verarbeitung für sich genommen den Verantwortlichen nicht daran hindern, der betroffenen Person eindeutige Erklärungen über die bei der Datenverarbeitung eingesetzten Zielsetzungen und Analysen bereitzustellen.¹⁰⁰⁸

Die Rechte der betroffenen Personen auf **Auskunft** über, **Berichtigung** und **Löschung** ihrer personenbezogenen Daten sowie ihr Recht auf **Einschränkung** der Verarbeitung enthalten keine vergleichbare Ausnahme. Die Pflicht des Verantwortlichen, der betroffenen Person jede Berichtigung oder Löschung ihrer personenbezogenen Daten mitzuteilen (siehe [Abschnitt 6.1.4](#)) kann jedoch auch aufgehoben werden, wenn eine solche Mitteilung „sich als unmöglich [erweist] oder [...] mit einem unverhältnismäßigen Aufwand verbunden [ist]“.¹⁰⁰⁹

Gemäß Artikel 21 DSGVO haben die betroffenen Personen auch das Recht, gegen die Verarbeitung sie betreffender personenbezogener Daten einschließlich in Fällen von Massendatenanalysen **Widerspruch einzulegen** (siehe [Abschnitt 6.1.6](#)). Die Verantwortlichen können von dieser Pflicht befreit werden, sofern sie vorrangige berechtigte Interessen nachweisen können, dies gilt nicht bei der Verarbeitung für Zwecke der Direktwerbung.

Auch bei der Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken können die Verantwortlichen besondere Ausnahmen von diesen Rechten geltend machen.¹⁰¹⁰

Im Zusammenhang mit **Profiling und automatisierter Entscheidungsfindung** hat die DSGVO besondere Vorschriften eingeführt: Artikel 22 Absatz 1 besagt, dass die betroffene Person „das Recht [hat], nicht einer ausschließlich auf einer automatisierten Verarbeitung [...] beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet“. Wie in den Leitlinien der Artikel-29-Datenschutzgruppe unterstrichen, enthält dieser Artikel ein allgemeines Verbot der vollautomatisierten Entscheidungsfindung.¹⁰¹¹ Die Verantwortlichen können von diesem Verbot nur in drei bestimmten Fällen

¹⁰⁰⁸ Artikel-29-Datenschutzgruppe, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3. Oktober 2017, S. 14.

¹⁰⁰⁹ DSGVO, Artikel 19.

¹⁰¹⁰ a.a.O., Artikel 89 Absatz 2 und 3.

¹⁰¹¹ Artikel-29-Datenschutzgruppe, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3. Oktober 2017, S. 9.

befreit werden: Wenn die Entscheidung 1) für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist, 2) aufgrund von Rechtsvorschriften der EU oder der Mitgliedstaaten zulässig ist, oder 3) mit ausdrücklicher Einwilligung erfolgt.¹⁰¹²

Individuelle Kontrolle

Die Komplexität und mangelnde Transparenz der Massendatenanalyse können ein Überdenken des Konzepts der individuellen Kontrolle personenbezogener Daten erfordern. Diese sollte auf den vorhandenen sozialen und technologischen Rahmen zugeschnitten werden und die mangelnden Kenntnisse der Einzelnen berücksichtigen. Demnach sollte Datenschutz in Bezug auf Big Data ein weiter gefasstes Konzept der Kontrolle über die Verwendung von Datenverfolgen, dem zufolge sich die individuelle Kontrolle zu einem komplexeren Prozess der mehrfachen Folgenabschätzung der mit der Verwendung der Daten verbundenen Risiken entwickelt.¹⁰¹³

Wie gut eine Massendatenanwendung ist, hängt davon ab, wie gut sie die Wünsche oder das Verhalten der Testpersonen (oder Verbraucher) vorhersagen kann. Die gegenwärtigen Vorhersagemodelle auf Grundlage der Massendatenanalyse werden kontinuierlich weiterentwickelt. Zu den jüngsten Entwicklungen zählt, dass die Daten nicht länger lediglich zur Kategorisierung von Persönlichkeiten verwendet werden (d. h. ihres Verhaltens und ihrer Einstellungen), sondern zur Analyse des Verhaltens mittels der Analyse von Sprachmustern und der Intensität, mit der Nachrichten eingetippt werden, oder der Körpertemperatur. Sämtliche dieser Informationen können in Echtzeit mit dem aus Massendatenauswertungen gewonnenen Wissen abgeglichen werden, um beispielsweise während eines Treffens mit einem Vertreter einer Bank die Kreditwürdigkeit zu beurteilen. Diese Beurteilung erfolgt nicht auf Grundlage der Eignung der den Kredit beantragenden Person, sondern vielmehr auf Grundlage der aus der Analyse und Auswertung von Massendateninformationen erhaltenen Verhaltensmerkmale, d. h. ob der Bewerber mit starker oder flatternder Stimme spricht, seine Körpersprache oder Körpertemperatur.

¹⁰¹² DSGVO, Artikel 22 Absatz 2.

¹⁰¹³ Europarat, Beratender Ausschuss für das Übereinkommen 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Straßburg, 23. Januar 2017.

Profiling und gezielte Werbung müssen nicht unbedingt ein Problem darstellen, sofern sich die Personen **darüber bewusst sind**, dass sie gezielten Werbeanzeigen unterliegen. Profiling wird zu einem Problem, wenn es zur Manipulation von Personen eingesetzt wird, d. h. zur Suche nach bestimmten Persönlichkeiten oder Personengruppen für politische Kampagnen. Gruppen unentschlossener Wähler können beispielsweise über politische Nachrichten angesprochen werden, die auf ihre „Persönlichkeit“ und Einstellung zugeschnitten sind. Ein anderes Problem könnte in der Nutzung des Profiling zur Verweigerung des Zugangs bestimmter Personen zu Waren und Dienstleistungen bestehen. Eine Maßnahme, die Schutz vor dem Missbrauch von Big Data und personenbezogenen Informationen bieten kann, ist die Pseudonymisierung (siehe [Abschnitt 2.1.1](#)).¹⁰¹⁴ Fälle, in denen personenbezogene Daten wirklich anonymisiert werden, d. h. keine Information vorliegt, die Spuren hinterlässt, die mit der betroffenen Person in Verbindung gebracht werden können, fallen nicht in den Anwendungsbereich der DSGVO. Auch die Einwilligung der betroffenen Person und anderer Personen in die Massendatenverarbeitung stellt eine Herausforderung für das Datenschutzrecht dar. Dies umfasst die Einwilligung dazu, gezielter Werbung und Profiling zu unterliegen, die aus Gründen einer „positiven Kundenerfahrung“ gerechtfertigt sein mögen, und die Einwilligung zur Verwendung großer Mengen personenbezogener Daten zur Weiterentwicklung und zum Ausbau von informationsbasierten Analyseinstrumenten. Das bestehende oder fehlende Bewusstsein über die Massendatenverarbeitung wirft mehrere Fragen in Bezug auf die Art und Weise auf, in der die betroffenen Personen ihre Rechte ausüben können, da die Massendatenverarbeitung sowohl auf pseudonymisierten als auch auf anonymisierten Informationen beruhen kann, die Algorithmen unterliegen. Während pseudonymisierte Daten in den Anwendungsbereich der DSGVO fallen, findet diese Verordnung auf anonymisierte Daten keine Anwendung. Die Kontrolle und das Bewusstsein der Personen über die Verarbeitung ihrer personenbezogenen Daten ist bei der Massendatenanalyse von entscheidender Bedeutung, da die Personen andernfalls die Identität des Verantwortlichen oder Auftragsverarbeiters nicht genau kennen, was sie an der wirksamen Ausübung ihrer Rechte hindert.

¹⁰¹⁴ a.a.O., S. 2.

10.2. Das Web 2.0 und das Web 3.0: Soziale Netzwerke und das Internet der Dinge

Kernpunkte

- Soziale Netzwerkdienste (SND) sind Online-Kommunikationsplattformen, die Personen den Beitritt zu oder die Erstellung von Netzwerken gleichgesinnter Nutzer ermöglichen.
- Das Internet der Dinge (IdD) ist die Verknüpfung von Gegenständen mit dem Internet und die Vernetzung dieser Gegenstände untereinander.
- Die Einwilligung der betroffenen Personen ist die gängigste Rechtsgrundlage für eine rechtmäßige Datenverarbeitung seitens der Verantwortlichen in Bezug auf soziale Netzwerke.
- Die Nutzer sozialer Netzwerke sind im Allgemeinen durch die „Haushaltsausnahme“ geschützt, die unter bestimmten Umständen jedoch aufgehoben werden kann.
- Die Anbieter sozialer Netzwerke sind nicht durch die „Haushaltsausnahme“ geschützt.
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sind entscheidend, um die Datensicherheit in diesem Bereich zu gewährleisten.

10.2.1. Bestimmung der Begriffe „Web 2.0“ und „Web 3.0“

Soziale Netzwerkdienste

Anfangs war das Internet als Netzwerk zur Vernetzung von Computern und zur Übertragung von Nachrichten konzipiert und verfügte lediglich über begrenzte Fähigkeiten zum Datenaustausch, da die Webseiten den Personen lediglich die Möglichkeit eines passiven Einblicks in ihre Inhalte boten.¹⁰¹⁵ Im Web-2.0-Zeitalter wurde das Internet in ein Forum umgewandelt, in dem die Nutzer interagieren, zusammenarbeiten und Beiträge erstellen. Dieses Zeitalter zeichnet

¹⁰¹⁵ Europäische Kommission, Arbeitsunterlage der Kommissionsdienststellen, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19. April 2016.

sich durch den großen Erfolg und die weitverbreitete Nutzung von sozialen Netzwerkdiensten aus, die nun wesentlicher Bestandteil im Alltagsleben von Millionen von Menschen sind.

Soziale Netzwerkdienste (SND) oder „soziale Medien“ können allgemein definiert werden als „Online-Kommunikationsplattformen, die Personen den Beitritt zu oder die Erstellung von Netzwerken gleichgesinnter Nutzer ermöglichen“.¹⁰¹⁶ Um einem Netzwerk beizutreten oder ein Netzwerk aufzubauen, werden die Personen zur Bereitstellung personenbezogener Daten und zur Erstellung ihres Profils aufgefordert. SND ermöglicht es den Nutzern, digitale „Inhalte“ zu generieren, die von Fotos und Videos über Zeitungslinks bis hin zu persönlichen Beiträgen reichen, um ihre Ansichten äußern. Über diese Online-Kommunikationsplattformen können die Nutzer interagieren und mit mehreren anderen Nutzern kommunizieren. Wichtig ist auch, dass die meisten beliebten SND keine Anmeldegebühren verlangen. Statt die Nutzer für den Beitritt zum Netzwerk zahlen zu lassen, erwirtschaften die Anbieter von SND den Großteil ihrer Einnahmen durch gezielte Werbung. Werbetreibende können in großem Umfang von den personenbezogenen Informationen profitieren, die tagtäglich auf diesen Seiten offenbart werden. Der Besitz von Informationen über das Alter, das Geschlecht, den Standort und die Interessen eines Nutzers ermöglicht ihnen, mit ihrer Werbung die „richtigen“ Personen anzusprechen.

