

Gesetzessammlung – Internetrecht und IT-Datenschutzrecht *Stand: 17. April 2024*

Inhalt – Auszüge aus folgenden Gesetzen:

Gesetzessammlung - Teil I: Internetrecht.....	6
Digital Services Act - VO EU 2022/2065	6
Artikel 1 Gegenstand	6
Artikel 3 Begriffsbestimmungen	7
Artikel 4 „Reine Durchleitung“	9
Artikel 5 „Caching“	10
Artikel 6 Hosting	10
Artikel 7 Freiwillige Untersuchungen auf Eigeninitiative und Einhaltung der Rechtsvorschriften	10
Artikel 8 Keine allgemeine Verpflichtung zur Überwachung oder aktiven Nachforschung	11
Artikel 9 Anordnungen zum Vorgehen gegen rechtswidrige Inhalte.....	11
Artikel 10 Auskunftsanordnungen.....	12
Artikel 11 Kontaktstellen für die Behörden der Mitgliedstaaten, die Kommission und den Vorstand.....	13
Artikel 12 Kontaktstellen für Nutzer der Dienste	13
Artikel 13 Gesetzlicher Vertreter.....	13
Artikel 14 Allgemeine Geschäftsbedingungen	14
Artikel 15 Transparenzberichtspflichten der Anbieter von Vermittlungsdiensten	14
Artikel 16 Melde- und Abhilfeverfahren.....	15
Artikel 17 Begründung	16
Artikel 18 Meldung des Verdachts auf Straftaten	17
Artikel 19 Ausnahme für Kleinst- und Kleinunternehmen.....	17
Artikel 20 Internes Beschwerdemanagementsystem.....	17
Artikel 21 Außergerichtliche Streitbeilegung	18
Artikel 22 Vertrauenswürdige Hinweisgeber.....	20
Artikel 23 Maßnahmen und Schutz vor missbräuchlicher Verwendung	21
Artikel 24 Transparenzberichtspflichten der Anbieter von Online-Plattformen.....	22
Artikel 25 Gestaltung und Organisation der Online-Schnittstelle.....	23
Artikel 26 Werbung auf Online-Plattformen	23
Artikel 27 Transparenz der Empfehlungssysteme	24
Artikel 28 Online-Schutz Minderjähriger.....	24
Artikel 29 Ausnahme für Kleinst- und Kleinunternehmen.....	24
Artikel 30 Nachverfolgbarkeit von Unternehmern	24
Artikel 31 Konformität durch Technikgestaltung.....	26
Artikel 32 Recht auf Information	26
Artikel 33 Sehr große Online-Plattformen und sehr große Online-Suchmaschinen.....	27
Artikel 34 Risikobewertung	28
Artikel 35 Risikominderung	29

Artikel 36 Krisenreaktionsmechanismus	30
Artikel 37 Unabhängige Prüfung	31
Artikel 38 Empfehlungssysteme	33
Artikel 39 Zusätzliche Transparenz der Online-Werbung	33
Artikel 40 Datenzugang und Kontrolle.....	34
Artikel 41 Compliance-Abteilung.....	36
Artikel 42 Transparenzberichtspflichten.....	37
Artikel 43 Aufsichtsgebühren	38
Digital Markets Act – VO /EU 2022/1925	39
Artikel 1 Gegenstand und Anwendungsbereich	39
Artikel 2 Begriffsbestimmungen.....	40
Artikel 3 Benennung von Torwächtern.....	42
Artikel 4 Überprüfung des Torwächter-Status.....	44
Artikel 5 Verpflichtungen von Torwächtern.....	45
Artikel 6 Verpflichtungen von Torwächtern, die möglicherweise noch durch Artikel 8 näher ausgeführt werden	46
Artikel 7 Verpflichtung von Torwächtern zur Interoperabilität nummernunabhängiger interpersoneller Kommunikationsdienste.....	49
Artikel 8 Einhaltung der Verpflichtungen durch Torwächter	50
GG - Grundgesetz für die Bundesrepublik Deutschland.....	51
Art 1	51
Art 2	51
Art 5	51
Art 10	51
Art 13	52
Art 14	52
Art 87f	52
TKG – Telekommunikationsgesetz.....	53
§ 1 Zweck des Gesetzes, Anwendungsbereich	53
§ 2 Ziele und Grundsätze der Regulierung	53
§ 3 Begriffsbestimmungen	54
§ 80 Informationen über Breitbandausbau.....	55
§ 84 Gebiete mit Ausbaufizit.....	55
§ 156 Recht auf Versorgung mit Telekommunikationsdiensten	56
§ 157 Verfügbarkeit der Telekommunikationsdienste.....	56
§ 158 Erschwinglichkeit der Telekommunikationsdienste.....	57
§ 159 Beitrag von Unternehmen zur Versorgung mit Telekommunikationsdiensten.....	57
§ 160 Feststellung der Unterversorgung.....	57
§ 172 Daten für Auskunftersuchen der Sicherheitsbehörden	57
DDG Digitale Dienste Gesetz (in der Entwurfsfassung der Bundesregierung)	59
§ 1 Anwendungsbereich, Begriffsbestimmungen.....	59

§ 2 Europäisches Sitzland	61
§ 3 Herkunftslandprinzip	62
§ 4 Zulassungsfreiheit.....	64
§ 5 Allgemeine Informationspflichten	64
§ 6 Besondere Pflichten bei kommerziellen Kommunikationen	65
§ 7 Beschränkte Verantwortlichkeit bei Durchleitung von Informationen	65
§ 8 Anspruch auf Sperrung bei Rechtsverletzung	66
§ 9 Listen der Anbieter von audiovisuellen Mediendiensten und der Videosharingplattform-Anbieter	66
§ 10 Auskunftsverlangen der nach Landesrecht zuständigen Behörde.....	66
§ 11 Vertragliche Nutzungsverbote.....	67
§ 12 Zuständige Behörden nach Artikel 49 Absatz 1 der Verordnung (EU) 2022/2065	67
§ 13 Meldung des Verdachts auf Straftaten gemäß Artikel 18 der Verordnung (EU) 2022/2065 an das Bundeskriminalamt	68
§ 14 Errichtung und Ausstattung.....	68
§ 15 Unabhängigkeit	68
§ 16 Leitung der Koordinierungsstelle für digitale Dienste	68
§ 17 Tätigkeitsbericht	68
§ 18 Zusammenarbeit der Koordinierungsstelle für digitale Dienste mit den zuständigen Behörden, Verwaltungsvereinbarung	69
§ 19 Zusammenarbeit mit anderen Behörden, Einrichtung von Verbindungsschnittstellen, Verwaltungsvereinbarung	70
§ 20 Zentrale Beschwerdestelle	71
§ 21 Beirat	71
§ 24 Ermittlungen.....	72
§ 25 Auskunftserteilung und Durchsuchungen	73
§ 33 Bußgeldvorschriften	73
Medienstaatsvertrag (MStV)	77
§ 18 Informationspflichten und Auskunftsrechte.....	77
UrhG - Gesetz über Urheberrecht und verwandte Schutzrechte.....	77
§ 1 Allgemeines	77
§ 2 Geschützte Werke	77
§ 7 Urheber	78
§ 11 Allgemeines	78
§ 12 Veröffentlichungsrecht	78
§ 15 Allgemeines	78
§ 16 Vervielfältigungsrecht.....	78
§ 17 Verbreitungsrecht.....	79
§ 19a Recht der öffentlichen Zugänglichmachung	79
§ 21 Recht der Wiedergabe durch Bild- oder Tonträger.....	79
§ 23 Bearbeitungen und Umgestaltungen	79
§ 25 Zugang zu Werkstücken.....	79

§ 28 Vererbung des Urheberrechts	80
§ 29 Rechtsgeschäfte über das Urheberrecht	80
§ 30 Rechtsnachfolger des Urhebers.....	80
§ 31 Einräumung von Nutzungsrechten	80
§ 32 Angemessene Vergütung.....	80
§ 45 Rechtspflege und öffentliche Sicherheit.....	81
§ 49 Zeitungsartikel und Rundfunkkommentare.....	81
§ 50 Berichterstattung über Tagesereignisse	81
§ 51 Zitate	81
§ 53 Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch	81
§ 54 Vergütungspflicht	82
§ 54a Vergütungshöhe	83
§ 60a Unterricht und Lehre	83
§ 60b Unterrichts- und Lehrmedien.....	84
§ 60c Wissenschaftliche Forschung.....	84
§ 63 Quellenangabe	84
§ 64 Allgemeines	84
§ 69a Gegenstand des Schutzes	85
§ 69b Urheber in Arbeits- und Dienstverhältnissen.....	85
§ 72 Lichtbilder.....	85
§ 97 Anspruch auf Unterlassung und Schadensersatz	85
§ 97a Abmahnung	85
§ 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke.....	86
§ 108 Unerlaubte Eingriffe in verwandte Schutzrechte	86
§ 108a Gewerbsmäßige unerlaubte Verwertung	87
§ 109 Strafantrag.....	87
§ 110 Einziehung	87
StGB – Strafgesetzbuch	87
§ 1 Keine Strafe ohne Gesetz	87
§ 202a Ausspähen von Daten.....	87
§ 202b Abfangen von Daten.....	87
§ 202c Vorbereiten des Ausspähens und Abfangens von Daten.....	87
§ 263a Computerbetrug.....	88
§ 267 Urkundenfälschung	88
§ 269 Fälschung beweiserheblicher Daten.....	88
§ 303a Datenveränderung.....	88
§ 303b Computersabotage.....	89
§ 303c Strafantrag	89
§ 353b Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht	89
StPO - Strafprozeßordnung	90

§ 100a Telekommunikationsüberwachung.....	90
§ 100b Online-Durchsuchung.....	94
§ 100d Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte	96
§ 100e Verfahren bei Maßnahmen nach den §§ 100a bis 100c.....	97
§ 100f Akustische Überwachung außerhalb von Wohnraum.....	98
§ 100g Erhebung von Verkehrsdaten	98
§ 100h Weitere Maßnahmen außerhalb von Wohnraum.....	101
§ 100i Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten.....	101
§ 100j Bestandsdatenauskunft.....	101
§ 100k Erhebung von Nutzungsdaten bei Telemediendiensten.....	102
§ 101a Gerichtliche Entscheidung; Datenkennzeichnung und -auswertung; Benachrichtigungspflichten bei Verkehrs- und Nutzungsdaten.....	105
Gesetzessammlung – Teil II: Datenschutzrecht.....	106
DSGVO - VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).....	106
Erwägungsgrund (1).....	106
Erwägungsgrund (2).....	106
Erwägungsgrund (4).....	107
Erwägungsgrund (19).....	107
Erwägungsgrund (22).....	107
Erwägungsgrund (26).....	107
Erwägungsgrund (32).....	107
Erwägungsgrund (39).....	108
Erwägungsgrund (47).....	108
Erwägungsgrund (50).....	109
Artikel 1 Gegenstand und Ziele	109
Artikel 2 Sachlicher Anwendungsbereich.....	109
Artikel 3 Räumlicher Anwendungsbereich.....	109
Artikel 4 Begriffsbestimmungen.....	110
Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten.....	112
Artikel 6 Rechtmäßigkeit der Verarbeitung.....	113
Artikel 7 Bedingungen für die Einwilligung	114
Artikel 8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft.....	114
Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten.....	115
Artikel 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person	116
Artikel 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person	117
Artikel 15 Auskunftsrecht der betroffenen Person.....	118
Artikel 17 Recht auf Löschung („Recht auf Vergessenwerden“).....	118
Artikel 24 Verantwortung des für die Verarbeitung Verantwortlichen	119

Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	120
Artikel 26 Gemeinsam für die Verarbeitung Verantwortliche	120
Artikel 28 Auftragsverarbeiter	120
Artikel 30 Verzeichnis von Verarbeitungstätigkeiten	122
Artikel 31 Zusammenarbeit mit der Aufsichtsbehörde	123
Artikel 32 Sicherheit der Verarbeitung	123
Artikel 44 Allgemeine Grundsätze der Datenübermittlung	123
Artikel 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses	123
Artikel 46 Datenübermittlung vorbehaltlich geeigneter Garantien	125
Artikel 47 Verbindliche interne Datenschutzvorschriften	125
Artikel 49 Ausnahmen für bestimmte Fälle	127
Artikel 82 Haftung und Recht auf Schadenersatz	128
Artikel 83 Allgemeine Bedingungen für die Verhängung von Geldbußen	128
Artikel 99 Inkrafttreten und Anwendung	130
Bundesdatenschutzgesetz (BDSG)	130
§ 1 Anwendungsbereich des Gesetzes	130
§ 2 Begriffsbestimmungen	131
§ 3 Verarbeitung personenbezogener Daten durch öffentliche Stellen	132
Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)	132
§ 1 Zweck	132
§ 2 Sicherstellung des Datenschutzes	132
§ 3 Zulässigkeit der Verarbeitung personenbezogener Daten	132
§ 5 Anwendungsbereich	133

Gesetzessammlung - Teil I: Internetrecht

Digital Services Act - VO EU 2022/2065

Artikel 1 Gegenstand

(1) Ziel dieser Verordnung ist es, durch die Festlegung harmonisierter Vorschriften für ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld, in dem Innovationen gefördert und die in der Charta verankerten Grundrechte, darunter der Grundsatz des Verbraucherschutzes, wirksam geschützt werden, einen Beitrag zum reibungslosen Funktionieren des Binnenmarkts für Vermittlungsdienste zu leisten.

(2) In dieser Verordnung werden harmonisierte Vorschriften für die Erbringung von Vermittlungsdiensten im Binnenmarkt festgelegt. Insbesondere wird Folgendes festgelegt:

- a) ein Rahmen für die bedingte Haftungsbefreiung der Anbieter von Vermittlungsdiensten;
- b) Vorschriften über besondere Sorgfaltspflichten, die auf bestimmte Kategorien von Anbietern von Vermittlungsdiensten zugeschnitten sind;
- c) Vorschriften über die Durchführung und Durchsetzung dieser Verordnung, einschließlich der Zusammenarbeit und Koordinierung zwischen den zuständigen Behörden.

Artikel 2 Geltungsbereich

(1) Diese Verordnung gilt für Vermittlungsdienste, die für Nutzer mit Niederlassungsort oder Sitz in der Union angeboten werden, ungeachtet des Niederlassungsortes des Anbieters dieser Vermittlungsdienste.

(2) Diese Verordnung gilt weder für Dienstleistungen, die keine Vermittlungsdienste sind, noch für Anforderungen, die an eine solche Dienstleistung gestellt werden, ungeachtet dessen, ob die Dienstleistung durch Inanspruchnahme eines Vermittlungsdienstes erbracht wird.

(3) Diese Verordnung hat keine Auswirkungen auf die Anwendung der Richtlinie 2000/31/EG.