Das Ministerkomitee des Europarates nahm eine Empfehlung zum Schutz der Menschenrechte in Zusammenhang mit sozialen Netzwerken an,¹⁰¹⁷ die dem Datenschutz einen speziellen Abschnitt widmet und 2018 durch eine weitere Empfehlung über die Aufgaben und Pflichten von Internetvermittlern ergänzt wurde.¹⁰¹⁸

Beispiel: Nora ist sehr glücklich, da ihr Partner ihr einen Heiratsantrag gemacht hat. Sie möchte die guten Neuigkeiten mit ihren Freunden und ihrer Familie teilen und beschließt, in einem sozialen Netzwerk einen emotionalen Beitrag zu verfassen, der ihrer Freude Ausdruck verleiht, und

¹⁰¹⁶ Artikel-29-Datenschutzgruppe (2009), *Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke*, WP 163, 12. Juni 2009, S. 4.

¹⁰¹⁷ Europarat, Ministerkomitee, *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services*, 4 April 2012.

¹⁰¹⁸ Europarat, Ministerkomitee, *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries*, 7 March 2018.

ihren Beziehungsstatus in „verlobt“ zu ändern. Immer wenn sich Nora in den darauf folgenden Tagen in ihren Account einloggt, sieht sie Werbung für Brautkleider und Blumengeschäfte. Warum ist das so?

Bei der Erstellung einer Werbeanzeige auf Facebook wählten die Brautkleider- und Blumengeschäfte bestimmte Parameter aus, um Personen wie Nora erreichen zu können. Wenn aus Noras Profil ersichtlich ist, dass sie eine Frau ist, verlobt ist und in Paris in der Nähe der die Werbeanzeige schaltenden Bekleidungs- und Blumengeschäfte lebt, werden ihr diese Werbeanzeigen unverzüglich angezeigt.

Internet der Dinge

Das Internet der Dinge (IdD) verkörpert den nächsten Schritt in der Entwicklung des Internets: Das Web-3.0-Zeitalter. Mit dem IdD können Geräte verbunden werden und interagieren über das Internet mit anderen Geräten. Dadurch können Gegenstände und Personen über Kommunikationsnetzwerke miteinander vernetzt sein, um über ihren Status und/oder den Status ihrer Umgebung zu berichten.¹⁰¹⁹ Das IdD und die damit verbundenen Geräte sind bereits Realität und es wird erwartet, dass es sich in den kommenden Jahren in starkem Maße ausdehnt, mit der Entwicklung und Weiterentwicklung intelligenter Geräte, die zum Aufbau intelligenter Städte, intelligenter Häuser und intelligenter Unternehmen führen.

Beispiel: Das IdD kann insbesondere der Gesundheitsversorgung zugutekommen. Unternehmen haben bereits Geräte, Sensoren und Anwendungen entwickelt, die die Überwachung des Gesundheitszustands eines Patienten ermöglichen. Durch die Nutzung eines tragbaren Alarmknopfes und anderer rund um die Wohnung angebrachter drahtloser Sensoren ist es möglich, den Tagesablauf älterer und allein lebender Menschen zu verfolgen und Alarm auszulösen, sobald ernsthafte Störungen in ihrer täglichen Routine festgestellt werden. Sturzerkennungssensoren werden beispielsweise von zahlreichen älteren Menschen genutzt. Diese Sensoren können Stürze genau feststellen und unterrichten den Arzt und/oder die Familie der betroffenen Person über den Sturz.

¹⁰¹⁹ Europäische Kommission, Arbeitsunterlage der Kommissionsdienststellen, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19. April 2016.

Beispiel: Barcelona ist eines der bekanntesten Beispiele für eine intelligente Stadt. Seit 2012 setzt die Stadt innovative Technologien ein, um intelligente Systeme in den Bereichen öffentlicher Personennahverkehr, Abfallwirtschaft, Parkplätze und Straßenbeleuchtung aufzubauen. Zur Verbesserung der Abfallwirtschaft setzt die Stadt beispielsweise intelligente Abfallbehälter ein. Diese ermöglichen die Überwachung des Füllstands der Abfallbehälter zur Optimierung der Sammelrouten. Wenn die Abfallbehälter fast voll sind, übermitteln sie über das mobile Kommunikationsnetz Signale, die an die seitens des Abfallwirtschaftsunternehmens verwendeten Softwareanwendungen gesendet werden. Auf diese Weise kann das Unternehmen die beste Route für die Abfallsammlung planen und die Abholung entweder auf die Behälter beschränken, die tatsächlich geleert werden müssen oder deren Leerung Vorrang einräumen.

10.2.2. Abwägung der Vorteile und Risiken

Die enorme Expansion und der Erfolg von SND im vergangenen Jahrzehnt deuten auf deren **beträchtliche Vorteile** hin. Zum Beispiel zielgerichtete Werbung (wie im Beispiel „Nora“) ist eine besonders effektive Möglichkeit für Unternehmen, ihre Kunden zu erreichen und dieser einen spezifischeren Produktmarkt anzubieten. Es könnte auch im Interesse der Verbraucher liegen, Werbeanzeigen unterbreitet zu bekommen, die besser auf sie abgestimmt und interessanter sind. Noch wichtiger ist allerdings, dass sich die sozialen Netzwerke und die sozialen Medien positiv auf die Gesellschaft und auf die Umsetzung von Reformen auswirken können. Sie befähigen die Nutzer zur Kommunikation, zur Interaktion und zur Organisation von Gruppen und Veranstaltungen zu Themen, die sie bewegen.

Ebenso wird erwartet, dass das IdD einen erheblichen Nutzen für die Wirtschaft bringt; zudem ist es Bestandteil der EU-Strategie zur Entwicklung eines digitalen Binnenmarktes. Schätzungen zufolge steigt die Anzahl der IdD-Verbindungen innerhalb der EU bis zum Jahr 2020 auf sechs Milliarden. Diese Ausbreitung der Vernetzung wird voraussichtlich erhebliche wirtschaftliche Vorteile bringen, und zwar durch die Entwicklung innovativer Dienste und Funktionen, einer besseren Gesundheitsversorgung, einem besseren Verständnis der Bedürfnisse der Verbraucher und verbesserter Leistungsfähigkeit.

Gleichzeitig, angesichts der großen Menge an personenbezogenen Daten, die die Nutzer sozialer Medien erzeugen und im Anschluss daran seitens der Betreiber der Dienste verarbeitet werden, geht die Expansion der SND gleichzeitig auch mit einer **wachsenden Sorge** darüber einher, wie die Privatsphäre und die personenbezogenen Daten geschützt werden können. SND können das Recht auf Privatsphäre und das Recht auf freie Meinungsäußerung gefährden. Zu diesen Gefahren können beispielsweise „der Mangel an Rechts- und Verfahrensgarantien rund um die Prozesse, die zum Ausschluss von Nutzern führen können; unangemessener Schutz von Kindern und Jugendlichen vor gefährlichen Inhalten oder Verhaltensweisen; mangelnde Achtung der Rechte anderer Personen; Fehlen von datenschutzfreundlichen Voreinstellungen; fehlende Transparenz über die Zwecke, zu denen personenbezogene Daten erhoben und verarbeitet werden“ gehören.¹⁰²⁰ Das europäische Datenschutzrecht hat versucht, auf die durch die sozialen Medien verursachten Herausforderungen für die Privatsphäre und den Datenschutz zu reagieren. Datenschutzgrundsätze wie die Einwilligung, der Schutz der Privatsphäre/Daten durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen und die Rechte der Einzelnen sind besonders wichtig im Zusammenhang mit sozialen Medien und Netzwerkdiensten.

Im Zusammenhang mit dem IdD hat die große Menge der von den verschiedenen vernetzten Geräten erzeugten personenbezogenen Daten auch Risiken für die Privatsphäre und den Datenschutz zur Folge. Obwohl Transparenz im europäischen Datenschutzrecht einen wichtigen Grundsatz darstellt, ist es aufgrund der Vielzahl der vernetzten Geräte nicht immer klar, wer die von IdD-Geräten erfassten Daten erheben, auf diese zugreifen und sie verwenden darf.¹⁰²¹ Im EU-Recht und im Recht des Europarates verpflichtet jedoch der Grundsatz der Transparenz die Verantwortlichen, die betroffenen Personen in klarer und einfacher Sprache darüber zu informieren, wie ihre Daten verwendet werden. Den betroffenen Personen müssen die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten deutlich gemacht werden. Die mit dem IdD verbundenen Geräte und die damit verbundenen zahlreichen Verarbeitungsvorgänge und Daten könnten auch das Erfordernis einer eindeutigen und in Kenntnis der Sachlage erfolgten Einwilligung in Frage stellen, sofern die Verarbeitung auf einer Einwilligung

1020 Europarat, Recommendation Rec (2012)4 to Member States on the protection of human rights with regard to social networking services, 4. April 2012.

1021 Europäischer Datenschutzbeauftragter (2017), *Understanding the Internet of Things*.

beruht. Den betroffenen Personen fehlt häufig das Verständnis der technischen Funktionsweise einer solchen Verarbeitung und demnach der Tragweite ihrer Einwilligung.

Ein weiteres wichtiges Anliegen betrifft die Sicherheit, da vernetzte Geräte sehr anfällig gegenüber Sicherheitsrisiken sind. Vernetzte Geräte haben unterschiedliche Sicherheitsniveaus. Da ihre Funktionsweise die gewöhnliche IT-Infrastruktur übersteigt, kann es sein, dass sie nicht über die angemessene Verarbeitungsleistung und Speicherfähigkeit verfügen, um Sicherheitssoftware zu hosten oder Techniken wie Verschlüsselung, Pseudonymisierung oder Anonymisierung anzuwenden, um die personenbezogenen Informationen der Nutzer zu schützen.