(4) Diese Verordnung lässt die Vorschriften anderer Rechtsakte der Union unberührt, die andere Aspekte der Erbringung von Vermittlungsdiensten im Binnenmarkt regeln oder diese Verordnung präzisieren und ergänzen, insbesondere folgende:

a) die Richtlinie 2010/13/EU,

b) die Unionsvorschriften auf dem Gebiet des Urheberrechts und der verwandten Schutzrechte,

c) die Verordnung (EU) 2021/784,

d) die Verordnung (EU) 2019/1148,

e) die Verordnung (EU) 2019/1150,

f) die Unionsvorschriften auf dem Gebiet des Verbraucherschutzes und der Produktsicherheit, einschließlich der Verordnungen (EU) 2017/2394 und (EU) 2019/1020 und der Richtlinien 2001/95/EG und 2013/11/EU,

g) die Unionsvorschriften zum Schutz personenbezogener Daten, insbesondere die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG,

h) die Unionsvorschriften im Bereich der justiziellen Zusammenarbeit in Zivilsachen, insbesondere die Verordnung (EU) Nr. 1215/2012 oder Rechtsakte der Union zur Festlegung der rechtlichen Regeln für vertragliche und außervertragliche Schuldverhältnisse anzuwendendes Recht,

i) die Unionsvorschriften im Bereich der justiziellen Zusammenarbeit in Strafsachen, insbesondere eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen,

j) eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren.

Artikel 3 Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

a) „Dienst der Informationsgesellschaft“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535;

b) „Nutzer“ jede natürliche oder juristische Person, die einen Vermittlungsdienst in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen;

c) „Verbraucher“ jede natürliche Person, die zu Zwecken handelt, die außerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit liegen;

d) „in der Union Dienstleistungen anbieten“ die Schaffung der Möglichkeit für natürliche oder juristische Personen in einem oder mehreren Mitgliedstaaten zur Nutzung der Dienste eines Anbieters von Vermittlungsdiensten, der eine wesentliche Verbindung zur Union hat;

e) „wesentliche Verbindung zur Union“ eine Verbindung eines Anbieters von Vermittlungsdiensten mit der Union entweder aufgrund seiner Niederlassung in der Union oder anhand besonderer faktischer Kriterien wie

- einer erheblichen Zahl von Nutzern in einem oder mehreren Mitgliedstaaten im Verhältnis zu dessen oder deren Bevölkerung; oder
- der Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten;
- f) „Unternehmer“ jede natürliche oder juristische Person, unabhängig davon, ob sie in privatem oder öffentlichem Eigentum steht, die für die Zwecke ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit entweder selbst oder durch eine andere in ihrem Namen oder Auftrag handelnde Person tätig wird;
- g) „Vermittlungsdienst“ eine der folgenden Dienstleistungen der Informationsgesellschaft:
 - i) eine „reine Durchleitung“, die darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln oder den Zugang zu einem Kommunikationsnetz zu vermitteln,
 - ii) eine „Caching“-Leistung, die darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln, wobei eine automatische, zeitlich begrenzte Zwischenspeicherung dieser Informationen zu dem alleinigen Zweck erfolgt, die Übermittlung der Information an andere Nutzer auf deren Anfrage effizienter zu gestalten,
 - iii) ein „Hosting“-Dienst, der darin besteht, von einem Nutzer bereitgestellte Informationen in dessen Auftrag zu speichern;
- h) „rechtswidrige Inhalte“ alle Informationen, die als solche oder durch ihre Bezugnahme auf eine Tätigkeit, einschließlich des Verkaufs von Produkten oder der Erbringung von Dienstleistungen, nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen, ungeachtet des genauen Gegenstands oder der Art der betreffenden Rechtsvorschriften;
- i) „Online-Plattform“ einen Hostingdienst, der im Auftrag eines Nutzers Informationen speichert und öffentlich verbreitet, sofern es sich bei dieser Tätigkeit nicht nur um eine unbedeutende und reine Nebenfunktion eines anderen Dienstes oder um eine unbedeutende Funktion des Hauptdienstes handelt, die aus objektiven und technischen Gründen nicht ohne diesen anderen Dienst genutzt werden kann, und sofern die Integration der Funktion der Nebenfunktion oder der unbedeutenden Funktion in den anderen Dienst nicht dazu dient, die Anwendbarkeit dieser Verordnung zu umgehen;
- j) „Online-Suchmaschine“ einen Vermittlungsdienst, der es Nutzern ermöglicht, in Form eines Stichworts, einer Spracheingabe, einer Wortgruppe oder einer anderen Eingabe Anfragen einzugeben, um prinzipiell auf allen Websites oder auf allen Websites in einer bestimmten Sprache eine Suche zu einem beliebigen Thema vorzunehmen und Ergebnisse in einem beliebigen Format, in dem Informationen im Zusammenhang mit dem angeforderten Inhalt zu finden sind, angezeigt zu bekommen;
- k) „öffentliche Verbreitung“ die Bereitstellung von Informationen für eine potenziell unbegrenzte Zahl von Dritten im Auftrag des Nutzers, der die Informationen bereitgestellt hat;
- l) „Fernabsatzvertrag“ einen Fernabsatzvertrag im Sinne des Artikels 2 Nummer 7 der Richtlinie 2011/83/EU;
- m) „Online-Schnittstelle“ eine Software, darunter auch Websites oder Teile davon sowie Anwendungen, einschließlich Mobil-Apps;
- n) „Koordinator für digitale Dienste am Niederlassungsort“ den Koordinator für digitale Dienste des Mitgliedstaats, in dem sich der Hauptsitz eines Anbieters eines Vermittlungsdienstes befindet oder in dem sein gesetzlicher Vertreter ansässig oder niedergelassen ist;
- o) „Koordinator für digitale Dienste am Bestimmungsort“ den Koordinator für digitale Dienste eines Mitgliedstaats, in dem der Vermittlungsdienst erbracht wird;
- p) „aktiver Nutzer einer Online-Plattform“ einen Nutzer des Dienstes, der eine Online-Plattform nutzt, indem er die Online-Plattform damit beauftragt, Informationen zur Verfügung zu stellen, oder der den Inhalten der Online-Plattform ausgesetzt ist, die diese zur Verfügung stellt und über ihre Online-Schnittstelle verbreitet;

- q) „aktiver Nutzer einer Online-Suchmaschine“ einen Nutzer des Dienstes, der eine Suchanfrage an eine Online-Suchmaschine stellt und dem auf ihrer Online-Schnittstelle dargestellten indexierten Informationen ausgesetzt ist;
- r) „Werbung“ Informationen, die dazu bestimmt sind, die Botschaft einer juristischen oder natürlichen Person zu verbreiten, unabhängig davon, ob damit gewerbliche oder nichtgewerbliche Zwecke verfolgt werden, und die von einer Online-Plattform auf ihrer Online-Schnittstelle gegen Entgelt speziell zur Bekanntmachung dieser Informationen dargestellt werden;
- s) „Empfehlungssystem“ ein vollständig oder teilweise automatisiertes System, das von einer Online-Plattform verwendet wird, um auf ihrer Online-Schnittstelle den Nutzern bestimmte Informationen vorzuschlagen oder diese Informationen zu priorisieren, auch infolge einer vom Nutzer veranlassten Suche, oder das auf andere Weise die relative Reihenfolge oder Hervorhebung der angezeigten Informationen bestimmt;
- t) „Moderation von Inhalten“ die – automatisierten oder nicht automatisierten – Tätigkeiten der Anbieter von Vermittlungsdiensten, mit denen insbesondere rechtswidrige Inhalte oder Informationen, die von Nutzern bereitgestellt werden und mit den allgemeinen Geschäftsbedingungen des Anbieters unvereinbar sind, erkannt, festgestellt und bekämpft werden sollen, darunter auch Maßnahmen in Bezug auf die Verfügbarkeit, Anzeige und Zugänglichkeit der rechtswidrigen Inhalte oder Informationen, z. B. Herabstufung, Demonetisierung, Sperrung des Zugangs oder Entfernung, oder in Bezug auf die Fähigkeit der Nutzer, solche Informationen bereitzustellen, z. B. Schließung oder Aussetzung des Kontos eines Nutzers;
- u) „allgemeine Geschäftsbedingungen“ alle Klauseln, ungeachtet ihrer Bezeichnung oder Form, die die vertraglichen Beziehungen zwischen dem Anbieter von Vermittlungsdiensten und den Nutzern regeln;
- v) „Menschen mit Behinderungen“ Menschen mit Behinderungen gemäß Artikel 3 Nummer 1 der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates [\(38\)](#);
- w) „kommerzielle Kommunikation“ kommerzielle Kommunikation im Sinne von Artikel 2 Buchstabe f der Richtlinie 2000/31/EG;
- x) „Umsatz“ die von einem Unternehmen im Sinne von Artikel 5 Absatz 1 der Verordnung (EG) Nr. 139/2004 des Rates [\(39\)](#) erzielten Umsätze.

KAPITEL II

HAFTUNG DER ANBIETER VON VERMITTLUNGSDIENSTEN

Artikel 4 „Reine Durchleitung“

(1) Bei der Durchführung eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln, haftet der Diensteanbieter nicht für die übermittelten oder abgerufenen Informationen, sofern er

- a) die Übermittlung nicht veranlasst,
- b) den Adressaten der übermittelten Informationen nicht auswählt und
- c) die übermittelten Informationen nicht auswählt oder verändert.

(2) Die Übermittlung von Informationen und die Vermittlung des Zugangs nach Absatz 1 umfassen auch die automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als es für die Übermittlung üblicherweise erforderlich ist.

(3) Dieser Artikel lässt die Möglichkeit unberührt, dass eine Justiz- oder Verwaltungsbehörde nach dem Rechtssystem eines Mitgliedstaats vom Diensteanbieter verlangt, eine Zuwiderhandlung abzustellen oder zu verhindern.

Artikel 5 „Caching“

(1) Bei der Durchführung eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln, haftet der Diensteanbieter nicht für die automatische, zeitlich begrenzte Zwischenspeicherung, die dem alleinigen Zweck dient, die Übermittlung der Information an andere Nutzer auf deren Anfrage effizienter oder sicherer zu gestalten, sofern seitens des Anbieters folgende Voraussetzungen erfüllt sind:

- a) er verändert die Informationen nicht,
- b) er beachtet die Bedingungen für den Zugang zu den Informationen,
- c) er beachtet die Regeln für die Aktualisierung der Informationen, die weithin in der Branche anerkannt und verwendet werden,
- d) er beeinträchtigt die zulässige Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die weithin in der Branche anerkannt und verwendet werden, nicht und
- e) er handelt zügig, um von ihm gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald er tatsächliche Kenntnis davon erhält, dass die Informationen am ursprünglichen Ausgangsort der Übermittlung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder eine Justiz- oder Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

(2) Dieser Artikel lässt die Möglichkeit unberührt, dass eine Justiz- oder Verwaltungsbehörde nach dem Rechtssystem eines Mitgliedstaats vom Diensteanbieter verlangt, eine Zuwiderhandlung abzustellen oder zu verhindern.

Artikel 6 Hosting

(1) Bei der Durchführung eines Dienstes der Informationsgesellschaft, der in der Speicherung der von einem Nutzer bereitgestellten Informationen besteht, haftet der Diensteanbieter nicht für die im Auftrag eines Nutzers gespeicherten Informationen, sofern er

- a) keine tatsächliche Kenntnis von einer rechtswidrigen Tätigkeit oder rechtswidrigen Inhalten hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder rechtswidrige Inhalte offensichtlich hervorgeht, oder
- b) sobald er diese Kenntnis oder dieses Bewusstsein erlangt, zügig tätig wird, um den Zugang zu den rechtswidrigen Inhalten zu sperren oder diese zu entfernen.

(2) Absatz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

(3) Absatz 1 findet keine Anwendung auf die Verbraucherschutzrechtliche Haftung von Online-Plattformen, die Verbrauchern das Abschließen von Fernabsatzverträgen mit Unternehmern ermöglichen, wenn die Online-Plattform die spezifischen Einzelinformationen dazu darstellt oder die betreffende Einzeltransaktion anderweitig in einer Weise ermöglicht, bei der ein durchschnittlicher Verbraucher davon ausgehen kann, dass die Information oder das Produkt oder die Dienstleistung, die bzw. das Gegenstand der Transaktion ist, entweder von der Online-Plattform selbst oder von einem ihrer Aufsicht unterstehenden Nutzer bereitgestellt wird.

(4) Dieser Artikel lässt die Möglichkeit unberührt, dass eine Justiz- oder Verwaltungsbehörde nach dem Rechtssystem eines Mitgliedstaats vom Diensteanbieter verlangt, eine Zuwiderhandlung abzustellen oder zu verhindern.

Artikel 7 Freiwillige Untersuchungen auf Eigeninitiative und Einhaltung der Rechtsvorschriften

Die Anbieter von Vermittlungsdiensten kommen für die in den Artikeln 4, 5 und 6 genannten Haftungsausschlüsse auch dann in Betracht, wenn sie auf Eigeninitiative nach Treu und Glauben und sorgfältig freiwillige Untersuchungen durchführen oder andere Maßnahmen zur Erkennung, Feststellung und Entfernung rechtswidriger Inhalte oder zur Sperrung des Zugangs zu rechtswidrigen Inhalten treffen oder die erforderlichen Maßnahmen ergreifen, um den Anforderungen des Unionsrechts und des nationalen Rechts im Einklang mit dem Unionsrecht und insbesondere den Anforderungen dieser Verordnung nachzukommen.

Artikel 8 Keine allgemeine Verpflichtung zur Überwachung oder aktiven Nachforschung

Anbietern von Vermittlungsdiensten wird keine allgemeine Verpflichtung auferlegt, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten.

Artikel 9 Anordnungen zum Vorgehen gegen rechtswidrige Inhalte

(1) Nach Eingang einer Anordnung zum Vorgehen gegen einen oder mehrere bestimmte rechtswidrige Inhalte, die von den zuständigen nationalen Justiz- oder Verwaltungsbehörden auf der Grundlage des geltenden Unionsrechts oder des nationalen Rechts im Einklang mit dem Unionsrecht erlassen wurde, informieren die Anbieter von Vermittlungsdiensten der eine Anordnung erlassenden Behörde oder einer anderen in der Anordnung genannten Behörde unverzüglich über die Ausführung der Anordnung, und geben an, ob und wann sie die Anordnung ausgeführt haben.

(2) Die Mitgliedstaaten sorgen dafür, dass eine in Absatz 1 genannte Anordnung bei der Übermittlung an den Diensteanbieter mindestens die folgenden Bedingungen erfüllt:

a) diese Anordnung enthält Folgendes:

- i) eine Angabe der Rechtsgrundlage nach Maßgabe des Unionsrechts oder des nationalen Rechts für die Anordnung,
- ii) eine Begründung, warum es sich bei den Informationen um rechtswidrige Inhalte handelt, mit Bezugnahme auf eine oder mehrere besondere Bestimmungen des Unionsrechts oder des nationalen Rechts im Einklang mit dem Unionsrecht,
- iii) Informationen zur Identifizierung der anordnenden Behörde,
- iv) klare Angaben, anhand deren der Anbieter von Vermittlungsdiensten die betreffenden rechtswidrigen Inhalte ermitteln und ausfindig machen kann, beispielsweise eine oder mehrere präzise URL-Adressen, und, soweit erforderlich, weitere Angaben,
- v) Angaben über Rechtsbehelfsmechanismen, die dem Anbieter von Vermittlungsdiensten und dem Nutzer, der den Inhalt bereitgestellt hat, zur Verfügung stehen,
- vi) unter Umständen Angaben dazu, welche Behörde über die Ausführung der Anordnung zu informieren ist;

b) der räumliche Geltungsbereich dieser Anordnung ist auf der Grundlage der geltenden Vorschriften des Unionsrechts und des nationalen Rechts, einschließlich der Charta, und, falls anwendbar, der allgemeinen Grundsätze des Völkerrechts auf das zur Erreichung ihres Ziels unbedingt erforderliche Maß beschränkt;

c) diese Anordnung wird in einer der vom Anbieter von Vermittlungsdiensten gemäß Artikel 11 Absatz 3 angegebenen Sprachen oder in einer anderen Amtssprache der Mitgliedstaaten, auf die sich die die Anordnung erlassende Behörde und dieser Anbieter geeinigt haben, übermittelt und an die von diesem Anbieter gemäß Artikel 11 benannte elektronische Kontaktstelle geschickt; ist die Anordnung nicht in der vom Anbieter von Vermittlungsdiensten angegebenen Sprache oder in einer anderen bilateral vereinbarten Sprache abgefasst, so kann die Anordnung in der Sprache der erlassenden Behörde übermittelt werden, sofern ihr zumindest eine Übersetzung der unter den Buchstaben a und b dieses Absatzes genannten Elemente in eine solche angegebene oder bilateral vereinbarte Sprache beigelegt ist.