Beispiel: In Deutschland hat die Bundesnetzagentur beschlossen, ein mit dem Internet verbundenes Spielzeug zu verbieten, da starke Bedenken in Bezug auf dessen Auswirkungen auf die Achtung des Privatlebens von Kindern bestehen. Die Bundesnetzagentur war der Ansicht, dass eine mit dem Internet verbundene Puppe mit dem Namen Cayla ein verstecktes Spionagegerät darstelle. Die Funktionsweise der Puppe war wie folgt: Die seitens des mit der Puppe spielenden Kindes gestellten Fragen wurden an eine App auf einem digitalen Gerät übermittelt, die diese Fragen in Text übersetzte und im Internet nach einer Antwort suchte. Im Anschluss daran übermittelte die App eine Antwort an die Puppe, die diese dem Kind nannte. Über diese Puppe konnte die Kommunikation des Kindes und der sich in seiner Nähe befindenden Erwachsenen aufgezeichnet und an die App übermittelt werden. Hätte der Hersteller der Puppe keine geeigneten Sicherheitsmaßnahmen eingesetzt, hätte die Puppe von jedem zum Mithören der Kommunikation verwendet werden können.

10.2.3. Datenschutzthemen

Einwilligung

In Europa ist die Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn sie nach europäischem Datenschutzrecht erlaubt ist. Für Anbieter sozialer Netzwerke stellt die Einwilligung der betroffenen Personen im Allgemeinen eine rechtmäßige Grundlage für die Datenverarbeitung dar. Die

Einwilligung muss freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben werden (siehe [Abschnitt 4.1.1](#)).¹⁰²² „Freiwillig“ bedeutet vor allem, dass die betroffenen Personen eine wirkliche und echte Wahl haben müssen. Die Einwilligung ist „für den bestimmten Fall“ und „in informierter Weise“, wenn sie verständlich ist und sich klar und deutlich auf den gesamten Umfang, die gesamten Zwecke und die gesamten Folgen der Datenverarbeitung bezieht. Im Zusammenhang mit sozialen Medien können Zweifel darüber auftauchen, ob die Einwilligung für alle Arten der seitens des Betreibers der sozialen Netzwerke und Dritter durchgeführten Verarbeitung freiwillig, für den bestimmten Fall und in informierter Weise abgegeben wird.

Beispiel: Um einem SND beizutreten oder Zugang dazu zu erhalten, müssen die Personen häufig verschiedenen Arten der Verarbeitung ihrer personenbezogenen Daten zustimmen, oft ohne über die erforderlichen Vorgaben oder alternativen Lösungen informiert worden zu sein. Ein Beispiel wäre das Erfordernis, dem Erhalt verhaltensorientierter Internetwerbung zuzustimmen, um sich bei einem SND anmelden zu können. Wie die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme zur Definition von Einwilligung erwähnt: „Angesichts der Bedeutung, die einige soziale Netzwerke haben, werden manche Kategorien von Nutzern (wie Jugendliche) den Empfang von verhaltensorientierter Internetwerbung akzeptieren, um das Risiko zu vermeiden, von manchen sozialen Interaktionen teilweise ausgeschlossen zu werden. Der Nutzer sollte in der Lage sein, in den Erhalt der verhaltensorientierten Internetwerbung ohne Zwang und für den konkreten Fall einzuwilligen und zwar unabhängig von seinem Zugang zu den sozialen Netzwerkdiensten.“¹⁰²³

Nach Maßgabe der DSGVO können personenbezogene Daten von Kindern, die das sechzehnte Lebensjahr noch nicht vollendet haben, grundsätzlich nicht auf Grundlage ihrer Einwilligung verarbeitet werden.¹⁰²⁴ Sofern die Verarbeitung einer Einwilligung bedarf, ist diese vom Erziehungsberechtigten oder Vormund

¹⁰²² DSGVO, Artikel 4 und Artikel 7; Modernisiertes Übereinkommen Nr. 108, Artikel 5.

¹⁰²³ Artikel-29-Datenschutzgruppe (2011), *Stellungnahme 15/2011 zur Definition von Einwilligung*, WP 187, 13. Juli 2011, S. 18. Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (WP 259 rev.01).

¹⁰²⁴ Siehe DSGVO, Artikel 8. Die EU-Mitgliedstaaten können durch Rechtsvorschriften eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

des Kindes zu erteilen. Kinder verdienen besonderen Schutz, da sie sich der mit der Datenverarbeitung verbundenen Risiken und Folgen möglicherweise weniger bewusst sind. Dies ist besonders wichtig im Zusammenhang mit sozialen Medien, da Kinder anfälliger sind für einige der negativen Folgen, die die Nutzung dieser Dienste mit sich bringen kann, wie beispielsweise Cyber-Mobbing, Online-Stalking oder Identitätsdiebstahl.

Sicherheit und Wahrung der Privatsphäre/Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Die Verarbeitung personenbezogener Daten bringt von Natur aus Sicherheitsrisiken mit sich, da ständig eine Sicherheitslücke auftreten kann, die zu einer unbeabsichtigten oder unrechtmäßigen, Vernichtung, zum Verlust, zur Veränderung, oder zum unbefugten Zugang zu beziehungsweise zur unbefugten Offenlegung der verarbeiteten personenbezogenen Daten führt. Nach Maßgabe des europäischen Datenschutzrechts sind Verantwortliche und Auftragsverarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um unbefugte Eingriffe in Datenverarbeitungsvorgänge zu verhindern. Die Anbieter sozialer Netzwerke, die in den Anwendungsbereich der europäischen Datenschutzvorschriften fallen, müssen dieser Verpflichtung ebenfalls nachkommen.

Die Grundsätze der Wahrung der Privatsphäre/des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen verpflichten die Verantwortlichen, bei der Planung ihrer Produkte die Sicherheit zu wahren und automatisch geeignete Privatsphäre- und Datenschutzeinstellungen anzuwenden. Dies bedeutet, dass der Diensteanbieter im Falle der Entscheidung einer Person zum Beitritt zu einem sozialen Netzwerk nicht automatisch allen übrigen Nutzern sämtliche Informationen über den neuen Nutzer zugänglich machen darf. Beim Beitritt zu dem Dienst sollten die Privatsphäre- und Datenschutzeinstellungen derart sein, dass solche Informationen ausschließlich den gewählten Kontakten der Person zur Verfügung stehen. Erweiterter Zugriff für Personen, die nicht auf dieser Liste stehen, sollte erst möglich sein, nachdem der Nutzer die Standardeinstellungen in Bezug auf die Privatsphäre und den Datenschutz manuell geändert hat. Dies kann sich auch auf Fälle auswirken, in denen trotz der eingerichteten Sicherheitsmaßnahmen eine Datenschutzverletzung auftritt. Hat diese voraussichtlich ein hohes Risiko für die

persönlichen Rechte und Freiheiten der betroffenen Personen zur Folge, so müssen die Diensteanbieter in solchen Fällen die betroffenen Nutzer darüber unterrichten.¹⁰²⁵

Privatsphäre/Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sind besonders wichtig im Zusammenhang mit SND, da das Teilen personenbezogener Daten in den sozialen Medien zusätzlich zu den bei den meisten Arten der Verarbeitung bestehenden Risiken des Zugangs Unbefugter noch weitere Sicherheitsrisiken birgt. Diese sind häufig darauf zurückzuführen, dass den Personen das Verständnis darüber fehlt, wer Zugang zu ihren Informationen haben kann und auf welche Weise diese Personen ihre Informationen gegebenenfalls verwenden. Mit der weitverbreiteten Nutzung sozialer Medien erhöhte sich die Anzahl der Identitätsdiebstähle und der diesbezüglichen Opfer.

Beispiel: Identitätsdiebstahl ist ein Phänomen, in dessen Rahmen eine Person in den Besitz von Informationen, Daten oder Dokumenten einer anderen Person (dem Opfer) gelangt, und diese Informationen im Anschluss daran dazu verwendet, sich als das Opfer auszugeben, um in dessen Namen Waren und Dienstleistungen zu erhalten. Nehmen wir beispielsweise Paul, der auf einer Social-Media-Website angemeldet ist. Paul ist Lehrer und aktives Mitglied seiner Community, sehr aufgeschlossen und macht sich keine übermäßigen Sorgen über die Privatsphäre- und Datenschutzeinstellungen seines Social-Media-Accounts. Er hat eine große Liste von Kontakten, zu denen zuweilen auch Leute gehören, die er nicht unbedingt persönlich kennt. Da er in einer großen Schule arbeitet und als Trainer der Fußballmannschaft der Schule recht bekannt ist, geht er davon aus, dass es sich bei diesen Leuten höchstwahrscheinlich um Eltern oder um Freunde der Schule handelt. Pauls E-Mail-Adresse und sein Geburtsdatum werden in seinem Social-Media-Account angezeigt. Darüber hinaus postet Paul regelmäßig Fotos von seinem Hund Toby, begleitet von Zeilen wie „Ich und Toby bei unserem morgendlichen Lauf“. Paul war sich nicht darüber bewusst, dass eine der gängigsten Sicherheitsfragen zum Schutz seines E-Mail- oder Handy-Accounts wie folgt lautet: „Wie heißt Ihr Haustier?“. Unter Verwendung der auf Pauls Social-Media-Profil verfügbaren Informationen gelingt es Nick problemlos, den Account von Paul zu hacken.

¹⁰²⁵ a.a.O., Artikel 34.

Rechte der Personen

Die Anbieter von SND müssen die Rechte der Personen achten (siehe [Abschnitt 6.1](#)), einschließlich des Rechts auf Unterrichtung über den Zweck der Verarbeitung und wie personenbezogene Daten zu Zwecken der Direktwerbung genutzt werden können. Den Personen muss auch das Recht auf Auskunft über die von ihnen auf der Plattform des sozialen Netzwerks erzeugten personenbezogenen Daten gewährt werden, sowie das Recht auf Löschung. Selbst in Fällen, in denen Personen in die Verarbeitung personenbezogener Daten eingewilligt und online Informationen hochgeladen haben, sollten sie in der Lage sein, das „Vergessenwerden“ zu verlangen, sofern sie die Dienstleistungen des sozialen Netzwerks nicht länger in Anspruch nehmen möchten. Das Recht auf Datenübertragbarkeit ermöglicht den Nutzern darüber hinaus, in einem strukturierten, gängigen und maschinenlesbaren Format eine Kopie der personenbezogenen Daten zu erhalten, die sie dem Anbieter der sozialen Netzwerkdienste bereitgestellt haben, und ihre Daten von einem Anbieter sozialer Netzwerkdienste an einen anderen zu übermitteln.¹⁰²⁶

Verantwortliche

Eine schwierige Frage, die sich im Zusammenhang mit sozialen Medien oftmals stellt, ist die Frage nach der Identität des Verantwortlichen, d. h. wer ist die Person, der die Verpflichtung und Zuständigkeit für die Einhaltung der Datenschutzvorschriften obliegt. Anbieter sozialer Netzwerkdienste werden nach dem europäischen Datenschutzrecht als Verantwortliche betrachtet. Aufgrund der breitgefassten Definition des Begriffs „Verantwortlicher“ und der Tatsache, dass diese Diensteanbieter über die Zwecke und Mittel der Verarbeitung der seitens der betroffenen Personen geteilten personenbezogenen Daten entscheiden, liegt dies auf der Hand. Im EU-Recht sind Verantwortliche, die Dienstleistungen an betroffene Personen in der EU bereitstellen, zur Einhaltung der Bestimmungen der DSGVO selbst dann verpflichtet, wenn sie nicht in der EU niedergelassen sind.

Können aber auch Nutzer sozialer Netzwerkdienste als Verantwortliche betrachtet werden? Wenn Personen personenbezogene Daten „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ verarbeiten, finden die Datenschutzvorschriften keine Anwendung. Dies wird im europäischen

¹⁰²⁶ DSGVO, Artikel 21.

Datenschutzrecht als „Haushaltsausnahme“ bezeichnet. Ein Nutzer sozialer Netzwerkdienste kann jedoch in einigen Fällen nicht unter die Haushaltsausnahme fallen.

Nutzer teilen ihre personenbezogenen Informationen freiwillig online. Gleichwohl enthalten die online geteilten Informationen oftmals auch personenbezogene Informationen anderer Personen.

Beispiel: Paul ist bei einer sehr bekannten Plattform eines sozialen Netzwerks registriert. Paul versucht, Schauspieler zu werden und nutzt seinen Account zum Posten von Fotos, Videos und Beiträgen, aus denen seine Leidenschaft für Kunst hervorgeht. Da seine Beliebtheit wichtig für seine Zukunft ist, entschied er, dass sein Profil nicht nur der engen Liste seiner Kontakte, sondern allen Internetnutzern zur Verfügung stehen solle, unabhängig davon, ob diese Mitglieder des Netzwerks sind oder nicht. Kann Paul Fotos und Videos posten, die ihn zusammen mit seiner Freundin Sarah zeigen, ohne dass diese ihre Einwilligung gegeben hat? Als Grundschullehrerin versucht Sarah, ihr Privatleben von ihrem Arbeitgeber, ihren Schülern und deren Eltern fernzuhalten. Stellen wir uns vor, dass Sarah, die keine sozialen Netzwerke nutzt, von ihrem gemeinsamen Freund Nick erfährt, dass ein Foto gepostet wurde, das sie mit Paul auf einer Party zeigt. In einem solchen Fall fällt die seitens Paul durchgeführte Datenverarbeitung nicht unter das EU-Recht, sondern unter die „Haushaltsausnahme“.

Für die Nutzer ist es jedoch nach wie vor von entscheidender Bedeutung, sich der Tatsache bewusst zu sein und darauf zu achten, dass das Hochladen von Informationen über andere Personen ohne deren Einwilligung ihre Rechte auf Wahrung der Privatsphäre/ Datenschutz verletzen kann. Selbst wenn die Haushaltsausnahme Anwendung findet, wie beispielsweise wenn das Profil eines Nutzers lediglich einer Liste von seitens ihm ausgewählter Kontakte zugänglich ist, kann er wegen der Veröffentlichung personenbezogener Informationen über andere haftbar sein. Obgleich die Datenschutzvorschriften im Falle der Anwendung der Haushaltsausnahme keine Anwendung finden, kann die Haftung durch die Anwendung anderer nationaler Rechtsvorschriften wie Rechtsvorschriften zu Verleumdung oder Persönlichkeitsverletzung ausgelöst werden. Schließlich sind ausschließlich Nutzer von SND durch die Haushaltsausnahme geschützt: Verantwortliche und Auftragsverarbeiter, die die

Instrumente für eine solche private Verarbeitung bereitstellen, fallen in den Anwendungsbereich des europäischen Datenschutzrechts.¹⁰²⁷

Mit der Reform der Datenschutzrichtlinie für elektronische Kommunikation sollen die nach Maßgabe des derzeitigen Rechtsrahmens für Anbieter von Telekommunikationsdiensten geltenden Vorschriften über den Datenschutz, die Privatsphäre und die Sicherheit auch auf den automatisierten Informationsaustausch zwischen Endgeräten und auf elektronische Kommunikationsdienste Anwendung finden, das heißt einschließlich der Kommunikationsdienste, die über das Internet angeboten werden (sogenannte „Over-The-Top-Kommunikationsdienste“).

¹⁰²⁷ a.a.O., Erwägungsgrund 18.

Weiterführende Literatur

Kapitel 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Wien, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. „Four fundamental rights: finding the balance“, *International Data Privacy Law*, Vol. 6, Nr. 3, S. 195–209.

EDRi, *An introduction to data protection*, Brüssel.

Frowein, J. und Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. und Gellert, G. (2012), „The fundamental right of data protection in the European Union: in search of an uncharted right“, *International Review of Law, Computers and Technology*, Vol. 26 (1), S. 73–82.

Grabenwarter, C. und Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Gutwirth, S., Pouillet, Y., de Hert, P., de Terwange, C. und Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. und Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), 'EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation'.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Kokott, J. und Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR“, *International Data Privacy Law*, Vol. 3, Nr. 4, S. 222–228.

Kranenborg, H. (2015), „Google and the Right to be Forgotten“, *European Data Protection Law Review*, Vol. 1, Nr. 1, S. 70–79.

Lynskey, O. (2014), „Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order“, *International and Comparative Law Quarterly*, Vol. 63, Nr. 3, S. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. und Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. und Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brüssel, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?“, *Neue Juristische Wochenschrift*, Nr. 5, S. 281–288.

Warren, S. und Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review*, Vol. 4, Nr. 5, S. 193–220.

White, R. und Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Kapitel 2

Acquisty, A., und Gross R. (2009), *Proceedings of the National Academy of Science*, 7. Juli 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., und Blondel V. D. (2013), „Unique in the Crowd: the Privacy Bounds of Human Mobility“, *Nature Scientific Reports*, Vol. 3, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. und Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization“, *UCLA Law Review*, Vol. 57, Nr. 6, S. 1701–1777.

Samarati, P. and Sweeney, L. (1998), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression“, Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), „K-Anonymity: A Model for Protecting Privacy“ *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, Nr. 5, S. 557–570.

Tinnefeld, M., Buchner, B. und Petri, T. (2018), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenburg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*.

Kapitel 3 bis 6

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ in: Grabitz, E., Hilf, M. und Nettesheim, M. (Hrsg.), *Das Recht der Europäischen Union*, Band IV, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Curren, L. und Kaye, J. (2010), „Revoking consent: a ‘blind spot’ in data protection law?“, *Computer Law & Security Review*, Vol. 26, Nr. 3, S. 273–283.

Dammann, U. und Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. und Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis“, *Computers & Law Magazine of SCL*, Vol. 22, Nr. 6, S. 1–5.

De Hert, P. und Papakonstantinou, V. (2012), „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals“, *Computer Law & Security Review*, Vol. 28, Nr. 2, S. 130–142.

Feretti, Federico (2012), „A European perspective on data processing consent through the re-conceptualization of European data protection’s looking glass after the Lisbon treaty: Taking rights seriously“, *European Review of Private Law*, Vol. 20, Nr. 2, S. 473–506.

FRA (Agentur der Europäischen Union für Grundrechte) (2010), *Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden (Stärkung der Grundrechtearchitektur in der EU II)*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union (Amt für Veröffentlichungen).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Konferenzausgabe), Wien, FRA.

FRA (2011), *Zugang zur Justiz in Europa: Ein Überblick über Herausforderungen und Chancen*, Luxemburg, Amt für Veröffentlichungen.

Irish Health Information and Quality Authority (2010), *Guidance on Privacy Impact Assessment in Health and Social Care*.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. and Saxby, S. (2011), „30 years on – The review of the Council of Europe Data Protection Convention 108“, *Computer Law & Security Review*, Vol. 27, Nr. 3, S. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner’s Office, *Privacy Impact Assessment*.

Kapitel 7

Artikel-29-Datenschutzgruppe (2005), *Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995*.

Europäischer Datenschutzbeauftragter (2014), *Positionspapier zur Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU*.

Gutwirth, S., Pouillet, Y., De Hert, P., De Terwangne, C. und Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Kapitel 8

Blasi Casagran, C. (2016), *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Berlin, Springer.

De Hert, P. und Papakonstantinou, V. (2012), „[The Police and Criminal Justice Data Protection Directive: Comment and Analysis](#)“, *Computers & Law Magazine of SCL*, Vol. 22, Nr. 6, S. 1–5.

Drewer, D. und Ellermann, J. (2012), „Europol’s data protection framework as an asset in the fight against cybercrime“, *ERA Forum*, Vol. 13, Nr. 3, S. 381–395.

Europol (2012), [Data Protection at Europol](#), Luxemburg, Amt für Veröffentlichungen.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Den Haag, Eurojust.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Pouillet, Y. und De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Pouillet, Y., De Hert, P. und Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem“, *European Law Review*, Vol. 36, Nr. 5, S. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Kapitel 9

Büllesbach, A., Gijrath, S., Pouillet, Y. und Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. und Pouillet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Pouillet, Y. und De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Pouillet, Y., De Hert, P. und Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem“, *European Law Review*, Vol. 36, Nr. 5, S. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Kapitel 10

El Emam, K. und Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques“, *International Data Privacy Law*, Vol. 5, Nr. 1, S. 73–87.

Mayer-Schönberger, V und Cate, F. (2013), „Notice and consent in a world of Big Data“, *International Data Privacy Law*, Vol. 3, Nr. 2, S. 67–73.

Rubinstein, I. (2013), „Big Data: The End of Privacy or a New Beginning?“, *International Data Privacy Law*, Vol. 3, Nr. 2, S. 74–87.