(3) Die die Anordnung erlassende Behörde oder die unter Umständen darin angegebene Behörde übermittelt sie zusammen mit jeglichen vom Anbieter von Vermittlungsdiensten erhaltenen Angaben über die Ausführung dieser Anordnung dem Koordinator für digitale Dienste im Mitgliedstaat der erlassenden Behörde.

(4) Nach Erhalt der Anordnung von der Justiz- oder Verwaltungsbehörde übermittelt der Koordinator für digitale Dienste des betroffenen Mitgliedstaats allen anderen Koordinatoren für digitale Dienste unverzüglich über das nach Artikel 85 eingerichtete System eine Kopie der in Absatz 1 genannten Anordnung.

(5) Spätestens zum Zeitpunkt der Befolgung der Anordnung oder gegebenenfalls zu dem Zeitpunkt, den die erlassende Behörde in ihrer Anordnung angegeben hat, informieren Anbieter von Vermittlungsdiensten den betroffenen Nutzer über die erhaltene Anordnung und deren Ausführung. Diese Unterrichtung des Nutzers

umfasst eine Begründung, die existierenden Rechtsbehelfsmöglichkeiten und eine Beschreibung des räumlichen Geltungsbereichs der Anordnung gemäß Absatz 2.

(6) Die in diesem Artikel festgelegten Bedingungen und Anforderungen lassen das nationale Zivil- und Strafprozessrecht unberührt.

Artikel 10 Auskunftsanordnungen

(1) Nach Eingang einer Auskunftsanordnung in Bezug auf bestimmte Informationen über einen oder mehrere bestimmte einzelne Nutzer, die von den zuständigen nationalen Justiz- oder Verwaltungsbehörden auf der Grundlage des geltenden Unionsrechts oder des nationalen Rechts im Einklang mit dem Unionsrecht erlassen wurde, informieren die Anbieter von Vermittlungsdiensten der erlassenden Behörde oder einer anderen in der Anordnung genannten Behörde unverzüglich über den Erhalt der Anordnung und die Ausführung der Anordnung, und geben an, ob und wann sie die Anordnung ausgeführt haben.

(2) Die Mitgliedstaaten sorgen dafür, dass eine in Absatz 1 genannte Anordnungen bei der Übermittlung an den Diensteanbieter mindestens die folgenden Bedingungen erfüllt:

a) diese Anordnung enthält Folgendes:

- i) eine Angabe der Rechtsgrundlage nach Maßgabe des Unionsrechts oder des nationalen Rechts für die Anordnung;
- ii) Informationen zur Identifizierung der erlassenden Behörde;
- iii) klare Angaben, anhand deren der Anbieter von Vermittlungsdiensten den bzw. die bestimmten Empfänger ermitteln können, zu dem Informationen angefordert werden, etwa einen oder mehrere Kontonamen oder eindeutige Kennungen;
- iv) eine Begründung, wozu die Informationen benötigt werden und warum die Auskunftsanordnung erforderlich und verhältnismäßig ist, um festzustellen, ob die Nutzer des Vermittlungsdienstes das geltende Unionsrecht oder nationale Recht im Einklang mit dem Unionsrecht einhalten, es sei denn, eine solche Begründung kann aus Gründen der Verhütung, Ermittlung, Erkennung und Verfolgung von Straftaten nicht gegeben werden;
- v) Angaben über Rechtsbehelfsmechanismen, die dem Diensteanbieter und den betreffenden Nutzern zur Verfügung stehen;
- vi) unter Umständen Angaben dazu, welche Behörde über die Ausführung der Anordnung zu informieren ist;

b) diese Anordnung verpflichtet den Diensteanbieter nur zur Bereitstellung von Informationen, die er ohnehin bereits für die Zwecke der Erbringung des Dienstes erfasst hat und die seiner Verfügungsgewalt unterliegen;

c) diese Anordnung wird in einer der vom Anbieter von Vermittlungsdiensten gemäß Artikel 11 Absatz 3 angegebenen Sprachen oder in einer anderen Amtssprache der Mitgliedstaaten, auf die sich die die Anordnung erlassende Behörde und der Diensteanbieter geeinigt haben, übermittelt und an die vom Anbieter gemäß Artikel 11 benannte elektronische Kontaktstelle geschickt. Ist die Anordnung nicht in der vom Anbieter von Vermittlungsdiensten angegebenen Sprache oder in einer anderen bilateral vereinbarten Sprache abgefasst, so kann die Anordnung in der Sprache der erlassenden Behörde übermittelt werden, sofern ihr zumindest eine Übersetzung der unter den Buchstaben a und b dieses Absatzes genannten Elemente in eine solche angegebene oder bilateral vereinbarte Sprache beigefügt ist.

(3) Die die Anordnung erlassende Behörde oder die unter Umständen darin angegebene Behörde übermittelt sie dem Koordinator für digitale Dienste im Mitgliedstaat der erlassenden Behörde zusammen mit den vom Anbieter von Vermittlungsdiensten erhaltenen Angaben über die Ausführung dieser Anordnung.

(4) Nach Erhalt der Anordnung von der Justiz- oder Verwaltungsbehörde übermittelt der Koordinator für digitale Dienste des betroffenen Mitgliedstaats allen Koordinatoren für digitale Dienste unverzüglich über das nach Artikel 85 eingerichtete System eine Kopie der in Absatz 1 genannten Anordnung.

(5) Spätestens zum Zeitpunkt der Befolgung der Anordnung oder gegebenenfalls zu dem Zeitpunkt, den die erlassende Behörde in ihrer Anordnung angegeben hat informieren Anbieter von Vermittlungsdiensten den

betreffenden Nutzer über den Erhalt der Anordnung und über deren Ausführung. Diese Unterrichtung des Nutzers umfasst eine Begründung und die existierenden Rechtsbehelfsmöglichkeiten gemäß Absatz 2.

(6) Die in diesem Artikel festgelegten Bedingungen und Anforderungen lassen das nationale Zivil- und Strafprozessrecht unberührt.

KAPITEL III SORGFALTSPFLICHTEN FÜR EIN TRANSPARENTES UND SICHERES ONLINE-UMFELD

ABSCHNITT 1 Bestimmungen für alle Anbieter von Vermittlungsdiensten

Artikel 11 Kontaktstellen für die Behörden der Mitgliedstaaten, die Kommission und den Vorstand

(1) Die Anbieter von Vermittlungsdiensten benennen eine zentrale Kontaktstelle, damit sie auf elektronischem Wege unmittelbar mit den Behörden der Mitgliedstaaten, der Kommission und dem in Artikel 61 genannten Gremium in Bezug auf die Anwendung dieser Verordnung kommunizieren können.

(2) Die Anbieter von Vermittlungsdiensten veröffentlichen die Informationen, die nötig sind, um ihre zentrale Kontaktstelle leicht zu ermitteln und mit ihr zu kommunizieren. Diese Informationen müssen leicht zugänglich sein und stets auf dem aktuellen Stand gehalten werden.

(3) In den in Absatz 2 genannten Informationen machen die Anbieter von Vermittlungsdiensten Angaben zu der bzw. den Amtssprachen der Mitgliedstaaten, die – zusätzlich zu einer Sprache, die von möglichst vielen Unionsbürgerinnen und Unionsbürgern verstanden wird – zur Kommunikation mit ihrer Kontaktstelle verwendet werden können und zu denen mindestens eine der Amtssprachen des Mitgliedstaats gehören muss, in dem der Anbieter von Vermittlungsdiensten seine Hauptniederlassung hat oder in dem sein gesetzlicher Vertreter ansässig oder niedergelassen ist.

Artikel 12 Kontaktstellen für Nutzer der Dienste

(1) Die Anbieter von Vermittlungsdiensten benennen eine zentrale Kontaktstelle, die es den Nutzern ermöglicht, direkt und schnell mit ihnen zu kommunizieren, und zwar auf elektronischem Wege und in einer benutzerfreundlichen Weise, indem sie den Nutzern auch die Wahl des Kommunikationsmittels überlassen, das nicht ausschließlich auf automatisierten Instrumenten beruhen darf.

(2) Zusätzlich zu den Verpflichtungen nach der Richtlinie 2000/31/EG veröffentlichen die Anbieter von Vermittlungsdiensten die Informationen, die erforderlich sind, damit die Nutzer die zentralen Kontaktstellen der Anbieter von Vermittlungsdiensten leicht ermitteln und mit ihnen kommunizieren können. Diese Informationen müssen leicht zugänglich sein und stets auf dem aktuellen Stand gehalten werden.

Artikel 13 Gesetzlicher Vertreter

(1) Die Anbieter von Vermittlungsdiensten, die keine Niederlassung in der Union haben, aber Dienstleistungen in der Union anbieten, benennen schriftlich eine juristische oder natürliche Person, die in einem der Mitgliedstaaten, in denen sie ihre Dienste anbieten, als ihr gesetzlicher Vertreter fungiert.

(2) Die Anbieter von Vermittlungsdiensten bevollmächtigen ihre gesetzlichen Vertreter, sodass diese zusätzlich oder anstelle der Diensteanbieter von den zuständigen Behörden der Mitgliedstaaten, der Kommission und dem Gremium zu allen Fragen in Anspruch genommen werden können, die für die Entgegennahme, Einhaltung und Durchsetzung von Beschlüssen im Zusammenhang mit dieser Verordnung erforderlich sind. Die Anbieter von Vermittlungsdiensten statten ihren gesetzlichen Vertreter mit den notwendigen Befugnissen und hinreichenden Ressourcen aus, damit er wirksam und zeitnah mit den zuständigen Behörden der Mitgliedstaaten, der Kommission und dem Gremium zusammenarbeiten und den Beschlüssen nachkommen kann.

(3) Es ist möglich, den benannten gesetzlichen Vertreter für Verstöße gegen Pflichten aus dieser Verordnung haftbar zu machen; die Haftung und die rechtlichen Schritte, die gegen den Anbieter von Vermittlungsdiensten eingeleitet werden können, bleiben hiervon unberührt.

(4) Die Anbieter von Vermittlungsdiensten melden dem Koordinator für digitale Dienste in dem Mitgliedstaat, in dem ihr gesetzlicher Vertreter ansässig oder niedergelassen ist, den Namen, die Postanschrift, die E-Mail-Adresse und die Telefonnummer ihres gesetzlichen Vertreters. Sie sorgen dafür, dass diese Angaben öffentlich verfügbar, leicht zugänglich, richtig und stets aktuell sind.

(5) Die Benennung eines gesetzlichen Vertreters in der Union gemäß Absatz 1 gilt nicht als Niederlassung in der Union.

Artikel 14 Allgemeine Geschäftsbedingungen

(1) Die Anbieter von Vermittlungsdiensten machen in ihren allgemeinen Geschäftsbedingungen Angaben zu etwaigen Beschränkungen in Bezug auf die von den Nutzern bereitgestellten Informationen, die sie im Zusammenhang mit der Nutzung ihres Dienstes auferlegen. Diese Angaben enthalten Angaben zu allen Leitlinien, Verfahren, Maßnahmen und Werkzeuge, die zur Moderation von Inhalten eingesetzt werden, einschließlich der algorithmischen Entscheidungsfindung und der menschlichen Überprüfung, sowie zu den Verfahrensregeln für ihr internes Beschwerdemanagementsystem. Sie werden in klarer, einfacher, verständlicher, benutzerfreundlicher und eindeutiger Sprache abgefasst und in leicht zugänglicher und maschinenlesbarer Form öffentlich zur Verfügung gestellt.

(2) Die Anbieter von Vermittlungsdiensten informieren die Nutzer über etwaige wesentliche Änderungen der allgemeinen Geschäftsbedingungen.

(3) Richtet sich ein Vermittlungsdienst in erster Linie an Minderjährige oder wird er überwiegend von Minderjährigen genutzt, so erläutert der Anbieter von Vermittlungsdiensten die Bedingungen und jegliche Einschränkungen für die Nutzung des Dienstes so, dass Minderjährige sie verstehen können.

(4) Die Anbieter von Vermittlungsdiensten gehen bei der Anwendung und Durchsetzung der in Absatz 1 genannten Beschränkungen sorgfältig, objektiv und verhältnismäßig vor und berücksichtigen dabei die Rechte und berechtigten Interessen aller Beteiligten sowie die Grundrechte der Nutzer, die in der Charta verankert sind, etwa das Recht auf freie Meinungsäußerung, die Freiheit und den Pluralismus der Medien und andere Grundrechte und -freiheiten.

(5) Die Anbieter sehr großer Online-Plattformen und sehr großer Suchmaschinen stellen den Nutzern eine kompakte, leicht zugängliche und maschinenlesbare Zusammenfassung der allgemeinen Geschäftsbedingungen einschließlich der verfügbaren Rechtsbehelfe und Rechtsbehelfsmechanismen in klarer und eindeutiger Sprache zur Verfügung.

(6) Sehr große Online-Plattformen und sehr große Online-Suchmaschinen im Sinne von Artikel 33 veröffentlichen ihre allgemeinen Geschäftsbedingungen in den Amtssprachen aller Mitgliedstaaten, in denen sie ihre Dienste anbieten.