Verzeichnis der Rechtssachen

Ausgewählte Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte

Zugang zu personenbezogenen Daten

Gaskin / Vereinigtes Königreich, Nr. 10454/83, 7. Juli 1989

Godelli / Italien, Nr. 33783/09, 25. September 2012

K.H. und andere / Slowakei, Nr. 32881/04, 28. April 2009

Leander / Schweden, Nr. 9248/81, 26. März 1987

M.K. / Frankreich, Nr. 19522/09, 18. April 2013

Odièvre / Frankreich [GK], Nr. 42326/98, 13. Februar 2003

Abwägung von Datenschutz und Meinungsfreiheit und dem Recht auf Information

Axel Springer AG / Deutschland [GK], Nr. 39954/08, 7. Februar 2012

Bohlen / Deutschland, Nr. 53495/09, 19. Februar 2015

Coudec und Hachette Filipacchi Associés / Frankreich [GK], Nr. 40454/07, 10. November 2015

Magyar Helsinki Bizottság / Ungarn [GK], Nr. 18030/11, 8. November 2016

Müller und andere / Schweiz, Nr. 10737/84, 24. Mai 1988

Satakunnan Markkinapörssi Oy und Satamedia Oy / Finnland, Nr. 931/13, 27. Juni 2017

Vereinigung bildender Künstler / Österreich, Nr. 68345/01, 25. Januar 2007

Von Hannover / Deutschland (Nr. 2) [GK], Nrn. 40660/08 und 60641/08, 7. Februar 2012

Abwägung von Datenschutz und Religionsfreiheit

Sinan Işık / Türkei, Nr. 21924/05, 2. Februar 2010

Herausforderungen beim Online-Datenschutz

K.U. / Finnland, Nr. 2872/02, 2. Dezember 2008

Einwilligung der betroffenen Person

Elberte / Lettland, Nr. 61243/08, 13. Januar 2015

Sinan Işık / Türkei, Nr. 21924/05, 2. Februar 2010

Y / Türkei, Nr. 648/10, 17. Februar 2015

Korrespondenz

Amann / Schweiz [GK], Nr. 27798/95, 16. Februar 2000

Association for European Integration and Human Rights und Ekimdzhiev / Bulgarien, Nr. 62540/00, 28. Juni 2007

Bernh Larsen Holding AS und andere / Norwegen, Nr. 24117/08, 14. März 2013

Cemalettin Canli / Türkei, Nr. 22427/04, 18. November 2008

D.L. / Bulgarien, Nr. 7472/14, 19. Mai 2016

Dalea / Frankreich, Nr. 964/07, 2. Februar 2010

Gaskin / Vereinigtes Königreich, Nr. 10454/83, 7. Juli 1989

Haralambie / Rumänien, Nr. 21737/03, 27. Oktober 2009

Khelili / Schweiz, Nr. 16188/07, 18. Oktober 2011

Leander / Schweden, Nr. 9248/81, 26. März 1987

Malone / Vereinigtes Königreich, Nr. 8691/79, 2. August 1984

Rotaru / Rumänien [GK], Nr. 28341/95, 4. Mai 2000

S. und Marper / Vereinigtes Königreich [GK], Nrn. 30562/04 und 30566/04, 4. Dezember 2008

Shimovolos / Russland, Nr. 30194/09, 21. Juni 2011

Silver und andere / Vereinigtes Königreich, Nrn. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. März 1983

The Sunday Times / Vereinigtes Königreich, Nr. 6538/74, 26. April 1979

Strafregisterdatenbanken

Aycaguer / Frankreich, Nr. 8806/12, 22. Juni 2017

B.B. / Frankreich, Nr. 5335/06, 17. Dezember 2009

Brunet / Frankreich, Nr. 21010/10, 18. September 2014

M.K. / Frankreich, Nr. 19522/09, 18. April 2013
M.M. / Vereinigtes Königreich, Nr. 24029/07, 13. November 2012

Datensicherheit

Haralambie / Rumänien, Nr. 21737/03, 27. Oktober 2009
K.H. und andere / Slowakei, Nr. 32881/04, 28. April 2009

DNA-Datenbanken

S. und Marper / Vereinigtes Königreich [GK], Nrn. 30562/04 und 30566/04,
4. Dezember 2008

GPS-Daten

Uzun / Deutschland, Nr. 35623/05, 2. September 2010

Gesundheitsdaten

Avilkina und andere / Russland, Nr. 1585/09, 6. Juni 2013
Biriuk / Litauen, Nr. 23373/03, 25. November 2008
I / Finnland, Nr. 20511/03, 17. Juli 2008
L.H. / Lettland, Nr. 52019/07, 29. April 2014
L.L. / Frankreich, Nr. 7508/02, 10. Oktober 2006
M.S. / Schweden, Nr. 20837/92, 27. August 1997
Szuluk / Vereinigtes Königreich, Nr. 36936/05, 2. Juni 2009
Y / Türkei, Nr. 648/10, 17. Februar 2015
Z / Finnland, Nr. 22009/93, 25. Februar 1997

Identität

Ciubotaru / Republik Moldau, Nr. 27138/04, 27. April 2010
Godelli / Italien, Nr. 33783/09, 25. September 2012
Odièvre / Frankreich [GK], Nr. 42326/98, 13. Februar 2003

Informationen über berufliche Tätigkeiten

G.S.B. / Schweiz, Nr. 28601/11, 22. Dezember 2015
M.N. und andere / San Marino, Nr. 28005/12, 7. Juli 2015
Michaud / Frankreich, Nr. 12323/11, 6. Dezember 2012
Niemietz / Deutschland, Nr. 13710/88, 16. Dezember 1992

Überwachung des Kommunikationsverkehrs

Amann / Schweiz [GK], Nr. 27798/95, 16. Februar 2000
Brito Ferrinho Bexiga Villa-Nova / Portugal, Nr. 69436/10, 1. Dezember 2015
Copland / Vereinigtes Königreich, Nr. 62617/00, 3. April 2007
Halford / Vereinigtes Königreich, Nr. 20605/92, 25. Juni 1997
Iordachi und andere / Republik Moldau, Nr. 25198/02, 10. Februar 2009
Kopp / Schweiz, Nr. 23224/94, 25. März 1998
Liberty und andere / Vereinigtes Königreich, Nr. 58243/00, 1. Juli 2008
Malone / Vereinigtes Königreich, Nr. 8691/79, 2. August 1984
Mustafa Sezgin Tanrikulu / Türkei, Nr. 27473/06, 18. Juli 2017
Pruteanu / Rumänien, Nr. 30181/05, 3. Februar 2015
Szuluk / Vereinigtes Königreich, Nr. 36936/05, 2. Juni 2009

Pflichten der Verantwortlichen

B.B. / Frankreich, Nr. 5335/06, 17. Dezember 2009
I / Finnland, Nr. 20511/03, 17. Juli 2008
Mosley / Vereinigtes Königreich, Nr. 48009/08, 10. Mai 2011

Personenbezogene Daten

Amann / Schweiz [GK], Nr. 27798/95, 16. Februar 2000
Bernh Larsen Holding AS und andere / Norwegen, Nr. 24117/08, 14. März 2013
Uzun / Deutschland, Nr. 35623/05, 2. September 2010

Lichtbilder

Sciacca / Italien, Nr. 50774/99, 11. Januar 2005
Von Hannover / Deutschland, Nr. 59320/00, 24. Juni 2004

Recht auf Vergessenwerden

Satakunnan Markkinapörssi Oy und Satamedia Oy / Finnland, Nr. 931/13, 27. Juni 2017
Segerstedt-Wiberg und andere / Schweden, Nr. 62332/00, 6. Juni 2006

Widerspruchsrecht

Leander / Schweden, Nr. 9248/81, 26. März 1987
M.S. / Schweden, Nr. 20837/92, 27. August 1997
Mosley / Vereinigtes Königreich, Nr. 48009/08, 10. Mai 2011

Rotaru / Rumänien [GK], Nr. 28341/95, 4. Mai 2000
Sinan Işık / Türkei, Nr. 21924/05, 2. Februar 2010

Sensible Datenkategorien

Brunet / Frankreich, Nr. 21010/10, 18. September 2014
I / Finnland, Nr. 20511/03, 17. Juli 2008
Michaud / Frankreich, Nr. 12323/11, 6. Dezember 2012
S. und Marper / Vereinigtes Königreich [GK], Nrn. 30562/04 und 30566/04, 4. Dezember 2008

Aufsicht und Durchsetzung (Rolle der verschiedenen Akteure einschließlich der Aufsichtsbehörden)

I / Finnland, Nr. 20511/03, 17. Juli 2008
K.U. / Finnland, Nr. 2872/02, 2. Dezember 2008
Von Hannover / Deutschland, Nr. 59320/00, 24. Juni 2004
Von Hannover / Deutschland (Nr. 2) [GK], Nrn. 40660/08 und 60641/08, 7. Februar 2012

Überwachungsmethoden

Allan / Vereinigtes Königreich, Nr. 48539/99, 5. November 2002
Association for European Integration and Human Rights und Ekimdzhiev / Bulgarien, Nr. 62540/00, 28. Juni 2007
Bărbulescu / Rumänien [GK], Nr. 61496/08, 5. September 2017
D.L. / Bulgarien, Nr. 7472/14, 19. Mai 2016
Dragojević / Kroatien, Nr. 68955/11, 15. Januar 2015
Karabeyoğlu / Türkei, Nr. 30083/10, 7. Juni 2016
Klass und andere / Deutschland, Nr. 5029/71, 6. September 1978
Rotaru / Rumänien [GK], Nr. 28341/95, 4. Mai 2000
Szabó und Vissy / Ungarn, Nr. 37138/14, 12. Januar 2016
Taylor-Sabori / Vereinigtes Königreich, Nr. 47114/99, 22. Oktober 2002
Uzun / Deutschland, Nr. 35623/05, 2. September 2010
Versini-Campinchi und Crasnianski / Frankreich, Nr. 49176/11, 16. Juni 2016
Vetter / Frankreich, Nr. 59842/00, 31. Mai 2005
Vukota-Bojić / Schweiz, Nr. 61838/10, 18. Oktober 2016
Roman Zakharov / Russland [GK], Nr. 47143/06, 4. Dezember 2015

Video-Überwachung

Köpke / Deutschland, Nr. 420/07, 5. Oktober 2010

Peck / Vereinigtes Königreich, Nr. 44647/98, 28. Januar 2003

Stimmproben

P.G. und J.H. / Vereinigtes Königreich, Nr. 44787/98, 25. September 2001

Wisse / Frankreich, Nr. 71611/01, 20. Dezember 2005

Ausgewählte Rechtsprechung des Gerichtshofs der Europäischen Union

Rechtsprechung zur Datenschutzrichtlinie

EuGH, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde / Rīgas pašvaldības SIA „Rīgas satiksme“*, 4. Mai 2017

[Grundsatz der rechtmäßigen Verarbeitung: berechtigtes Interesse eines Dritten]

EuGH, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni*, 9. März 2017

[Recht auf Löschung personenbezogener Daten; Recht auf Widerspruch gegen die Verarbeitung]

Verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB / Post-och telestyrelsen und Secretary of State for the Home Department / Tom Watson und andere* [GK], 21. Dezember 2016

[Vertraulichkeit der elektronischen Kommunikation; Betreiber elektronischer Kommunikationsdienste; Pflicht zur allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten; keine vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde; Charta der Grundrechte der Europäischen Union; Vereinbarkeit mit dem Unionsrecht]

EuGH, C-582/14, *Patrick Breyer / Bundesrepublik Deutschland*, 19. Oktober 2016

[Begriff „personenbezogene Daten“; Internetprotokoll-Adressen; Speicherung durch einen Anbieter von Online-Mediendiensten; nationale Regelung, die eine Berücksichtigung des berechtigten Interesses des für die Verarbeitung Verantwortlichen nicht zulässt]

C-362/14, *Maximilian Schrems / Data Protection Commissioner* [GK], 6. Oktober 2015