Artikel 15 Transparenzberichtspflichten der Anbieter von Vermittlungsdiensten

(1) Die Anbieter von Vermittlungsdiensten stellen mindestens einmal jährlich in einem maschinenlesbaren Format und auf leicht zugängliche Art und Weise klare, leicht verständliche Berichte über die von ihnen in dem betreffenden Zeitraum durchgeführte Moderation von Inhalten öffentlich zur Verfügung. Diese Berichte enthalten – soweit zutreffend – insbesondere folgende Angaben:

a) bei Anbietern von Vermittlungsdiensten die Anzahl der von Behörden der Mitgliedstaaten erhaltenen Anordnungen einschließlich der gemäß den Artikeln 9 und 10 erlassenen Anordnungen, aufgeschlüsselt nach der Art der betroffenen rechtswidrigen Inhalte, dem die Anordnung erlassenden Mitgliedstaat und der Medianzeit, die benötigt wurde, um die die Anordnung erlassende Behörde bzw. die anderen in der Anordnung angegebenen Behörden über den Eingang der Anordnung zu unterrichten und der Anordnung nachzukommen;

b) bei Hostingdiensteanbietern die Anzahl der nach Artikel 16 gemachten Meldungen, aufgeschlüsselt nach der Art der betroffenen mutmaßlich rechtswidrigen Inhalte, die Anzahl der durch vertrauenswürdige Hinweisgeber übermittelten Meldungen, alle aufgrund der Meldungen ergriffenen Maßnahmen, unterschieden danach, ob dies auf gesetzlicher Grundlage oder gemäß den allgemeinen Geschäftsbedingungen des Anbieters erfolgt ist, die Anzahl der ausschließlich automatisch verarbeiteten Meldungen und die Mediandauer bis zur Ergreifung der Maßnahmen;

c) bei Anbietern von Vermittlungsdiensten aussagekräftige und verständliche Informationen über die auf Eigeninitiative des Anbieters durchgeführte Moderation von Inhalten einschließlich der Nutzung automatisierter Werkzeuge, der Maßnahmen zur Schulung und Unterstützung der für die Moderation von Inhalten zuständigen Personen, der Anzahl und Art der ergriffenen Maßnahmen, die sich auf die

Verfügbarkeit, Erkennbarkeit und Zugänglichkeit der von den Nutzern bereitgestellten Informationen auswirken, und der Fähigkeit der Nutzer, solche Informationen über den Dienst bereitzustellen, und anderer entsprechender Beschränkungen des Dienstes; die gemeldeten Informationen werden nach der Art der rechtswidrigen Inhalte oder des Verstoßes gegen die allgemeinen Geschäftsbedingungen des Diensteanbieters, nach der zur Aufspürung verwendeten Methode und der Art der angewendeten Beschränkung aufgeschlüsselt;

d) bei Anbietern von Vermittlungsdiensten die Anzahl der Beschwerden, die gemäß den allgemeinen Geschäftsbedingungen des Anbieters über die internen Beschwerdemanagementsysteme und darüber hinaus – bei Anbietern von Online-Plattformen – gemäß Artikel 20 eingegangen sind, die Grundlage dieser Beschwerden, die zu diesen Beschwerden getroffenen Entscheidungen, die bis zur Entscheidung benötigte Mediandauer und die Anzahl der Fälle, in denen diese Entscheidungen rückgängig gemacht wurden.

e) die etwaige Verwendung automatisierter Mittel zur Moderation von Inhalten, mit einer qualitativen Beschreibung, mit Angabe der genauen Zwecke, mit Indikatoren für die Genauigkeit und mit der möglichen Fehlerquote der bei der Erfüllung dieser Zwecke verwendeten automatisierten Mittel und mit angewandten Schutzvorkehrungen.

(2) Absatz 1 des vorliegenden Artikels gilt nicht für Anbieter von Vermittlungsdiensten, bei denen es sich um Kleinst- oder Kleinunternehmen gemäß der Empfehlung 2003/361/EG handelt und die nicht als sehr große Online-Plattform im Sinne von Artikel 33 dieser Verordnung gelten.

(3) Die Kommission kann Durchführungsrechtsakte erlassen, in denen sie Vorlagen für Form, Inhalt und sonstige Einzelheiten der Berichte nach Absatz 1 des vorliegenden Artikels einschließlich harmonisierter Berichtszeiträume festlegt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 88 genannten Beratungsverfahren erlassen.

ABSCHNITT 2 Zusätzliche Bestimmungen für Hostingdiensteanbieter, einschließlich Online-Plattformen

Artikel 16 Melde- und Abhilfeverfahren

(1) Die Hostingdiensteanbieter richten Verfahren ein, nach denen Personen oder Einrichtungen ihnen das Vorhandensein von Einzelinformationen in ihren Diensten melden können, die die betreffende Person oder Einrichtung als rechtswidrige Inhalte ansieht. Diese Verfahren müssen leicht zugänglich und benutzerfreundlich sein und eine Übermittlung von Meldungen ausschließlich auf elektronischem Weg ermöglichen.

(2) Mit den in Absatz 1 genannten Verfahren muss das Übermitteln hinreichend genauer und angemessen begründeter Meldungen erleichtert werden. Dazu ergreifen die Hostingdiensteanbieter die erforderlichen Maßnahmen, um die Übermittlung von Meldungen zu ermöglichen und zu erleichtern, die alle folgenden Elemente enthalten:

- a) eine hinreichend begründete Erläuterung, warum die betreffende Person oder Einrichtung die fraglichen Informationen als rechtswidrige Inhalte ansieht;
- b) eine eindeutige Angabe des genauen elektronischen Speicherorts dieser Informationen, etwa die präzise URL-Adresse bzw. die präzisen URL-Adressen, oder, soweit erforderlich, weitere, hinsichtlich der Art der Inhalte und der konkreten Art des Hostingdienstes zweckdienliche Angaben zur Ermittlung der rechtswidrigen Inhalte;
- c) den Namen und die E-Mail-Adresse der meldenden Person oder Einrichtung, es sei denn, es handelt sich um Informationen, bei denen davon ausgegangen wird, dass sie eine in den Artikeln 3 bis 7 der Richtlinie 2011/93/EU genannte Straftat betreffen;
- d) eine Erklärung darüber, dass die meldende Person oder Einrichtung in gutem Glauben davon überzeugt ist, dass die in der Meldung enthaltenen Angaben und Anführungen richtig und vollständig sind.

(3) Die im vorliegenden Artikel genannten Meldungen bewirken, dass für die Zwecke des Artikels 6 von einer tatsächlichen Kenntnis oder einem Bewusstsein in Bezug auf die betreffende Einzelinformation ausgegangen wird, wenn sie es einem sorgfältig handelnden Anbieter von Hostingdiensten ermöglichen, ohne eingehende rechtliche Prüfung festzustellen, dass die einschlägige Tätigkeit oder Information rechtswidrig ist.

(4) Enthält die Meldung die elektronische Kontaktangabe der meldenden Person oder Einrichtung, so schickt der Hostingdiensteanbieter dieser Person oder Einrichtung unverzüglich eine Empfangsbestätigung.

(5) Ferner teilt der Anbieter der betreffenden Person oder Einrichtung unverzüglich seine Entscheidung in Bezug auf die gemeldeten Informationen mit und weist dabei auf die möglichen Rechtsbehelfe gegen diese Entscheidung hin.

(6) Die Hostingdiensteanbieter bearbeiten alle Meldungen, die sie im Rahmen der in Absatz 1 genannten Verfahren erhalten, und entscheiden zeitnah, sorgfältig, frei von Willkür und objektiv über die gemeldeten Informationen. Wenn sie zu dieser Bearbeitung oder Entscheidungsfindung automatisierte Mittel einsetzen, machen sie in ihrer Mitteilung nach Absatz 5 auch Angaben über den Einsatz dieser Mittel.

Artikel 17 Begründung

(1) Die Hostingdiensteanbieter legen allen betroffenen Nutzern eine klare und spezifische Begründung für alle folgenden Beschränkungen vor, die mit der Begründung verhängt werden, dass es sich bei den vom Nutzer bereitgestellten Informationen um rechtswidrige Inhalte handelt oder diese nicht mit ihren Nutzungsbedingungen vereinbar sind:

- a) etwaige Beschränkungen der Anzeige bestimmter Einzelinformationen, die vom Nutzer bereitgestellt werden, einschließlich Entfernung von Inhalten, Sperrung des Zugangs zu Inhalten oder Herabstufung von Inhalten;
- b) Aussetzung, Beendigung oder sonstige Beschränkung von Geldzahlungen;
- c) Aussetzung oder Beendigung der gesamten oder teilweisen Bereitstellung des Dienstes;
- d) Aussetzung oder Schließung des Kontos des Nutzers.

(2) Absatz 1 findet nur Anwendung, wenn dem Anbieter die einschlägigen elektronischen Kontaktangaben bekannt sind. Er findet spätestens ab dem Datum Anwendung, zu dem die Beschränkung verhängt wird, ungeachtet dessen, warum oder wie sie verhängt wurde.

Absatz 1 findet keine Anwendung, wenn es sich um einen irreführenden, umfangreichen kommerziellen Inhalt handelt.

(3) Die in Absatz 1 genannte Begründung muss mindestens folgende Angaben enthalten:

- a) Angaben darüber, ob die Entscheidung die Entfernung der Information, die Sperrung des Zugangs zu der Information, die Herabstufung der Information oder die Einschränkung der Anzeige der Information oder die Aussetzung oder Beendigung von Zahlungen in Verbindung mit dieser Information betrifft oder mit der Entscheidung andere in Absatz 1 genannte Maßnahmen im Zusammenhang mit der Information verhängt werden, und den etwaigen räumlichen Geltungsbereich der Entscheidung und die Dauer ihrer Gültigkeit;
- b) die Tatsachen und Umstände, auf denen die Entscheidung beruht, gegebenenfalls einschließlich Angaben darüber, ob die Entscheidung infolge einer nach Artikel 16 gemachten Meldung oder infolge freiwilliger Untersuchungen auf Eigeninitiative getroffen wurde sowie, falls unbedingt notwendig, die Identität der meldenden Person;
- c) gegebenenfalls Angaben darüber, ob automatisierte Mittel zur Entscheidungsfindung verwendet wurden, einschließlich Angaben darüber, ob die Entscheidung in Bezug auf Inhalte getroffen wurde, die mit automatisierten Mitteln erkannt oder festgestellt wurden;
- d) falls die Entscheidung mutmaßlich rechtswidrige Inhalte betrifft, einen Verweis auf die Rechtsgrundlage und Erläuterungen, warum die Informationen auf dieser Grundlage als rechtswidrige Inhalte angesehen werden;
- e) falls die Entscheidung auf der mutmaßlichen Unvereinbarkeit der Informationen mit den allgemeinen Geschäftsbedingungen des Hostingdiensteanbieters beruht, einen Verweis auf die betreffende vertragliche Bestimmung und Erläuterungen, warum die Informationen als damit unvereinbar angesehen werden;

f) klare und benutzerfreundliche Informationen über die dem Nutzer gegen die Maßnahme zur Verfügung stehenden Rechtsbehelfe, insbesondere – je nach Sachlage – interne Beschwerdemanagementverfahren, außergerichtliche Streitbeilegung und gerichtliche Rechtsmittel.

(4) Die von den Hostingdiensteanbietern nach diesem Artikel übermittelten Informationen müssen klar und leicht verständlich und so genau und spezifisch sein, wie dies unter den gegebenen Umständen nach vernünftigem Ermessen möglich ist. Die Informationen müssen insbesondere so beschaffen sein, dass der betreffende Nutzer damit nach vernünftigem Ermessen in der Lage ist, die in Absatz 3 Buchstabe f genannten Rechtsbehelfe wirksam wahrzunehmen.

(5) Dieser Artikel gilt nicht für in Artikel 9 genannte Anordnungen.

Artikel 18 Meldung des Verdachts auf Straftaten

(1) Erhält ein Hostingdiensteanbieter Kenntnis von Informationen, die den Verdacht begründen, dass eine Straftat, die eine Gefahr für das Leben oder die Sicherheit einer Person oder von Personen darstellt, begangen wurde, begangen wird oder begangen werden könnte, so teilt er seinen Verdacht unverzüglich den Strafverfolgungs- oder Justizbehörden des betreffenden Mitgliedstaats oder der betreffenden Mitgliedstaaten mit und stellt alle vorliegenden einschlägigen Informationen zur Verfügung.

(2) Kann der Hostingdiensteanbieter den betreffenden Mitgliedstaat nicht mit hinreichender Gewissheit ermitteln, so unterrichtet er die Strafverfolgungsbehörden des Mitgliedstaats, in dem er niedergelassen ist oder in dem sein gesetzlicher Vertreter ansässig oder niedergelassen ist, oder Europol oder beide Stellen.

Für die Zwecke dieses Artikels gilt als betreffender Mitgliedstaat der Mitgliedstaat, in dem die Straftat begangen wurde, begangen wird oder begangen werden könnte, oder der Mitgliedstaat, in dem der Verdächtige seinen Wohnsitz oder Aufenthaltsort hat, oder der Mitgliedstaat, in dem das Opfer seinen Wohnsitz oder Aufenthaltsort hat.

ABSCHNITT 3 Zusätzliche Bestimmungen für Anbieter von Online-Plattformen

Artikel 19 Ausnahme für Kleinst- und Kleinunternehmen

(1) Der vorliegende Abschnitt gilt mit Ausnahme von Artikel 24 Absatz 3 nicht für Anbieter von Online-Plattformen, bei denen es sich um Kleinst- oder Kleinunternehmen gemäß der Empfehlung 2003/361/EG handelt.

Wenn Unternehmen den Status eines Kleinst- oder Kleinunternehmens gemäß der Empfehlung 2003/361/EG verlieren, findet der vorliegende Abschnitt mit Ausnahme von Artikel 24 Absatz 3 auch in den 12 Monaten nach dem Verlust dieses Status gemäß Artikel 4 Absatz 2 der Empfehlung keine Anwendung auf Anbieter von Online-Plattformen, es sei denn, sie sind sehr große Online-Plattformen im Sinne des Artikels 33.

(2) Abweichend von Absatz 1 findet der vorliegende Abschnitt Anwendung auf Anbieter von Online-Plattformen, die im Sinne des Artikels 33 als sehr große Online-Plattformen eingestuft wurden, unabhängig davon, ob sie als Kleinst- oder Kleinunternehmen gelten.

Artikel 20 Internes Beschwerdemanagementsystem

(1) Die Anbieter von Online-Plattformen gewähren den Nutzern einschließlich meldenden Personen oder Einrichtungen während eines Zeitraums von mindestens sechs Monaten nach einer Entscheidung gemäß diesem Absatz Zugang zu einem wirksamen internen Beschwerdemanagementsystem, das eine elektronische und kostenlose Einreichung von Beschwerden gegen die Entscheidung des Anbieters einer Online-Plattform nach Erhalt der Meldung oder gegen folgende Entscheidungen des Anbieters einer Online-Plattform ermöglicht, die damit begründet worden sind, dass die von den Nutzern bereitgestellten Informationen rechtswidrige Inhalte darstellen oder mit den allgemeinen Geschäftsbedingungen der Plattform unvereinbar sind:

a) Entscheidungen, ob die Information entfernt oder der Zugang dazu gesperrt oder die Anzeige der Information beschränkt wird;

b) Entscheidungen, ob die Erbringung des Dienstes gegenüber den Nutzern vollständig oder teilweise ausgesetzt oder beendet wird;

c) Entscheidungen, ob das Konto des Nutzers ausgesetzt oder geschlossen wird;

d) Entscheidungen, ob Geldzahlungen im Zusammenhang mit von den Nutzern bereitgestellten Informationen ausgesetzt, beendet oder die Fähigkeit der Nutzer zu deren Monetarisierung anderweitig eingeschränkt werden.

(2) Der Tag, an dem der Nutzer gemäß Artikel 16 Absatz 5 oder Artikel 17 von der Entscheidung in Kenntnis gesetzt wird, gilt als Beginn des in Absatz 1 des vorliegenden Artikels genannten Zeitraums von mindestens sechs Monaten.

(3) Die Anbieter von Online-Plattformen stellen sicher, dass ihre internen Beschwerdemanagementsysteme leicht zugänglich und benutzerfreundlich sind und die Einreichung hinreichend präziser und angemessen begründeter Beschwerden ermöglichen und erleichtern.

(4) Die Anbieter von Online-Plattformen bearbeiten Beschwerden, die über ihr internes Beschwerdemanagementsystem eingereicht werden, zeitnah, diskriminierungsfrei, sorgfältig und frei von Willkür. Enthält eine Beschwerde ausreichende Gründe für die Annahme, dass die Entscheidung, auf eine Meldung hin nicht tätig zu werden, unbegründet ist oder dass die Informationen, auf die sich die Beschwerde bezieht, weder rechtswidrig sind noch gegen die allgemeinen Geschäftsbedingungen verstoßen, oder enthält sie Informationen, aus denen hervorgeht, dass das Verhalten des Beschwerdeführers keine Aussetzung oder Kündigung des Dienstes oder Schließung des Kontos rechtfertigt, so macht der Anbieter der Online-Plattform seine in Absatz 1 genannte Entscheidung unverzüglich rückgängig.