[Grundsatz der rechtmäßigen Verarbeitung; Grundrechte; Ungültigkeit der Safe-Harbor-Entscheidung; Befugnisse der unabhängigen Aufsichtsbehörden]

C-230/14, *Weltimmo s.r.o. / Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. Oktober 2015

[Befugnisse der nationalen Aufsichtsbehörden]

C-201/14 *Smaranda Bara und andere / Casa Națională de Asigurări de Sănătate und andere*, 1. Oktober 2015

[Recht auf Unterrichtung über die Verarbeitung personenbezogener Daten]

C-212/13, *František Ryneš / Úřad pro ochranu osobních údajů*, 11. Dezember 2014

[Begriffe „Datenverarbeitung“ und „Verantwortlicher“]

C-473/12, *Institut professionnel des agents immobiliers (IPI) / Geoffrey Englebert und andere*, 7. November 2013

[Recht auf Unterrichtung über die Verarbeitung personenbezogener Daten]

T-462/12 R, *Pilkington Group Ltd / Europäische Kommission*, Beschluss des Präsidenten des Gerichts, 11. März 2013

C-342/12, *Worten – Equipamentos para o Lar SA / Autoridade para as Condições de Trabalho (ACT)*, 30. Mai 2013

[Begriff „personenbezogene Daten“; Aufzeichnungen über die Arbeitszeiten; Grundsätze in Bezug auf die Qualität der Daten und die Zulässigkeit der Verarbeitung von Daten; Zugang der für die Überwachung der Arbeitsbedingungen zuständigen nationalen Behörde; Verpflichtung des Arbeitgebers, die Aufzeichnungen über die Arbeitszeiten so zur Verfügung zu stellen, dass sie unverzüglich eingesehen werden können]

Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere* [GK], 8. April 2014

[Verletzung des Primärrechts der EU durch die Richtlinie über die Vorratsspeicherung von Daten; rechtmäßige Verarbeitung; Zweckbindung und Speicherbegrenzung]

C-288/12, *Europäische Kommission / Ungarn* [GK], 8. April 2014

[Rechtmäßigkeit der Amtsenthebung des nationalen Datenschutzbeauftragten]

Verbundene Rechtssachen C-141/12 und C-372/12, *YS / Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel / M und S*, 17. Juli 2014

[Umfang des Auskunftsrechts der betroffenen Person; Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten; Begriff der „personenbezogenen

Daten“; Daten in Bezug auf den Antragsteller einer Aufenthaltserlaubnis und rechtliche Bewertung in einem Verwaltungsdokument, das die Entscheidung vorbereitet; Charta der Grundrechte der Europäischen Union]

C-131/12, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GK], 13. Mai 2014

[Verpflichtung von Suchmaschinenbetreibern, auf Antrag der betroffenen Person von der Anzeige personenbezogener Daten in den Suchergebnissen abzusehen; Anwendbarkeit der Datenschutzrichtlinie; Begriff der „Datenverarbeitung“; Bedeutung des Begriffs „Verantwortliche“; Abwägung des Datenschutzes und der Meinungsfreiheit; das Recht auf Vergessenwerden]

C-614/10, *Europäische Kommission / Republik Österreich* [GK], 16. Oktober 2012
Unabhängigkeit einer nationalen Aufsichtsbehörde]

Verbundene Rechtssachen C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24. November 2011

[Richtige Umsetzung von Artikel 7 Buchstabe f der Datenschutzrichtlinie - „berechtigzte Interessen anderer“ - in nationales Recht]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) / Netlog NV*, 16. Februar 2012

[Verpflichtung von Betreibern sozialer Netzwerke zur Verhinderung der unrechtmäßigen Nutzung von musikalischen und audiovisuellen Werken seitens Nutzern der Netzwerke]

C-70/10, *Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. November 2011

[Informationsgesellschaft; Urheberrecht; Internet; „Peer-to-Peer“-Programme; Anbieter von Internetzugangsdiensten; Einrichtung eines Systems zum Filtern elektronischer Kommunikationen, um urheberrechtsverletzenden Austausch von Dateien zu verhindern; keine allgemeine Verpflichtung, die übermittelten Informationen zu überwachen]

C-543/09, *Deutsche Telekom AG / Bundesrepublik Deutschland*, 5. Mai 2011
[Erfordernis der erneuten Einwilligung]

Verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen* [GK], 9. November 2010

[Begriff der „personenbezogenen Daten“; Verhältnismäßigkeit der rechtlichen Verpflichtung zur Veröffentlichung personenbezogener Daten über die Empfänger bestimmter EU-Landwirtschaftsfonds]

C-553/07, *College van burgemeester en wethouders van Rotterdam / M. E. E. Rijkeboer*, 7. Mai 2009

[Auskunftsrecht der betroffenen Person]

C-518/07, *Europäische Kommission / Bundesrepublik Deutschland* [GK], 9. März 2010

[Unabhängigkeit einer nationalen Aufsichtsbehörde]

C-73/07 *Tietosuoja-valtuutus / Satakunnan Markkinapörssi Oy und Satamedia Oy* [GK], 16. Dezember 2008.

[Begriff der „journalistischen Tätigkeiten“ im Sinne von Artikel 9 der Datenschutzrichtlinie]

C-524/06, *Heinz Huber / Bundesrepublik Deutschland* [GK], 16. Dezember 2008

[Rechtmäßigkeit der Speicherung von Daten über Ausländer in einem statistischen Register]

C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU* [GK], 29. Januar 2008

[Begriff der „personenbezogenen Daten“; Verpflichtung von Internetzugangsanbietern zur Offenlegung der Identität von Nutzern des Programms KaZaA zum Austausch von Dateien gegenüber einem Verband zum Schutz des geistigen Eigentums]

C-101/01, *Strafverfahren gegen Bodil Lindqvist*, 6. November 2003

[Besondere Kategorien personenbezogener Daten]

Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Rechnungshof / Österreichischer Rundfunk und andere und Christa Neukomm und Joseph Lauermann / Österreichischer Rundfunk*, 20. Mai 2003

[Verhältnismäßigkeit der Rechtspflicht, personenbezogener Daten über die Bezüge von Arbeitnehmern bestimmter Kategorien von Einrichtungen des öffentlichen Sektors, zu veröffentlichen]

C-434/16, *Peter Nowak / Data Protection Commissioner*, Schlussanträge der Generalanwältin Juliane Kokott, 20. Juli 2017

[Begriff der „personenbezogenen Daten“; Zugang zu der eigenen Prüfungsarbeit; Korrekturanmerkungen]

C-291/12, *Michael Schwarz / Stadt Bochum*, 17. Oktober 2013

[Vorabentscheidungsersuchen; Raum der Freiheit, der Sicherheit und des Rechts; biometrischer Reisepass; digitale Fingerabdrücke; Rechtsgrundlage; Verhältnismäßigkeit]

Rechtsprechung zur Richtlinie (EU) 2016/681

Gutachten 1/15 des Gerichtshofs [GK], 26. Juli 2017

[Rechtsgrundlage; geplantes Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen; Vereinbarkeit des geplanten Abkommens mit Artikel 16 AEUV und Artikel 7 und 8 und Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union]

Rechtsprechung zur Datenschutzverordnung für EU-Organe

C-615/13P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) / Europäische Behörde für Lebensmittelsicherheit (EFSA), Europäische Kommission*, 16. Juli 2015

[Zugang zu Dokumenten]

C-28/08 P, *Europäische Kommission / The Bavarian Lager Co. Ltd.* [GK], 29. Juni 2010

[Zugang zu Dokumenten]

Rechtsprechung zur Richtlinie 2002/58/EG

C-536/15, *Tele2 (Netherlands) BV und andere / Autoriteit Consument en Markt (AMC)*, 15. März 2017

[Diskriminierungsverbot; Zurverfügungstellung personenbezogener Teilnehmerdaten zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen; Einwilligung des Teilnehmers; Unterscheidung

nach dem Mitgliedstaat, in dem die öffentlich zugänglichen Auskunftsdienste und Teilnehmerverzeichnisse bereitgestellt werden]

Verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB / Post-och telestyrelsen* und *Secretary of State for the Home Department / Tom Watson und andere* [GK], 21. Dezember 2016

[Vertraulichkeit der elektronischen Kommunikation; Betreiber elektronischer Kommunikationsdienste; Pflicht zur allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten; keine vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde; Charta der Grundrechte der Europäischen Union; Vereinbarkeit mit dem Unionsrecht]

C-70/10, *Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. November 2011

[Informationsgesellschaft; Urheberrecht; Internet; „Peer-to-Peer“-Programme; Anbieter von Internetzugangsdiensten; Einrichtung eines Systems der Filterung elektronischer Kommunikationen zur Verhinderung des urheberrechtsverletzenden Austauschs von Dateien; keine allgemeine Verpflichtung, die übermittelten Informationen zu überwachen]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB / Perfect Communication Sweden AB*, 19. April 2012

[Urheberrecht und verwandte Schutzrechte; Datenverarbeitung über das Internet; Beeinträchtigung eines ausschließlichen Rechts; Hörbücher, die mittels eines FTP-Servers über das Internet durch eine vom Internetdienstleister zur Verfügung gestellte IP-Adresse zugänglich gemacht werden; Anordnung an den Internetdienstleister, den Namen und die Adresse des Nutzers der IP-Adresse herauszugeben]

Index

Rechtsprechung des Gerichtshofs der Europäischen Union

- Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*,
Verbundene Rechtssachen C-468/10 und C-469/10,
24. November 2011 35, 63, 166, 169, 187, 188
- Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) / Netlog NV*, C-360/10, 16. Februar 2012 91
- Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB / Perfect Communication Sweden AB*, C-461/10, 19. April 2012 91
- Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni*, C-398/15,
9. März 2017 19, 94, 98, 118, 242, 243, 268, 274
- ClientEarth, Pesticide Action Network Europe (PAN Europe) / Europäische Behörde für Lebensmittelsicherheit (EFSA), Europäische Kommission*, C-615/13 P, 16. Juli 2015 19, 79, 258
- College van burgemeester en wethouders van Rotterdam / M. E. E. Rijkeboer*, C-553/07, 7. Mai 2009 138, 152, 242, 260
- Deutsche Telekom AG / Bundesrepublik Deutschland*, C-543/09,
5. Mai 2011 99, 165, 176

<i>Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources und andere und Kärntner Landesregierung und andere</i> [GK], Verbundene Rechtssachen C-293/12 und C-594/12, 8. April 2014	24, 53, 55, 73, 137, 138, 150, 155, 288, 290, 324, 352, 353, 412
<i>Europäische Kommission / Bundesrepublik Deutschland</i> [GK], C-518/07, 9. März 2010	223, 228
<i>Europäische Kommission / Republik Österreich</i> [GK], C-614/10, 16. Oktober 2012	223, 229
<i>Europäische Kommission / Ungarn</i> [GK], C-288/12, 8. April 2014	223, 230
<i>Europäische Kommission / The Bavarian Lager Co. Ltd.</i> [GK], C-28/08 P, 29. Juni 2010	19, 77, 244, 287
<i>František Ryneš / Úřad pro ochranu osobních údajů</i> , C-212/13, 11. Dezember 2014	98, 111, 117, 125
<i>Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [GK], C-131/12, 13. Mai 2014	19, 66, 93, 98, 119, 126, 242, 266, 267, 273
<i>Gutachten 1/15 des Gerichtshofs</i> (GK), 26. Juli 2017	51, 318
<i>Heinz Huber / Bundesrepublik Deutschland</i> [GK], C-524/06, 16. Dezember 2008	165, 169, 182, 183, 386, 404
<i>Institut professionnel des agents immobiliers (IPI) / Geoffrey Englebert und andere</i> , C-473/12, 7. November 2013	241, 247
<i>International Transport Workers' Federation, Finnish Seamen's Union / Viking Line ABP, OÜ Viking Line Eesti</i> [GK], C-438/05, 11. Dezember 2007	290
<i>Maximillian Schrems / Data Protection Commissioner</i> [GK], C-362/14, 6. Oktober 2015	52, 223, 226, 232, 244, 284, 288, 297, 303, 304, 305, 310, 312
<i>Michael Schwarz / Stadt Bochum</i> , C-291/12, 17. Oktober 2013	58, 60
<i>Pasquale Foglia / Mariella Novello</i> (Nr. 2), C-244/80, 16. Dezember 1981	290
<i>Patrick Breyer / Bundesrepublik Deutschland</i> , C-582/14, 19. Oktober 2016	97, 109, 110

<i>Peter Nowak / Data Protection Commissioner, C-434/16,</i> Schlussanträge der Generalanwältin Juliane Kokott, 20. Juli 2017	98, 242
<i>Pilkington Group Ltd / Europäische Kommission, T-462/12 R,</i> Beschluss des Präsidenten des Gerichts, 11. März 2013	82
<i>Productores de Música de España (Promusicae) / Telefónica de España SAU [GK], C-275/06, 29. Januar 2008.....</i>	19, 63, 89, 92, 97, 107
<i>Rechnungshof / Österreichischer Rundfunk und andere und Christa Neukomm und Joseph Lauer mann / Österreichischer Rundfunk, Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, 20. Mai 2003.....</i>	76, 169
<i>Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, 24. November 2011</i>	51, 97, 107
<i>Smaranda Bara und andere / Casa Națională de Asigurări de Sănătate und andere, C-201/14,</i> 1. Oktober 2015	108, 137, 145, 241, 248, 409
<i>Strafverfahren gegen Bodil Lindqvist, C-101/01, 6. November 2003</i>	97, 98, 116, 119, 124, 125, 203
<i>Strafverfahren gegen Giuseppe Francesco Gasparini und andere, C-467/04, 28. September 2006</i>	290
<i>Tele2 (Netherlands) BV und andere / Autoriteit Consument en Markt (AMC), C-536/15, 15. März 2017</i>	99, 165, 176, 177
<i>Tele2 Sverige AB / Post- och telestyrelsen und Secretary of State for the Home Department / Tom Watson und andere [GK], Verbundene Rechtssachen C-203/15 und C-698/15,</i> 21. Dezember 2016	51, 56, 73, 324, 353
<i>Tietosuoja valtuutettu / Satakunnan Markkinapörssi Oy und Satamedia Oy [GK], C-73/07, 16. Dezember 2008.....</i>	19, 64
<i>Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen [GK], Verbundene Rechtssachen C-92/09 und C-93/09, 9. November 2010</i>	18, 22, 43, 55, 75, 97, 102, 104
<i>Weltimmo s.r.o. / Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1. Oktober 2015.....</i>	233

*Worten – Equipamentos para o Lar SA / Autoridade para as
Condições de Trabalho (ACT), C-342/12, 30. Mai 2013.....392*

*YS / Minister voor Immigratie, Integratie en Asiel und Minister
voor Immigratie, Integratie en Asiel / M und S, Verbundene
Rechtssachen C-141/12 und C-372/12, 17. Juli 2014.....97, 104, 242, 258*

Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte

Allan / Vereinigtes Königreich, Nr. 48539/99, 5. November 2002323, 329

Amann / Schweiz [GK], Nr. 27798/95, 16. Februar 2000 44, 45, 97, 104, 106

*Association for European Integration and Human Rights und
Ekimdzhiev / Bulgarien, Nr. 62540/00, 28. Juni 2007 45*

*Avilkina und andere / Russland, Nr. 1585/09, 6. Juni 2013 (nicht
rechtskräftig)398*

Axel Springer AG / Deutschland [GK], Nr. 39954/08, 7. Februar 2012 19, 68

Aycaguer / Frankreich, Nr. 8806/12, 22. Juni 2017 327

B.B. / Frankreich, Nr. 5335/06, 17. Dezember 2009 323, 324, 327

Bărbulescu / Rumänien [GK], Nr. 61496/08, 5. September 2017 105, 394

*Bernh Larsen Holding AS und andere / Norwegen, Nr. 24117/08,
14. März 2013.....97, 101*

Biriuk / Litauen, Nr. 23373/03, 25. November 200871, 244, 397, 398

Bohlen / Deutschland, Nr. 53495/09, 19. Februar 2015 19, 71

*Brito Ferrinho Bexiga Villa-Nova / Portugal, Nr. 69436/10,
1. Dezember 2015..... 83*

Brunet / Frankreich, Nr. 21010/10, 18. September 2014 264

Cemalettin Canli / Türkei, Nr. 22427/04, 18. November 2008 242, 262

Ciubotaru / Republik Moldau, Nr. 27138/04, 27. April 2010 242, 261

Copland / Vereinigtes Königreich, Nr. 62617/00, 3. April 200727, 385, 393

*Coudec und Hachette Filipacchi Associés / Frankreich [GK],
Nr. 40454/07, 10. November 2015 69*

D.L. / Bulgarien, Nr. 7472/14, 19. Mai 2016..... 326

Dalea / Frankreich, Nr. 964/07, 2. Februar 2010 262, 324, 370

Dragojević / Kroatien, Nr. 68955/11, 15. Januar 2015 327

<i>Elberte / Lettland</i> , Nr. 61243/08, 13. April 2015.....	99
<i>G.S.B. / Schweiz</i> , Nr. 28601/11, 22. Dezember 2015.....	407, 408
<i>Gaskin / Vereinigtes Königreich</i> , Nr. 10454/83, 7. Juli 1989	258
<i>Godelli / Italien</i> , Nr. 33783/09, 25. September 2012.....	258
<i>Halford / Vereinigtes Königreich</i> , Nr. 20605/92, 25. Juni 1997	407
<i>Haralambie / Rumänien</i> , Nr. 21737/03, 27. Oktober 2009.....	137, 143
<i>I / Finnland</i> , Nr. 20511/03, 17. Juli 2008	28, 166, 200, 397
<i>Iordachi und andere / Republik Moldau</i> , Nr. 25198/02, 10. Februar 2009.....	44
<i>K.H. und andere / Slowakei</i> , Nr. 32881/04, 28. April 2009.....	137, 141, 258, 397
<i>K.U. / Finnland</i> , Nr. 2872/02, 2. Dezember 2008	28, 244, 291
<i>Karabeyoğlu / Türkei</i> , Nr. 30083/10, 7. Juni 2016.....	284, 332
<i>Khelili / Schweiz</i> , Nr. 16188/07, 18. Oktober 2011.....	48
<i>Klass und andere / Deutschland</i> , Nr. 5029/71, 6. September 1978.....	27, 28, 323, 325
<i>Köpke / Deutschland</i> , Nr. 420/07, 5. Oktober 2010.....	111, 291
<i>Kopp / Schweiz</i> , Nr. 23224/94, 25. März 1998.....	44
<i>L.H. / Lettland</i> , Nr. 52019/07, 29. April 2014.....	398
<i>L.L. / Frankreich</i> , Nr. 7508/02, 10. Oktober 2006.....	397
<i>Leander / Schweden</i> , Nr. 9248/81, 26. März 1987.....	47, 50, 242, 258, 273, 327
<i>Liberty und andere / Vereinigtes Königreich</i> , Nr. 58243/00, 1. Juli 2008.....	101
<i>M.K. / Frankreich</i> , Nr. 19522/09, 18. April 2013.....	263, 327
<i>M.M. / Vereinigtes Königreich</i> , Nr. 24029/07, 13. November 2012.....	154, 327
<i>M.N. und andere / San Marino</i> , Nr. 28005/12, 7. Juli 2015	108, 407
<i>M.S. / Schweden</i> , Nr. 20837/92, 27. August 1997	273, 397
<i>Magyar Helsinki Bizottság / Ungarn [GK]</i> , Nr. 18030/11, 8. November 2016.....	19, 80
<i>Malone / Vereinigtes Königreich</i> , Nr. 8691/79, 2. August 1984.....	27, 45, 323
<i>Michaud / Frankreich</i> , Nr. 12323/11, 6. Dezember 2012	386, 407
<i>Mosley / Vereinigtes Königreich</i> , Nr. 48009/08, 10. Mai 2011	19, 70, 273
<i>Müller und andere / Schweiz</i> , Nr. 10737/84, 24. Mai 1988	88
<i>Mustafa Sezgin Tanrikulu / Türkei</i> , Nr. 27473/06, 18. Juli 2017	27, 284