(5) Die Anbieter von Online-Plattformen teilen den Beschwerdeführern unverzüglich ihre begründete Entscheidung mit, die sie in Bezug auf die Informationen, auf die sich die Beschwerde bezieht, getroffen haben, und weisen die Beschwerdeführer auf die Möglichkeit der außergerichtlichen Streitbeilegung gemäß Artikel 21 und auf andere verfügbare Rechtsbehelfe hin.

(6) Die Anbieter von Online-Plattformen stellen sicher, dass die in Absatz 5 genannten Entscheidungen unter der Aufsicht angemessen qualifizierten Personals und nicht allein mit automatisierten Mitteln getroffen werden.

Artikel 21 Außergerichtliche Streitbeilegung

(1) Nutzer, einschließlich meldender Personen oder Einrichtungen, die von den in Artikel 20 Absatz 1 genannten Entscheidungen betroffen sind, haben das Recht, zur Beilegung von Streitigkeiten im Zusammenhang mit diesen Entscheidungen sowie mit Beschwerden, die nicht mit den Mitteln des in dem Artikel genannten internen Beschwerdemanagementsystems gelöst wurden, eine gemäß Absatz 3 des vorliegenden Artikels zertifizierte außergerichtliche Streitbeilegungsstelle zu wählen.

Die Anbieter von Online-Plattformen stellen sicher, dass die Informationen über die in Unterabsatz 1 genannte Möglichkeit der Nutzer hinsichtlich des Zugangs zu einer außergerichtlichen Streitbeilegung in klarer und benutzerfreundlicher Form auf ihrer Online-Schnittstelle leicht zugänglich sind.

Unterabsatz 1 lässt das Recht des betroffenen Nutzers unberührt, im Einklang mit dem anwendbaren Recht zur Beanstandung der Entscheidungen von Anbietern von Online-Plattformen jederzeit vor Gericht zu ziehen.

(2) Beide Parteien arbeiten nach Treu und Glauben mit der ausgewählten zertifizierten außergerichtlichen Streitbeilegungsstelle zusammen, um die Streitigkeit beizulegen.

Die Anbieter von Online-Plattformen können die Zusammenarbeit mit einer solchen außergerichtlichen Streitbeilegungsstelle verweigern, wenn ein Streit bezüglich derselben Informationen und derselben Gründe für die mutmaßliche Rechtswidrigkeit der Inhalte oder ihre mutmaßliche Unvereinbarkeit mit den allgemeinen Geschäftsbedingungen bereits beigelegt wurde.

Die zugelassene außergerichtliche Streitbeilegungsstelle ist nicht befugt, den Parteien eine bindende Streitbeilegung aufzuerlegen.

(3) Der Koordinator für digitale Dienste des Mitgliedstaats, in dem die außergerichtliche Streitbeilegungsstelle niedergelassen ist, lässt diese Stelle auf deren Antrag hin für einen Zeitraum von höchstens fünf Jahren, der verlängert werden kann, zu, nachdem die Stelle nachgewiesen hat, dass sie alle folgenden Bedingungen erfüllt:

- a) sie ist unparteiisch und unabhängig, einschließlich finanziell unabhängig, von Anbietern von Online-Plattformen und von Nutzern der von diesen Plattformen erbrachten Dienste und auch von den meldenden Personen oder Einrichtungen;
- b) sie hat die erforderliche Sachkenntnis in Bezug auf Fragen, die sich in einem oder mehreren bestimmten Bereichen rechtswidriger Inhalte ergeben, oder in Bezug auf die Anwendung und Durchsetzung der allgemeinen Geschäftsbedingungen einer oder mehrerer Arten von Online-Plattformen, sodass die Stelle einen wirksamen Beitrag zur Beilegung einer Streitigkeit leisten kann;
- c) ihre Mitglieder werden auf eine Weise vergütet, die nicht mit dem Ergebnis des Verfahrens im Zusammenhang steht;
- d) die angebotene außergerichtliche Streitbeilegung ist über elektronische Kommunikationsmittel leicht zugänglich, und es besteht die Möglichkeit, die Streitbeilegung online einzuleiten und die erforderlichen einschlägigen Dokumente online einzureichen;
- e) sie ist in der Lage, Streitigkeiten rasch, effizient und kostengünstig in mindestens einer der Amtssprachen der Organe der Union beizulegen;
- f) die angebotene außergerichtliche Streitbeilegung erfolgt nach klaren und fairen Verfahrensregeln, die leicht und öffentlich zugänglich sind und die mit dem geltenden Recht, einschließlich dieses Artikels, vereinbar sind.

Der Koordinator für digitale Dienste gibt folgendes in der Zulassung an:

- a) die besonderen Angelegenheiten gemäß Unterabsatz 1 Buchstabe b, in denen die Stelle Sachkenntnis besitzt, und
- b) die Amtssprache bzw. die Amtssprachen der Organe der Union, in der bzw. denen die Stelle in der Lage ist, Streitigkeiten gemäß Unterabsatz 1 Buchstabe e beizulegen.

(4) Die zugelassenen außergerichtlichen Streitbeilegungsstellen erstatten dem Koordinator für digitale Dienste, der sie zugelassen hat, jährlich Bericht über ihre Tätigkeit und geben dabei zumindest die Zahl der bei ihnen eingegangenen Streitfälle, die Informationen über die Ergebnisse dieser Streitfälle, die durchschnittliche Dauer der Streitbeilegung und etwaige Mängel oder Schwierigkeiten an. Auf Anforderung des Koordinators für digitale Dienste erteilen sie zusätzliche Auskünfte.

Die Koordinatoren für digitale Dienste erstellen alle zwei Jahre einen Bericht über das Funktionieren der von ihnen zugelassenen außergerichtlichen Streitbeilegungsstellen. Dieser Bericht umfasst insbesondere

- a) eine Liste mit der Anzahl der bei den einzelnen zugelassenen außergerichtlichen Streitbeilegungsstellen pro Jahr eingegangenen Streitfälle;
- b) Angaben über die Ergebnisse der bei ihnen eingegangenen Streitfälle und über die durchschnittliche Dauer der Streitbeilegung;
- c) eine Darlegung und Erläuterung der etwaigen systematischen oder branchenbezogenen Mängel oder Schwierigkeiten im Zusammenhang mit der Arbeitsweise dieser Stellen;
- d) eine Darlegung der bewährten Verfahren in Bezug auf diese Arbeitsweise;
- e) etwaige Empfehlungen zur Verbesserung dieser Arbeitsweise.

Die zugelassenen außergerichtlichen Streitbeilegungsstellen stellen den Parteien innerhalb einer angemessenen Frist, spätestens jedoch 90 Kalendertage nach Eingang der Beschwerde, ihre Entscheidungen zur Verfügung. Im Fall hochkomplexer Streitfälle kann die zugelassene außergerichtliche Streitbeilegungsstelle den Zeitraum von 90 Kalendertagen nach eigenem Ermessen um einen weiteren Zeitraum verlängern, der 90 Tage nicht überschreiten darf, sodass sich die maximale Gesamtdauer auf 180 Tage beläuft.

(5) Entscheidet die außergerichtliche Streitbeilegungsstelle die Streitigkeit zugunsten des Nutzers, einschließlich der meldenden Person oder Einrichtung, so trägt der Anbieter der Online-Plattform sämtliche von der außergerichtlichen Streitbeilegungsstelle erhobenen Gebühren und erstattet dem Nutzer, einschließlich der Person oder Einrichtung, alle sonstigen angemessenen Kosten, die er bzw. sie im Zusammenhang mit der

Streitbeilegung gezahlt haben. Entscheidet die außergerichtliche Streitbeilegungsstelle die Streitigkeit zugunsten des Anbieters der Online-Plattform, so ist der Nutzer, einschließlich der meldenden Person oder Einrichtung, nicht verpflichtet, Gebühren oder sonstige Kosten zu erstatten, die der Anbieter der Online-Plattform im Zusammenhang mit der Streitbeilegung gezahlt hat oder noch zahlen muss, es sei denn, die außergerichtliche Streitbeilegungsstelle gelangt zu der Erkenntnis, dass der Nutzer eindeutig böswillig gehandelt hat.

Die von der außergerichtlichen Streitbeilegungsstelle von den Anbietern von Online-Plattformen erhobenen Gebühren müssen angemessen sein und dürfen in keinem Fall die der Streitbeilegungsstelle entstandenen Kosten übersteigen. Für Nutzer ist die Streitbeilegung kostenlos oder für eine Schutzgebühr verfügbar sein.

Die zugelassenen außergerichtlichen Streitbeilegungsstellen geben dem Nutzer, einschließlich der meldenden Personen oder Einrichtungen, und dem Anbieter der Online-Plattform die Gebühren oder das zur Gebührenfestsetzung verwendete Verfahren vor der Einleitung der Streitbeilegung bekannt.

(6) Die Mitgliedstaaten können für die Zwecke des Absatzes 1 außergerichtliche Streitbeilegungsstellen einrichten oder die Tätigkeiten einiger oder aller außergerichtlichen Streitbeilegungsstellen, die sie gemäß Absatz 3 zugelassen haben, unterstützen.

Die Mitgliedstaaten stellen sicher, dass ihre nach Unterabsatz 1 unternommenen Handlungen ihre Koordinatoren für digitale Dienste nicht darin beeinträchtigen, die betreffenden Stellen gemäß Absatz 3 zuzulassen.

(7) Ein Koordinator für digitale Dienste, der eine außergerichtliche Streitbeilegungsstelle zugelassen hat, widerruft diese Zulassung, wenn er infolge einer Untersuchung, die er auf eigene Initiative oder aufgrund von von Dritten erhaltenen Informationen durchführt, feststellt, dass die betreffende außergerichtliche Streitbeilegungsstelle die in Absatz 3 genannten Bedingungen nicht mehr erfüllt. Bevor er diese Zulassung widerruft, gibt der Koordinator für digitale Dienste dieser Stelle Gelegenheit, sich zu den Ergebnissen seiner Untersuchung und zu dem beabsichtigten Widerruf der Zulassung der außergerichtlichen Streitbeilegungsstelle zu äußern.

(8) Die Koordinatoren für digitale Dienste teilen der Kommission die außergerichtlichen Streitbeilegungsstellen mit, die sie gemäß Absatz 3 zugelassen haben, gegebenenfalls einschließlich der in Unterabsatz 2 jenes Absatzes genannten Spezifikationen, sowie die außergerichtlichen Streitbeilegungsstellen, deren Zulassung sie widerrufen haben. Die Kommission veröffentlicht auf einer eigens hierfür eingerichteten und leicht zugänglichen Website eine Liste dieser Stellen, einschließlich der genannten Spezifikationen, und hält diese auf dem neuesten Stand.

(9) Dieser Artikel lässt die Richtlinie 2013/11/EU sowie die alternativen Streitbeilegungsverfahren und -stellen für Verbraucher, die nach jener Richtlinie eingerichtet wurden, unberührt.

Artikel 22 Vertrauenswürdige Hinweisgeber

(1) Die Anbieter von Online-Plattformen ergreifen die erforderlichen technischen und organisatorischen Maßnahmen, damit Meldungen, die von in ihrem ausgewiesenen Fachgebiet tätigen vertrauenswürdigen Hinweisgebern über die in Artikel 16 genannten Mechanismen übermittelt werden, vorrangig behandelt und unverzüglich bearbeitet und einer Entscheidung zugeführt werden.

(2) Der Status des vertrauenswürdigen Hinweisgebers nach dieser Verordnung wird auf Antrag einer Stelle vom Koordinator für digitale Dienste des Mitgliedstaats, in dem der Antragsteller niedergelassen ist, einem Antragsteller zuerkannt, der nachgewiesen hat, dass er alle folgenden Bedingungen erfüllt:

- a) die Stelle hat besondere Sachkenntnis und Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte;
- b) sie ist unabhängig von jeglichen Anbietern von Online-Plattformen;
- c) sie übt ihre Tätigkeiten zur Übermittlung von Meldungen sorgfältig, genau und objektiv aus.

(3) Vertrauenswürdige Hinweisgeber veröffentlichen mindestens einmal jährlich leicht verständliche und ausführliche Berichte über die während des betreffenden Zeitraums gemäß Artikel 16 eingereichten Meldungen. In dem Bericht wird mindestens die Anzahl der Meldungen nach folgenden Kategorien aufgeführt:

- a) Identität des Hostingdiensteanbieters,
- b) Art der gemeldeten mutmaßlich rechtswidrigen Inhalte,
- c) vom Anbieter ergriffene Maßnahmen.

Diese Berichte enthalten eine Erläuterung der Verfahren, mit denen sichergestellt wird, dass der vertrauenswürdige Hinweisgeber seine Unabhängigkeit bewahrt.

Vertrauenswürdige Hinweisgeber übermitteln dem Koordinator für digitale Dienste diese Berichte und machen sie öffentlich zugänglich. Die Informationen in diesen Berichten dürfen keine personenbezogenen Daten enthalten.

(4) Die Koordinatoren für digitale Dienste teilen der Kommission und dem Gremium die Namen, Anschriften und E-Mail-Adressen der Stellen mit, denen sie den Status des vertrauenswürdigen Hinweisgebers nach Absatz 2 zuerkannt haben bzw. deren Status als vertrauenswürdige Hinweisgeber sie im Einklang mit Absatz 6 aufgehoben oder im Einklang mit Absatz 7 aberkannt haben.

(5) Die Kommission veröffentlicht die in Absatz 4 genannten Angaben in einem leicht zugänglichen und maschinenlesbaren Format in einer öffentlich zugänglichen Datenbank und hält diese auf dem neuesten Stand.

(6) Hat ein Anbieter von Online-Plattformen Informationen, aus denen hervorgeht, dass ein vertrauenswürdiger Hinweisgeber über die in Artikel 16 genannten Mechanismen eine erhebliche Anzahl nicht hinreichend präziser, ungenauer oder unzureichend begründeter Meldungen übermittelt hat, was auch Informationen einschließt, die im Zusammenhang mit der Bearbeitung von Beschwerden über die in Artikel 20 Absatz 4 genannten internen Beschwerdemanagementsysteme erfasst wurden, so übermittelt er dem Koordinator für digitale Dienste, der der betreffenden Stelle den Status des vertrauenswürdigen Hinweisgebers zuerkannt hat, diese Informationen zusammen mit den nötigen Erläuterungen und Nachweisen. Bei Erhalt der Information des Anbieters von Online-Plattformen und in dem Fall, dass der Koordinator für digitale Dienste der Ansicht ist, dass es berechnete Gründe für die Einleitung einer Untersuchung gibt, wird der Status des vertrauenswürdigen Hinweisgebers für den Zeitraum der Untersuchung aufgehoben. Diese Untersuchung wird unverzüglich durchgeführt.

(7) Der Koordinator für digitale Dienste, der einer Stelle den Status des vertrauenswürdigen Hinweisgebers zuerkannt hat, widerruft diesen Status, wenn er infolge einer Untersuchung, die er auf eigene Initiative oder aufgrund von Informationen durchführt, die er von Dritten erhalten hat, auch der von einem Anbieter von Online-Plattformen nach Absatz 6 vorgelegten Informationen, feststellt, dass die betreffende Stelle die in Absatz 2 genannten Bedingungen nicht mehr erfüllt. Bevor er diesen Status widerruft, gibt der Koordinator für digitale Dienste der Stelle Gelegenheit, sich zu den Ergebnissen seiner Untersuchung und zu dem beabsichtigten Widerruf des Status der Stelle als vertrauenswürdiger Hinweisgeber zu äußern.