<i>Niemietz / Deutschland</i> , Nr. 13710/88, 16. Dezember 1992.....	104, 407
<i>Odièvre / Frankreich</i> [GK], Nr. 42326/98, 13. Februar 2003	258
<i>P.G. und J.H. / Vereinigtes Königreich</i> , Nr. 44787/98, 25. September 2001	111
<i>Peck / Vereinigtes Königreich</i> , Nr. 44647/98, 28. Januar 2003.....	47, 111
<i>Pruteanu / Rumänien</i> , Nr. 30181/05, 3. Februar 2015.....	19, 82
<i>Roman Zakharov / Russland</i> [GK], Nr. 47143/06, 4. Dezember 2015	28, 329
<i>Rotaru / Rumänien</i> [GK], Nr. 28341/95, 4. Mai 2000	27, 45, 104, 262, 325
<i>S. und Marper / Vereinigtes Königreich</i> [GK], Nrn. 30562/04 und 30566/04, 4. Dezember 2008.....	18, 44, 48, 138, 154, 323, 324, 328
<i>Satakunnan Markkinapörssi Oy und Satamedia Oy / Finnland</i> [GK], Nr. 931/13, 27. Juni 2017.....	21, 65
<i>Sciacca / Italien</i> , Nr. 50774/99, 11. Januar 2005	111
<i>Segerstedt-Wiberg und andere / Schweden</i> , Nr. 62332/00, 6. Juni 2006.....	242, 263
<i>Shimovolos / Russland</i> , Nr. 30194/09, 21. Juni 2011.....	45
<i>Silver und andere / Vereinigtes Königreich</i> , Nrn. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. März 1983.....	45
<i>Sinan Işık / Türkei</i> , Nr. 21924/05, 2. Februar 2010.....	86
<i>Szabó und Vissy / Ungarn</i> , Nr. 37138/14, 12. Januar 2016.....	27, 28, 323, 325, 329
<i>Szuluk / Vereinigtes Königreich</i> , Nr. 36936/05, 2. Juni 2009	397
<i>Taylor-Sabori / Vereinigtes Königreich</i> , Nr. 47114/99, 22. Oktober 2002	45
<i>The Sunday Times / Vereinigtes Königreich</i> , Nr. 6538/74, 26. April 1979.....	45
<i>Uzun / Deutschland</i> , Nr. 35623/05, 2. September 2010	28, 97
<i>Vereinigung bildender Künstler / Österreich</i> , Nr. 68345/01, 25. Januar 2007	19, 88
<i>Versini-Campinchi und Crasnianski / Frankreich</i> , Nr. 49176/11, 16. Juni 2016	331
<i>Vetter / Frankreich</i> , Nr. 59842/00, 31. Mai 2005	45, 323
<i>Von Hannover / Deutschland</i> , Nr. 59320/00, 24. Juni 2004.....	111
<i>Von Hannover / Deutschland (Nr. 2)</i> [GK], Nrn. 40660/08 und 60641/08, 7. Februar 2012	63

<i>Vukota-Bojić / Schweiz</i> , Nr. 61838/10, 18. Oktober 2016.....	46
<i>Wisse / Frankreich</i> , Nr. 71611/01, 20. Dezember 2005	111
<i>Y / Türkei</i> , Nr. 648/10, 17. Februar 2015.....	166, 189
<i>Z / Finnland</i> , Nr. 22009/93, 25. Februar 1997.....	29, 385, 397

Rechtsprechung nationaler Gerichte

Deutschland, <i>Bundesverfassungsgericht</i> , 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (<i>Volkszählungsurteil</i>), 15. Dezember 1983	21
Deutschland, (<i>Bundesverfassungsgericht</i>), 1 BvR 256/08, 2. März 2010	351
Rumänien, Verfassungsgerichtshof (<i>Curtea Constituțională a României</i>), Nr. 1258, 8. Oktober 2009	351
Tschechische Republik, Verfassungsgerichtshof (<i>Ústavní soud České republiky</i>), 94/2011 Coll., 22. März 2011.....	351

Anmerkung zur Zitierweise

Die Verweise auf die Rechtsprechung beinhalten umfassende Informationen, anhand derer die vollständigen Urteile bzw. Entscheidungen zu den betreffenden Fällen recherchiert werden können. Dies kann sinnvoll sein, wenn sich der Leser eingehender mit den Argumenten und Analysen auseinandersetzen möchte, aufgrund derer die Gerichte zu ihren Entscheidungen gelangt sind.

Viele der in dieser Veröffentlichung angeführten Rechtssachen wurden durch den EGMR oder den EuGH entschieden. Daher wird im Folgenden die Suche nach den Entscheidungen dieser beiden Gerichtshöfe dargestellt. Ähnlich kann jedoch auch vorgegangen werden, wenn nationale Datenbanken zur Rechtsprechung herangezogen werden.

Für die Suche nach der Rechtsprechung des EGMR empfiehlt sich das [Portal HUDOC des EGMR](#), über das dessen Rechtsprechung frei zugänglich ist: Das Portal HUDOC stellt eine benutzerfreundliche Suchmaske bereit, mit der die gewünschte Entscheidung oder das gewünschte Urteil ganz einfach gefunden werden können. Der einfachste Weg ist dabei die Eingabe der Beschwerdennummer in das Suchfeld „Application Number“.

Für die Suche nach der Rechtsprechung des EuGH empfiehlt sich die Suchmaschine [CURIA](#), über das dessen Rechtsprechung frei zugänglich ist. Die Suchmaschine CURIA stellt eine benutzerfreundliche Suchmaske bereit, mit der die gewünschte Entscheidung oder das gewünschte Urteil ganz einfach gefunden werden können. Der einfachste Weg ist dabei die Eingabe der Nummer der Rechtssache in das Suchfeld „Nr. der Rechtssache“.

In beiden Fällen (sowie in anderen Suchmaschinen/Datenbanken) hat der Nutzer auch die Möglichkeit, die Rechtsprechung nach dem Datum zu durchsuchen. Um eine solche datumsbezogene Suche nach der Rechtsprechung zu erleichtern, wurden alle in diesem Handbuch aufgeführten Urteile und Entscheidungen mit ihrem Datum versehen.

Zahlreiche Informationen über die Agentur der Europäischen Union für Grundrechte finden Sie im Internet auf der FRA-Website unter fra.europa.eu.

Weitere Informationen über die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte sind auf der Webseite des Gerichtshofs unter: echr.coe.int. verfügbar. Die elektronische Datenbank HUDOC ermöglicht den Zugang zu Entscheidungen und Urteilen in den offiziellen Sprachen des Gerichtshofs Englisch und/oder Französisch sowie zu Übersetzungen in weitere Sprachen, Zusammenfassungen von Rechtssachen, Pressemitteilungen und weiteren Informationen über die Tätigkeit des Gerichtshofs: <http://HUDOC.echr.coe.int>.

So erhalten Sie Publikationen des Europarates

Der Europarat veröffentlicht zu allen Referenzbereichen der Organisation, einschließlich der Menschenrechte, der Rechtswissenschaften, der Bereiche Gesundheit, Ethik, Soziales, Umwelt, Bildung, Kultur, Sport, Jugend und architektonisches Kulturerbe. Bücher und elektronische Publikationen aus dem umfangreichen Katalog können online über folgende Webseite bestellt werden: <http://book.coe.int/>.

Ein virtueller Lesesaal ermöglicht es Benutzern, kostenlos Textauszüge aus kürzlich erschienenen Hauptwerken einzusehen oder auch eine Auswahl von vollständigen offiziellen Dokumenten.

Informationen über die Übereinkommen des Europarates sowie deren Volltext erhalten Sie über die offizielle Webseite des Vertragsbüros: <http://conventions.coe.int/>.

So treten Sie in Kontakt mit der EU

Persönlich

In der gesamten Europäischen Union finden sich zahlreiche Europe-Direct-Informationszentren. Die Adresse des nächstgelegenen Zentrums finden Sie unter: https://europa.eu/european-union/contact_en

Telefonisch oder per E-Mail

Europe Direct soll Ihnen helfen, Antworten auf Ihre Fragen zur Europäischen Union zu finden. Kontaktieren Sie dieses Service:

- unter der gebührenfreien Rufnummer: 00 800 6 7 8 9 10 11 (manche Anbieter verrechnen möglicherweise Gebühren für diesen Anruf),
- unter der folgenden Standardnummer: +32 22999696 oder
- per E-Mail unter: https://europa.eu/european-union/contact_de

So finden Sie Informationen über die EU

Online

Informationen zur Europäischen Union in allen offiziellen Sprachen der EU finden Sie auf der Europa-Website unter: https://europa.eu/european-union/index_de

EU-Veröffentlichungen

Sie können kostenlose oder kostenpflichtige EU-Veröffentlichungen herunterladen oder bestellen, unter: <https://publications.europa.eu/de/publications>. Mehrere Ausgaben kostenloser Veröffentlichungen erhalten Sie über Europe Direct oder über Ihr lokales Informationszentrum (siehe: https://europa.eu/european-union/contact_de).

EU-Recht und damit in Zusammenhang stehende Dokumente

Rechtliche Informationen der EU, darunter sämtliche EU-Rechtsvorschriften seit 1952 in allen offiziellen Sprachversionen, finden Sie in EUR-Lex unter: <http://eur-lex.europa.eu>

Offene Daten der EU

Das Offene Datenportal der EU (<http://data.europa.eu/euodp/de>) bietet Zugang zu Daten der EU, die kostenfrei bereitgestellt werden und für kommerzielle und nichtkommerzielle Zwecke heruntergeladen und weiterverwendet werden dürfen.

Die rasante Entwicklung der Informationstechnologie hat den Bedarf nach einem stabilen Schutz personenbezogener Daten verschärft, das Recht darauf wird sowohl durch Instrumente der Europäischen Union (EU) als auch des Europarates geschützt. Der Schutz dieses wichtigen Rechts steht vor neuen und großen Herausforderungen, da technologische Fortschritte die Möglichkeiten beispielsweise bei der Überwachung, beim Abfangen von Kommunikation und bei der Datenspeicherung erweitern. Dieses Handbuch bietet für Angehörige der Rechtsberufe, die sich im Bereich des Datenschutzes nicht so gut auskennen, eine Einführung in diesen aufstrebenden Rechtsbereich. Es gibt einen Überblick über die geltenden Regelwerke von EU und Europarat. Es erläutert auch die wichtigsten Rechtsfälle und fasst die wesentlichen Aspekte in den Urteilen sowohl des Gerichtshofs der Europäischen Union als auch des Europäischen Gerichtshofs für Menschenrechte zusammen. Darüber hinaus bietet das Handbuch in Form hypothetischer Szenarien praxisnahe Beispiele der verschiedenen Themen, auf die man in diesem sich ständig weiterentwickelnden Bereich trifft.

AGENTUR DER EUROPÄISCHEN UNION FÜR GRUNDRECHTE

Schwarzenbergplatz 11 – 1040 Wien – Österreich

Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-699

fra.europa.eu – info@fra.europa.eu – [@EURightsAgency](https://twitter.com/EURightsAgency)

EUROPÄISCHER GERICHTSHOF FÜR MENSCHENRECHTE EUROPARAT

67075 Straßburg Cedex – Frankreich

Tel. +33 (0) 3 88 41 20 18 - Fax +33 (0) 3 88 41 27 30

echr.coe.int – publishing@echr.coe.int – [@ECHRPublication](https://twitter.com/ECHRPublication)

EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

Rue Wiertz 60 – 1047 Brüssel – Belgien

Tel. +32 2 283 19 00

www.edps.europa.eu – edps@edps.europa.eu – [@EU_EDPS](https://twitter.com/EU_EDPS)



Amt für Veröffentlichungen
der Europäischen Union

ISBN 978-92-871-9848-8 (Europarat)
ISBN 978-92-9491-904-5 (FRA)