(8) Die Kommission gibt nach Anhörung des Gremiums, soweit erforderlich, Leitlinien heraus, um die Anbieter von Online-Plattformen und die Koordinatoren für digitale Dienste bei der Anwendung der Absätze 2, 6 und 7 zu unterstützen.

Artikel 23 Maßnahmen und Schutz vor missbräuchlicher Verwendung

(1) Die Anbieter von Online-Plattformen setzen die Erbringung ihrer Dienste für Nutzer, die häufig und offensichtlich rechtswidrige Inhalte bereitstellen, für einen angemessenen Zeitraum nach vorheriger Warnung aus.

(2) Die Anbieter von Online-Plattformen setzen die Bearbeitung von Meldungen und Beschwerden, die über die in den Artikeln 16 und 20 genannten Melde- und Abhilfeverfahren bzw. interne Beschwerdemanagementsysteme von Personen oder Stellen oder von Beschwerdeführern eingehen, die häufig offensichtlich unbegründete Meldungen oder Beschwerden einreichen, für einen angemessenen Zeitraum nach vorheriger Warnung aus.

(3) Bei der Entscheidung über die Aussetzung bewerten die Anbieter von Online-Plattformen von Fall zu Fall zeitnah, sorgfältig und in objektiver Weise, ob der Nutzer, die Person, die Einrichtung oder der Beschwerdeführer an einer in den Absätzen 1 und 2 genannten missbräuchlichen Verwendung beteiligt ist, wobei sie alle einschlägigen Tatsachen und Umstände berücksichtigen, die aus den dem Anbieter von Online-Plattformen vorliegenden Informationen ersichtlich sind. Zu solchen Umständen gehören zumindest:

- a) die absolute Anzahl der offensichtlich rechtswidrigen Inhalte oder der offensichtlich unbegründeten Meldungen oder Beschwerden, die innerhalb eines bestimmten Zeitraums bereitgestellt bzw. eingereicht wurden;
- b) deren relativer Anteil an der Gesamtzahl der in einem bestimmten Zeitraum bereitgestellten Einzelinformationen oder innerhalb eines bestimmten Zeitraums gemachten Meldungen;
- c) die Schwere der Fälle der missbräuchlichen Verwendung, einschließlich der Art der rechtswidrigen Inhalte, und deren Folgen;
- d) die von dem Nutzer, der Person, der Einrichtung oder dem Beschwerdeführer verfolgten Absichten, sofern diese Absichten ermittelt werden können.

(4) Die Anbieter von Online-Plattformen legen in ihren allgemeinen Geschäftsbedingungen klar und ausführlich ihre Regeln für den Umgang mit der in den Absätzen 1 und 2 des vorliegenden Artikels genannten missbräuchlichen Verwendung dar und nennen Beispiele für Tatsachen und Umstände, die sie bei der Beurteilung, ob ein bestimmtes Verhalten eine missbräuchliche Verwendung darstellt, berücksichtigen, und für die Dauer der Aussetzung.

Artikel 24 Transparenzberichtspflichten der Anbieter von Online-Plattformen

(1) Zusätzlich zu den in Artikel 15 genannten Informationen nehmen die Anbieter von Online-Plattformen in die in jenem Artikel genannten Berichte folgende Informationen auf:

- a) Anzahl der Streitigkeiten, die den in Artikel 21 genannten außergerichtlichen Streitbeilegungsstellen vorgelegt wurden, Ergebnisse der Streitbeilegung und Mediandauer bis zum Abschluss der Streitbeilegungsverfahren sowie Anteil der Streitigkeiten, bei denen die Anbieter von Online-Plattform die Entscheidungen der Stelle umgesetzt haben;
- b) Anzahl der Aussetzungen nach Artikel 23, wobei zwischen Aussetzungen wegen offensichtlich rechtswidriger Inhalte, wegen Übermittlung offensichtlich unbegründeter Meldungen und wegen Einreichung offensichtlich unbegründeter Beschwerden zu unterscheiden ist.

(2) Bis zum 17. Februar 2023 und danach mindestens alle sechs Monate veröffentlichen Anbieter für jede Online-Plattform oder Online-Suchmaschine in einem öffentlich zugänglichen Bereich ihrer Online-Schnittstelle Informationen über die durchschnittliche monatliche Zahl ihrer aktiven Nutzer in der Union, berechnet als Durchschnitt der vergangenen sechs Monate und nach der Methode, die in den in Artikel 33 Absatz 3 genannten delegierten Rechtsakten festgelegt wird, wenn diese delegierten Rechtsakte erlassen wurden.

(3) Die Anbieter von Online-Plattformen oder Online-Suchmaschinen übermitteln dem Koordinator für digitale Dienste am Niederlassungsort und der Kommission auf deren Verlangen und unverzüglich die in Absatz 2 genannten Informationen, die zum Zeitpunkt dieses Verlangens aktualisiert werden. Dieser Koordinator für digitale Dienste oder die Kommission kann vom Anbieter der Online-Plattform oder der Online-Suchmaschine zusätzliche Informationen über die in jenem Absatz genannte Berechnung sowie Erläuterungen und Begründungen in Bezug auf die verwendeten Daten verlangen. Diese Informationen dürfen keine personenbezogenen Daten enthalten.

(4) Hat der Koordinator für digitale Dienste am Niederlassungsort auf der Grundlage der gemäß den Absätzen 2 und 3 dieses Artikels erhaltenen Informationen Grund zu der Annahme, dass ein Anbieter einer Online-Plattform oder einer Online-Suchmaschine den in Artikel 33 Absatz 1 festgelegten Schwellenwert der durchschnittlichen monatlichen aktiven Nutzer in der Union erreicht, so teilt er dies der Kommission mit.

(5) Die Anbieter von Online-Plattformen übermitteln der Kommission unverzüglich die in Artikel 17 Absatz 1 genannten Entscheidungen und Begründungen für die Aufnahme in eine öffentlich zugängliche, von der

Kommission verwaltete maschinenlesbare Datenbank. Die Anbieter von Online-Plattformen stellen sicher, dass die übermittelten Informationen keine personenbezogenen Daten enthalten.

(6) Die Kommission kann Durchführungsrechtsakte erlassen, in denen sie Vorlagen für Form, Inhalt und sonstige Einzelheiten der Berichte nach Absatz 1 des vorliegenden Artikels festlegt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 88 genannten Beratungsverfahren erlassen.

Artikel 25 Gestaltung und Organisation der Online-Schnittstelle

(1) Anbieter von Online-Plattformen dürfen ihre Online-Schnittstellen nicht so konzipieren, organisieren oder betreiben, dass Nutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden.

(2) Das Verbot in Absatz 1 gilt nicht für Praktiken, die unter die Richtlinie 2005/29/EG oder die Verordnung (EU) 2016/679 fallen.

(3) Die Kommission kann Leitlinien für die Anwendung von Absatz 1 auf eine bestimmte Praxis herausgeben, insbesondere in Bezug darauf,

- a) dass bestimmte Auswahlmöglichkeiten stärker hervorgehoben werden, wenn der Nutzer eine Entscheidung treffen muss,
- b) dass der Nutzer wiederholt aufgefordert wird, eine Auswahl zu treffen, obwohl eine solche Auswahl bereits getroffen wurde, insbesondere durch die Einblendung eines Fensters, mit der die Nutzererfahrung beeinträchtigt wird,
- c) dass das Verfahren zur Beendigung eines Dienstes schwieriger als das Verfahren zur Anmeldung bei diesem Dienst gestaltet wird.

Artikel 26 Werbung auf Online-Plattformen

(1) Die Anbieter von Online-Plattformen, die Werbung auf ihren Online-Schnittstellen darstellen, stellen sicher, dass Nutzer für jede einzelne Werbung, die jedem einzelnen Nutzer dargestellt wird, in der Lage sind, in klarer, präziser und eindeutiger Weise und in Echtzeit Folgendes zu erkennen:

- a) dass es sich bei den Informationen um Werbung handelt, einschließlich durch hervorgehobene Kennzeichnungen, die Standards gemäß Artikel 44 folgen können,
- b) die natürliche oder juristische Person, in deren Namen die Werbung angezeigt wird,
- c) die natürliche oder juristische Person, die für die Werbung bezahlt hat, wenn sich diese Person von der in Buchstabe b genannten natürlichen oder juristischen Person unterscheidet,
- d) aussagekräftige, über die Werbung direkt und leicht zugängliche Informationen über die wichtigsten Parameter zur Bestimmung der Nutzer, denen die Werbung angezeigt wird, und darüber, wie diese Parameter unter Umständen geändert werden können.

(2) Die Anbieter von Online-Plattformen bieten den Nutzern eine Funktion, mit der sie erklären können, ob der von ihnen bereitgestellte Inhalt eine kommerzielle Kommunikation darstellt oder eine solche kommerzielle Kommunikation enthält.

Gibt ein Nutzer eine Erklärung gemäß diesem Absatz ab, so stellt der Anbieter der Online-Plattform sicher, dass die anderen Nutzer klar und eindeutig und in Echtzeit, einschließlich durch hervorgehobene Kennzeichnungen, die Standards gemäß Artikel 44 folgen können, feststellen können, dass der von dem Nutzer bereitgestellte Inhalt eine kommerzielle Kommunikation wie in dieser Erklärung beschrieben darstellt oder enthält.

(3) Die Anbieter von Online-Plattformen dürfen Nutzern keine Werbung anzeigen, die auf Profiling gemäß Artikel 4 Nummer 4 der Verordnung (EU) 2016/679 unter Verwendung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 beruht.

Artikel 27 Transparenz der Empfehlungssysteme

(1) Anbieter von Online-Plattformen, die Empfehlungssysteme verwenden, müssen in ihren allgemeinen Geschäftsbedingungen in klarer und verständlicher Sprache die wichtigsten Parameter, die in ihren Empfehlungssystemen verwendet werden, sowie alle Möglichkeiten für die Nutzer, diese wichtigen Parameter zu ändern oder zu beeinflussen, darlegen.

(2) Im Rahmen der in Absatz 1 genannten wichtigen Parameter wird erläutert, warum dem Nutzer bestimmte Informationen vorgeschlagen werden. Sie umfassen mindestens Folgendes:

a) die Kriterien, die für die Bestimmung der Informationen, die dem Nutzer vorgeschlagen werden, am wichtigsten sind,

b) die Gründe für die relative Bedeutung dieser Parameter.

(3) Stehen mehrere Optionen gemäß Absatz 1 für Empfehlungssysteme zur Verfügung, anhand deren die relative Reihenfolge der den Nutzern bereitgestellten Informationen bestimmt wird, so machen die Anbieter von Online-Plattformen auch eine Funktion zugänglich, die es dem Nutzer ermöglicht, seine bevorzugte Option jederzeit auszuwählen und zu ändern. Diese Funktion ist von dem spezifischen Abschnitt der Online-Schnittstelle der Online-Plattform, in dem die Informationen vorrangig sind, unmittelbar und leicht zugänglich.

Artikel 28 Online-Schutz Minderjähriger

(1) Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, müssen geeignete und verhältnismäßige Maßnahmen ergreifen, um für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu sorgen.

(2) Anbieter von Online-Plattformen dürfen auf ihrer Schnittstelle keine Werbung auf der Grundlage von Profiling gemäß Artikel 4 Absatz 4 der Verordnung (EU) 2016/679 unter Verwendung personenbezogener Daten des Nutzers darstellen, wenn sie hinreichende Gewissheit haben, dass der betreffende Nutzer minderjährig ist.

(3) Zur Einhaltung der in diesem Artikel festgelegten Verpflichtungen sind die Anbieter von Online-Plattformen nicht verpflichtet, zusätzliche personenbezogene Daten zu verarbeiten, um festzustellen, ob der Nutzer minderjährig ist.

(4) Die Kommission kann nach Anhörung des Ausschusses Leitlinien herausgeben, um die Anbieter von Online-Plattformen bei der Anwendung von Absatz 1 zu unterstützen.

ABSCHNITT 4 Bestimmungen für Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen

Artikel 29 Ausnahme für Kleinst- und Kleinunternehmen

(1) Der vorliegende Abschnitt gilt nicht für Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, bei denen es sich um Kleinst- oder Kleinunternehmen gemäß der Empfehlung 2003/361/EG handelt.

Wenn Unternehmen den Status eines Kleinst- oder Kleinunternehmens gemäß der Empfehlung 2003/361/EG verlieren, findet der vorliegende Abschnitt auch in den 12 Monaten nach dem Verlust dieses Status gemäß Artikel 4 Absatz 2 der Empfehlung keine Anwendung auf Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, es sei denn, sie sind sehr große Online-Plattformen im Sinne des Artikels 33.

(2) Abweichend von Absatz 1 findet der vorliegende Abschnitt Anwendung auf Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, die im Sinne des Artikels 33 als sehr große Online-Plattformen eingestuft wurden, unabhängig davon, ob sie als Kleinst- oder Kleinunternehmen gelten.

Artikel 30 Nachverfolgbarkeit von Unternehmern

(1) Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, stellen sicher, dass Unternehmer diese Online-Plattformen nur dann benutzen können, um bei Verbrauchern in der Union für ihre Produkte oder Dienstleistungen zu werben und ihnen diese

anzubieten, wenn sie vor der Benutzung ihrer Dienste zu diesen Zwecken folgende Informationen erhalten haben, soweit dies auf den Unternehmer zutrifft:

- a) Name, Anschrift, Telefonnummer und E-Mail-Adresse des Unternehmers,
- b) Kopie des Identitätsdokuments des Unternehmers oder eine andere elektronische Identifizierung im Sinne des Artikels 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates [\(40\)](#),
- c) Angaben zum Zahlungskonto des Unternehmers,
- d) falls der Unternehmer in einem Handelsregister oder einem ähnlichen öffentlichen Register eingetragen ist, das Handelsregister, in dem er eingetragen ist, und seine Handelsregisternummer oder eine gleichwertige in diesem Register verwendete Kennung,
- e) Selbstbescheinigung des Unternehmers, in der sich dieser verpflichtet, nur Produkte oder Dienstleistungen anzubieten, die den geltenden Vorschriften des Unionsrechts entsprechen.

(2) Nach Erhalt der in Absatz 1 genannten Informationen und bevor er dem betreffenden Unternehmer die Nutzung seiner Dienste gestattet, bemüht sich der Anbieter der Online-Plattform, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, nach besten Kräften darum, zu prüfen, ob die in Absatz 1 Buchstaben a bis e genannten Informationen verlässlich und vollständig sind, indem er frei zugängliche amtliche Online-Datenbanken abfragt oder Online-Schnittstellen nutzt, die von einem Mitgliedstaat oder der Union zur Verfügung gestellt werden, oder indem er vom Unternehmer Nachweise aus verlässlichen Quellen verlangt. Für die Zwecke dieser Verordnung haften die Unternehmer für die Richtigkeit der übermittelten Informationen.

In Bezug auf Unternehmer, die bereits die Dienste von Anbietern von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, für die in Absatz 1 genannten Zwecke am 17. Februar 2024 nutzen, bemühen sich die Anbieter nach besten Kräften darum, von diesen Unternehmern innerhalb von 12 Monaten die in der Liste aufgeführten Informationen zu erhalten. Übermitteln diese Unternehmer die Informationen nicht innerhalb dieser Frist, so setzen die Anbieter die Erbringung ihrer Dienstleistungen für diese Unternehmer aus, bis sie alle Informationen zur Verfügung gestellt haben.

(3) Erhält der Anbieter der Online-Plattform, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, ausreichend Hinweise darauf oder hat er Grund zu der Annahme, dass eine in Absatz 1 genannte Einzelinformation, die er vom betreffenden Unternehmer erhalten hat, unrichtig, unvollständig oder nicht auf dem aktuellen Stand ist, fordert der Anbieter den Unternehmer auf, unverzüglich oder innerhalb der im Unionsrecht und im nationalen Recht festgelegten Frist Abhilfe zu schaffen.

Versäumt es der Unternehmer, diese Informationen zu berichtigen oder zu vervollständigen, so setzt der Anbieter der Online-Plattform, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, seine Dienste in Bezug auf das Angebot von Produkten oder Dienstleistungen für Verbraucher in der Union für den Unternehmer zügig aus, bis dieser der Aufforderung vollständig nachgekommen ist.

(4) Unbeschadet des Artikels 4 der Verordnung (EU) 2019/1150 hat ein Unternehmen, wenn ihm ein Anbieter einer Online-Plattform, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, die Nutzung seines Dienstes gemäß Absatz 1 verweigert oder die Bereitstellung seines Dienstes gemäß Absatz 3 des vorliegenden Artikels aussetzt, das Recht, eine Beschwerde gemäß den Artikeln 20 und 21 der vorliegenden Verordnung einzureichen.

(5) Der Anbieter der Online-Plattform, der Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, speichert die nach den Absätzen 1 und 2 erhaltenen Informationen für die Dauer von sechs Monaten nach Beendigung des Vertragsverhältnisses mit dem betreffenden Unternehmer in sicherer Weise. Anschließend löscht er die Informationen.

(6) Unbeschadet des Absatzes 2 dieses Artikels gibt der Anbieter der Online-Plattform, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, die Informationen nur dann an Dritte weiter, wenn sie nach geltendem Recht, einschließlich der in Artikel 10 genannten Anordnungen und der Anordnungen, die von den zuständigen Behörden der Mitgliedstaaten oder der Kommission zur Erfüllung ihrer Aufgaben gemäß dieser Verordnung erlassen werden, dazu verpflichtet sind.

(7) Der Anbieter der Online-Plattform, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, stellt den Nutzern die in Absatz 1 Buchstaben a, d und e genannten Informationen in klarer, leicht zugänglicher und verständlicher Weise auf seiner Online-Plattform zur Verfügung. Diese Informationen müssen zumindest auf der Online-Schnittstelle der Online-Plattform verfügbar sein, auf der die Informationen über das Produkt oder den Dienst bereitgestellt werden.

Artikel 31 Konformität durch Technikgestaltung

(1) Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, stellen sicher, dass ihre Online-Schnittstelle so konzipiert und organisiert ist, dass die Unternehmer ihren Verpflichtungen in Bezug auf vorvertragliche Informationen, Konformität und Produktsicherheitsinformationen nach geltendem Unionsrecht nachkommen können.

Insbesondere gewährleistet der Anbieter, dass seine Online-Schnittstelle es den Unternehmern ermöglicht, Informationen zu Namen, Adresse, Telefonnummer und E-Mail-Adresse des Wirtschaftsakteurs im Sinne von Artikel 3 Nummer 13 der Verordnung (EU) 2019/1020 und anderen Rechtsvorschriften der Union bereitzustellen.

(2) Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmen ermöglichen, stellen sicher, dass ihre Online-Schnittstelle so konzipiert und organisiert ist, dass Unternehmer zumindest Folgendes bereitstellen können:

- a) die Informationen, die für eine klare und eindeutige Identifizierung der Produkte oder Dienstleistungen erforderlich sind, die den Verbrauchern in der Union über die Dienste der Anbieter beworben oder angeboten werden,
- b) ein Zeichen zur Identifizierung des Unternehmers, etwa die Marke, das Symbol oder das Logo, und,
- c) falls vorgeschrieben, die Informationen in Bezug auf die Etikettierung und Kennzeichnung im Einklang mit den Vorschriften des geltenden Unionsrechts über Produktsicherheit und Produktkonformität.

(3) Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, bemühen sich nach besten Kräften darum, zu bewerten, ob solche Unternehmer die in den Absätzen 1 und 2 genannten Informationen bereitgestellt haben, bevor sie diesen gestatten, ihre Produkte oder Dienstleistungen auf diesen Plattformen anzubieten. Nachdem er dem Unternehmer gestattet hat, Produkte oder Dienstleistungen auf seiner Online-Plattform anzubieten, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, bemüht sich der Anbieter, in angemessener Weise darum, stichprobenartig in einer amtlichen, frei zugänglichen und maschinenlesbaren Online-Datenbank oder Online-Schnittstelle zu prüfen, ob die angebotenen Produkte oder Dienstleistungen als rechtswidrig eingestuft wurden.

Artikel 32 Recht auf Information

(1) Erhält ein Anbieter einer Online-Plattform, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglicht, unabhängig von den verwendeten Mitteln Kenntnis, dass ein rechtswidriges Produkt oder eine rechtswidrige Dienstleistung von einem Unternehmer über seine Dienste Verbrauchern in der Union angeboten wurde, so informiert er – sofern ihm deren Kontaktdaten vorliegen – die Verbraucher, die das rechtswidrige Produkt oder die rechtswidrige Dienstleistung über seine Dienste erworben haben über Folgendes:

- a) die Tatsache, dass das Produkt oder die Dienstleistung rechtswidrig ist
- b) die Identität des Unternehmers und
- c) die einschlägigen Rechtsbehelfe.

Die Pflicht nach Unterabsatz 1 gilt nur für den Erwerb von rechtswidrigen Produkten oder Dienstleistungen in den vergangenen sechs Monaten ab dem Zeitpunkt, zu dem der Anbieter von der Rechtswidrigkeit Kenntnis erlangt hat.

(2) Verfügt der Anbieter der Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, in der in Absatz 1 genannten Situation nicht über die Kontaktdaten aller

betroffenen Verbraucher, so macht dieser Anbieter die Informationen über das rechtswidrige Produkt oder die rechtswidrige Dienstleistung, die Identität des Unternehmers und die einschlägigen Rechtsbehelfe auf seiner Online-Schnittstelle öffentlich und leicht zugänglich.

ABSCHNITT 5 Zusätzliche Verpflichtungen in Bezug auf den Umgang mit systemischen Risiken für Anbieter von sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen

Artikel 33 Sehr große Online-Plattformen und sehr große Online-Suchmaschinen

(1) Dieser Abschnitt gilt für Online-Plattformen und Online-Suchmaschinen, die eine durchschnittliche monatliche Zahl von mindestens 45 Millionen aktiven Nutzern in der Union haben und die gemäß Absatz 4 als sehr große Online-Plattformen oder sehr große Online-Suchmaschinen benannt sind.

(2) Die Kommission erlässt delegierte Rechtsakte gemäß Artikel 87, um die in Absatz 1 genannte durchschnittliche monatliche Zahl der aktiven Nutzer in der Union anzupassen, falls die Bevölkerung der Union gegenüber ihrer Bevölkerung im Jahr 2020 oder – nach einer Anpassung durch einen delegierten Rechtsakt – gegenüber ihrer Bevölkerung in dem Jahr, in dem der letzte delegierte Rechtsakt erlassen wurde, um mindestens 5 % zu- oder abnimmt. In diesem Fall passt sie die Zahl so an, dass sie 10 % der Bevölkerung der Union in dem Jahr entspricht, in dem sie den delegierten Rechtsakt erlässt, und zwar so auf- oder abgerundet, dass die Zahl in Millionen ausgedrückt werden kann.

(3) Die Kommission kann – nach Anhörung des Gremiums – delegierte Rechtsakte gemäß Artikel 87 erlassen, um für die Zwecke von Absatz 1 des vorliegenden Artikels und von Artikel 24 Absatz 2 die Bestimmungen dieser Verordnung zu ergänzen, indem sie die Methode zur Berechnung der durchschnittlichen monatlichen Zahl der aktiven Nutzer in der Union ergänzt und sicherstellt, dass die Methode den Markt- und Technologieentwicklungen Rechnung trägt.

(4) Die Kommission erlässt nach Konsultation des Mitgliedstaats der Niederlassung oder nach Berücksichtigung der vom Koordinator für digitale Dienste am Niederlassungsort gemäß Artikel 24 Absatz 4 bereitgestellten Informationen einen Beschluss, mit dem für die Zwecke dieser Verordnung die Online-Plattform oder die Online-Suchmaschine als sehr große Online-Plattform oder sehr große Online-Suchmaschine benannt wird, deren durchschnittliche monatliche Zahl aktiver Nutzer mindestens der in Absatz 1 des vorliegenden Artikels genannten Zahl entspricht. Die Kommission fasst ihren Beschluss auf der Grundlage der vom Anbieter der Online-Plattform oder der Online-Suchmaschine gemeldeten Daten gemäß Artikel 24 Absatz 2 oder der gemäß Artikel 24 Absatz 3 verlangten Informationen oder etwaiger anderer der Kommission zur Verfügung stehender Informationen.

Kommt der Anbieter der Online-Plattform oder der Online-Suchmaschine den Bestimmungen des Artikels 24 Absatz 2 oder der Aufforderung des Koordinators für digitale Dienste am Niederlassungsort oder der Aufforderung der Kommission gemäß Artikel 24 Absatz 3 nicht nach, so hindert dies die Kommission nicht daran, diesen Anbieter gemäß diesem Absatz als Anbieter einer sehr großen Online-Plattform oder einer sehr großen Online-Suchmaschine zu benennen.

Stützt die Kommission ihren Beschluss auf andere Informationen, die ihr gemäß Unterabsatz 1 vorliegen, oder auf zusätzliche Informationen, die gemäß Artikel 24 Absatz 3 angefordert werden, so gibt sie dem betroffenen Anbieter der Online-Plattform oder der Online-Suchmaschine zehn Arbeitstage, um zu den vorläufigen Feststellungen der Kommission, dass sie die Online-Plattform oder die Online-Suchmaschine als sehr große Online-Plattform bzw. sehr große Online-Suchmaschine zu benennen beabsichtigt, Stellung zu nehmen. Die Kommission trägt den Stellungnahmen des betroffenen Anbieters gebührend Rechnung.

Nimmt der Anbieter der Online-Plattform oder der Online-Suchmaschine nicht gemäß Unterabsatz 3 Stellung, so hindert dies die Kommission nicht daran, diese Online-Plattform oder diese Online-Suchmaschine auf der Grundlage anderer ihr zur Verfügung stehender Informationen als sehr große Online-Plattform bzw. sehr große Online-Suchmaschine zu benennen.

(5) Die Kommission hebt die Benennung auf, wenn die Online-Plattform oder die Online-Suchmaschine während eines ununterbrochenen Zeitraums von einem Jahr nicht über eine durchschnittliche monatliche Zahl aktiver Nutzer verfügt, die der in Absatz 1 genannten Zahl entspricht oder darüber liegt.

(6) Die Kommission teilt dem betroffenen Anbieter der Online-Plattform oder der Online-Suchmaschine, dem Gremium und dem Koordinator für digitale Dienste am Niederlassungsort ihre Beschlüsse gemäß den Absätzen 4 und 5 unverzüglich mit.

Die Kommission sorgt dafür, dass die Liste der benannten sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen im Amtsblatt der Europäischen Union veröffentlicht wird, und hält diese Liste auf dem neuesten Stand. Nach Ablauf von vier Monaten nach der in Unterabsatz 1 genannten Mitteilung an den Anbieter finden die Pflichten dieses Abschnitts auf die betroffenen sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen Anwendung bzw. keine Anwendung mehr.

Artikel 34 Risikobewertung

(1) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen ermitteln, analysieren und bewerten sorgfältig alle systemischen Risiken in der Union, die sich aus der Konzeption oder dem Betrieb ihrer Dienste und seinen damit verbundenen Systemen, einschließlich algorithmischer Systeme, oder der Nutzung ihrer Dienste ergeben.

Sie führen die Risikobewertungen bis zu dem in Artikel 33 Absatz 6 Unterabsatz 2 genannten Anwendungsbeginn und danach mindestens einmal jährlich, in jedem Fall aber vor der Einführung von Funktionen durch, die voraussichtlich kritische Auswirkungen auf die gemäß diesem Artikel ermittelten Risiken haben. Diese Risikobewertung erfolgt spezifisch für ihre Dienste und verhältnismäßig zu den systemischen Risiken unter Berücksichtigung ihrer Schwere und Wahrscheinlichkeit und umfasst die folgenden systemischen Risiken:

- a) Verbreitung rechtswidriger Inhalte über ihre Dienste;
- b) etwaige tatsächliche oder vorhersehbare nachteilige Auswirkungen auf die Ausübung der Grundrechte, insbesondere des in Artikel 1 der Charta verankerten Grundrechts auf Achtung der Menschenwürde, des in Artikel 7 der Charta verankerten Grundrechts auf Achtung des Privat- und Familienlebens, des in Artikel 8 der Charta verankerten Grundrechts auf Schutz personenbezogener Daten, des in Artikel 11 der Charta verankerten Grundrechts auf die Meinungs- und Informationsfreiheit, einschließlich Medienfreiheit und -pluralismus auf das in Artikel 21 der Charta verankerte Grundrecht auf Nichtdiskriminierung, die in Artikel 24 der Charta verankerten Rechte des Kindes und den in Artikel 38 der Charta verankerten umfangreichen Verbraucherschutz;
- c) alle tatsächlichen oder absehbaren nachteiligen Auswirkungen auf die gesellschaftliche Debatte und auf Wahlprozesse und die öffentliche Sicherheit;
- d) alle tatsächlichen oder absehbaren nachteiligen Auswirkungen in Bezug auf geschlechtsspezifische Gewalt, den Schutz der öffentlichen Gesundheit und von Minderjährigen sowie schwerwiegende nachteilige Folgen für das körperliche und geistige Wohlbefinden einer Person.

(2) Bei der Durchführung der Risikobewertung berücksichtigen die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen insbesondere, ob und wie die folgenden Faktoren die in Absatz 1 genannten systemischen Risiken beeinflussen:

- a) die Gestaltung ihrer Empfehlungssysteme und anderer relevanter algorithmischer Systeme;
- b) ihre Systeme zur Moderation von Inhalten;
- c) die anwendbaren allgemeinen Geschäftsbedingungen und ihre Durchsetzung;
- d) Systeme zur Auswahl und Anzeige von Werbung;
- e) die datenbezogene Praxis des Anbieters.

Bei den Bewertungen wird auch analysiert, ob und wie die Risiken gemäß Absatz 1 durch vorsätzliche Manipulation ihres Dienstes, auch durch unauthentische Verwendung oder automatisierte Ausnutzung des Dienstes, sowie durch die Verstärkung und die Möglichkeit der raschen und weiten Verbreitung von rechtswidrigen Inhalten und von Informationen, die mit ihren allgemeinen Geschäftsbedingungen unvereinbar sind, beeinflusst werden.

Bei der Bewertung werden spezifische regionale oder sprachliche Aspekte auch dann berücksichtigt, wenn sie für einen Mitgliedstaat spezifisch sind.

(3) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen bewahren die entsprechenden Dokumente der Risikobewertungen mindestens drei Jahre nach Durchführung der Risikobewertungen auf und übermitteln sie der Kommission und dem Koordinator für digitale Dienste am Niederlassungsort bei Bedarf.

Artikel 35 Risikominderung

(1) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen ergreifen angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen, die auf die gemäß Artikel 34 ermittelten besonderen systemischen Risiken zugeschnitten sind, wobei die Auswirkungen solcher Maßnahmen auf die Grundrechte besonders zu berücksichtigen sind. Hierzu können unter Umständen gehören:

- a) Anpassung der Gestaltung, der Merkmale oder der Funktionsweise ihrer Dienste einschließlich ihrer Online-Schnittstellen;
- b) Anpassung der allgemeinen Geschäftsbedingungen und ihrer Durchsetzung;
- c) Anpassung der Verfahren zur Moderation von Inhalten, einschließlich der Geschwindigkeit und Qualität der Bearbeitung von Meldungen zu bestimmten Arten rechtswidriger Inhalte, und, soweit erforderlich, rasche Entfernung der gemeldeten Inhalte oder Sperrung des Zugangs dazu, insbesondere in Bezug auf rechtswidrige Hetze oder Cybergewalt; sowie Anpassung aller einschlägigen Entscheidungsprozesse und der für die Moderation von Inhalten eingesetzten Mittel;
- d) Erprobung und Anpassung ihrer algorithmischen Systeme, einschließlich ihrer Empfehlungssysteme;
- e) Anpassung ihrer Werbesysteme und Annahme von gezielten Maßnahmen zur Beschränkung oder Anpassung der Anzeige von Werbung in Verbindung mit dem von ihnen erbrachten Dienst;
- f) Stärkung der internen Prozesse, der Ressourcen, der Prüfung, der Dokumentation oder der Beaufsichtigung ihrer Tätigkeiten, insbesondere im Hinblick auf die Erkennung systemischer Risiken;
- g) Beginn oder Anpassung der Zusammenarbeit mit vertrauenswürdigen Hinweisgebern gemäß Artikel 22 und der Umsetzung der Entscheidungen von außergerichtlichen Streitbelegungsstellen gemäß Artikel 21;
- h) Beginn oder Anpassung der Zusammenarbeit mit anderen Anbietern von Online-Plattformen oder Online-Suchmaschinen anhand der in Artikel 45 und Artikel 48 genannten Verhaltenskodizes bzw. Krisenprotokolle;
- i) Sensibilisierungsmaßnahmen und Anpassung ihrer Online-um Nutzern mehr Informationen zu geben;
- j) gezielte Maßnahmen zum Schutz der Rechte des Kindes, darunter auch Werkzeuge zur Altersüberprüfung und zur elterlichen Kontrolle sowie Werkzeuge, die es Minderjährigen ermöglichen sollen, Missbrauch zu melden bzw. Unterstützung zu erhalten;
- k) Sicherstellung, dass eine Einzelinformation, unabhängig davon, ob es sich um einen erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt handelt, der bestehenden Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen merklich ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheint, durch eine auffällige Kennzeichnung erkennbar ist, wenn sie auf ihren Online-Schnittstellen angezeigt wird, und darüber hinaus Bereitstellung einer benutzerfreundlichen Funktion, die es den Nutzern des Dienstes ermöglicht, solche Informationen anzuzeigen.

(2) Das Gremium veröffentlicht in Zusammenarbeit mit der Kommission einmal jährlich einen umfassenden Bericht. Der Bericht enthält folgende Informationen:

- a) Ermittlung und Bewertung der auffälligsten wiederkehrenden systemischen Risiken, die von Anbietern sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen gemeldet oder über andere Informationsquellen, insbesondere aus den gemäß den Artikeln 39, 40 und 42 bereitgestellten Informationen, ermittelt wurden;

b) bewährte Verfahren für Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen zur Minderung der ermittelten systemischen Risiken.

Dieser Bericht enthält Angaben über systemische Risiken, aufgeschlüsselt nach den Mitgliedstaaten, in denen sie gegebenenfalls auftraten, und – falls zweckmäßig – in der Union als Ganzes.

(3) Die Kommission kann in Zusammenarbeit mit den Koordinatoren für digitale Dienste Leitlinien für die Anwendung des Absatzes 1 in Bezug auf besondere Risiken herausgeben, um insbesondere bewährte Verfahren vorzustellen und mögliche Maßnahmen zu empfehlen, wobei sie die möglichen Auswirkungen der Maßnahmen auf die in der Charta verankerten Grundrechte aller Beteiligten gebührend berücksichtigt. Im Hinblick auf die Ausarbeitung dieser Leitlinien führt die Kommission öffentliche Konsultationen durch.

Artikel 36 Krisenreaktionsmechanismus

(1) Im Krisenfall kann die Kommission auf Empfehlung des Gremiums einen Beschluss erlassen, in dem ein oder mehrere Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen aufgefordert werden, eine oder mehrere der folgenden Maßnahmen zu ergreifen:

- a) eine Bewertung, ob und, wenn ja, in welchem Umfang und wie der Betrieb und die Nutzung ihrer Dienste erheblich zu einer schwerwiegenden Bedrohung im Sinne von Absatz 2 beitragen oder voraussichtlich beitragen werden;
- b) die Ermittlung und Anwendung von gezielten, wirksamen und verhältnismäßigen Maßnahmen, etwa Maßnahmen gemäß Artikel 35 Absatz 1 oder Artikel 48 Absatz 2, um einen solchen Beitrag zu der gemäß Buchstabe a ermittelten schwerwiegenden Bedrohung zu verhindern, zu beseitigen oder zu begrenzen;
- c) Berichterstattung an die Kommission bis zu einem bestimmten im Beschluss festgelegten Zeitpunkt oder in regelmäßigen Abständen über die unter Buchstabe a genannten Bewertungen, über den genauen Inhalt, die Durchführung und die qualitativen und quantitativen Auswirkungen der gemäß Buchstabe b ergriffenen gezielten Maßnahmen sowie über alle anderen Fragen im Zusammenhang mit diesen Bewertungen oder Maßnahmen, wie in dem Beschluss festgelegt;

Bei der Ermittlung und Anwendung von Maßnahmen gemäß Buchstabe b berücksichtigt bzw. berücksichtigen der bzw. die Diensteanbieter gebührend die Schwere der in Absatz 2 genannten schwerwiegenden Bedrohung, die Dringlichkeit der Maßnahmen und die tatsächlichen oder potenziellen Auswirkungen auf die Rechte und berechtigten Interessen aller betroffenen Parteien, einschließlich des möglichen Versäumnisses, bei den Maßnahmen die in der Charta verankerten Grundrechte zu achten.

(2) Für die Zwecke dieses Artikels gilt eine Krise als eingetreten, wenn außergewöhnliche Umstände eintreten, die zu einer schwerwiegenden Bedrohung der öffentlichen Sicherheit oder der öffentlichen Gesundheit in der Union oder in wesentlichen Teilen der Union führen können.

(3) Bei der Beschlussfassung nach Absatz 1 stellt die Kommission sicher, dass alle folgenden Anforderungen erfüllt sind:

- a) die in dem Beschluss geforderten Maßnahmen sind unbedingt erforderlich, gerechtfertigt und verhältnismäßig, insbesondere in Bezug auf die Schwere der in Absatz 2 genannten schwerwiegenden Bedrohung, die Dringlichkeit der Maßnahmen und die tatsächlichen oder potenziellen Auswirkungen auf die Rechte und berechtigten Interessen aller betroffenen Parteien, einschließlich des möglichen Versäumnisses, bei den Maßnahmen die in der Charta verankerten Grundrechte zu achten;
- b) in dem Beschluss wird eine angemessene Frist festgelegt, innerhalb deren die in Absatz 1 Buchstabe b genannten gezielten Maßnahmen zu treffen sind, wobei insbesondere der Dringlichkeit dieser Maßnahmen und der für ihre Vorbereitung und Durchführung erforderlichen Zeit Rechnung zu tragen ist;
- c) die in dem Beschluss geforderten Maßnahmen sind auf eine Dauer von höchstens drei Monaten begrenzt.

(4) Nach der Annahme des Beschlusses nach Absatz 1 ergreift die Kommission unverzüglich folgende Maßnahmen:

- a) sie teilt den Beschluss dem Anbieter bzw. den Anbietern mit, an den bzw. die der Beschluss gerichtet ist;

b) sie macht den Beschluss öffentlich zugänglich; und

c) sie setzt das Gremium von dem Beschluss in Kenntnis, fordert es auf, dazu Stellung zu nehmen, und hält es über alle weiteren Entwicklungen im Zusammenhang mit dem Beschluss auf dem Laufenden.

(5) Die Wahl der gemäß Absatz 1 Buchstabe b und Absatz 7 Unterabsatz 2 zu treffenden gezielten Maßnahmen verbleibt bei dem Anbieter bzw. den Anbietern, an den bzw. die sich der Beschluss der Kommission richtet.

(6) Die Kommission kann von sich aus oder auf Ersuchen des Anbieters mit dem Anbieter in einen Dialog treten, um festzustellen, ob die in Absatz 1 Buchstabe b genannten geplanten oder durchgeführten Maßnahmen angesichts der besonderen Umstände des Anbieters wirksam und verhältnismäßig sind, um die verfolgten Ziele zu erreichen. Insbesondere stellt die Kommission sicher, dass die vom Diensteanbieter gemäß Absatz 1 Buchstabe b ergriffenen Maßnahmen den in Absatz 3 Buchstaben a und c genannten Anforderungen entsprechen.

(7) Die Kommission überwacht die Anwendung der gezielten Maßnahmen, die gemäß dem in Absatz 1 genannten Beschluss getroffen wurden, auf der Grundlage der in Absatz 1 Buchstabe c genannten Berichte und aller sonstigen einschlägigen Informationen, einschließlich der Informationen, die sie gemäß Artikel 40 oder 67 anfordern kann, wobei sie der Entwicklung der Krise Rechnung trägt. Die Kommission erstattet dem Gremium regelmäßig, mindestens jedoch monatlich, über diese Überwachung Bericht.

Ist die Kommission der Auffassung, dass die geplanten oder durchgeführten gezielten Maßnahmen gemäß Absatz 1 Buchstabe b nicht wirksam oder verhältnismäßig sind, so kann sie den Anbieter durch Erlass eines Beschlusses nach Anhörung des Gremiums auffordern, die Ermittlung oder Anwendung dieser gezielten Maßnahmen zu überprüfen.

(8) Wenn dies angesichts der Entwicklung der Krise angemessen ist, kann die Kommission auf Empfehlung des Gremiums den in Absatz 1 oder Absatz 7 Unterabsatz 2 genannten Beschluss ändern, indem sie

a) den Widerruf des Beschlusses und – falls angezeigt – die Aufforderung an die sehr große Online-Plattform oder sehr große Online-Suchmaschine, die gemäß Absatz 1 Buchstabe b oder Absatz 7 Unterabsatz 2 ermittelten und umgesetzten Maßnahmen nicht mehr anwendet, insbesondere wenn die Gründe für solche Maßnahmen nicht mehr vorliegen;

b) den in Absatz 3 Buchstabe c genannten Zeitraum um höchstens drei Monate verlängert;

c) die bei der Anwendung der Maßnahmen gesammelten Erfahrungen, insbesondere das mögliche Versäumnis, bei den Maßnahmen die in der Charta verankerten Grundrechte zu achten, berücksichtigt.

(9) Die Anforderungen der Absätze 1 bis 6 gelten für den in diesem Artikel genannten Beschluss und dessen Änderung.

(10) Die Kommission trägt etwaigen Stellungnahmen des Gremiums gemäß den Empfehlungen in diesem Artikel weitestgehend Rechnung.

(11) Die Kommission erstattet dem Europäischen Parlament und dem Rat nach der Annahme von Beschlüssen gemäß diesem Artikel jährlich, in jedem Fall jedoch drei Monate nach dem Ende der Krise, über die Anwendung der aufgrund dieser Beschlüsse getroffenen spezifischen Maßnahmen Bericht.

Artikel 37 Unabhängige Prüfung

(1) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen werden mindestens einmal jährlich auf eigene Kosten einer unabhängigen Prüfung unterzogen, bei der die Einhaltung folgender Pflichten und Verpflichtungszusagen bewertet wird:

a) die in Kapitel III festgelegten Pflichten,

b) die Verpflichtungszusagen, die gemäß den in den Artikeln 45 und 46 genannten Verhaltenskodizes und den in Artikel 48 genannten Krisenprotokollen gemacht wurden.

(2) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen leisten den Organisationen, die die Prüfungen gemäß diesem Artikel durchführen, die erforderliche Unterstützung und

arbeiten mit ihnen zusammen, damit sie diese Prüfungen wirksam, effizient und rechtzeitig durchführen können, unter anderem indem sie ihnen Zugang zu allen relevanten Daten und Räumlichkeiten gewähren und mündliche oder schriftliche Fragen beantworten. Sie dürfen die Durchführung der Prüfung nicht behindern, übermäßig beeinflussen oder untergraben.

Diese Prüfungen sorgen in Bezug auf die Informationen, die sie von den Anbietern sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen und Dritten im Rahmen der Prüfungen, auch nach Abschluss der Prüfungen, erhalten, für ein angemessenes Maß an Vertraulichkeit und die Einhaltung der Geheimhaltungspflicht. Die Einhaltung dieser Anforderung darf sich jedoch nicht nachteilig auf die Durchführung der Prüfungen und anderer Bestimmungen dieser Verordnung, insbesondere der Bestimmungen über Transparenz, Überwachung und Durchsetzung, auswirken. Soweit es für die Zwecke der Transparenzberichtspflichten gemäß Artikel 42 Absatz 4 erforderlich ist, sind dem Bericht über die Durchführung der Prüfung gemäß den Absätzen 4 und 6 dieses Artikels Fassungen des Prüfberichts beizufügen, die keine Informationen enthalten, die nach angemessenem Ermessen als vertraulich angesehen werden könnten.

(3) Die Prüfungen gemäß Absatz 1 werden von Stellen durchgeführt, die

a) von dem Anbieter der betreffenden sehr großen Online-Plattform oder sehr großen Online-Suchmaschine und jeder juristischen Person, die mit diesem Anbieter in Verbindung steht, unabhängig sind und sich in keinen Interessenkonflikten mit diesen befinden; insbesondere

i) in den 12 Monaten vor Beginn der Prüfung keine prüfungsfremden Leistungen im Zusammenhang mit den geprüften Sachverhalten für den Anbieter der betreffenden sehr großen Online-Plattform oder sehr großen Online-Suchmaschine und für mit diesem in Verbindung stehende juristische Personen erbracht haben und sich verpflichtet haben, ihnen diese Dienstleistungen in den 12 Monaten nach Abschluss der Prüfung nicht zu erbringen,

ii) für den betreffenden Anbieter einer sehr großen Online-Plattform oder sehr großen Online-Suchmaschine und für mit ihm in Verbindung stehende juristische Personen während eines Zeitraums von mehr als zehn aufeinanderfolgenden Jahren keine Prüfungsleistungen gemäß diesem Artikel erbracht haben,

iii) die Prüfung nicht gegen Honorare durchführen, die vom Ergebnis der Prüfung abhängen;

b) nachgewiesene Sachkenntnis auf dem Gebiet des Risikomanagements sowie technische Kompetenzen und Kapazitäten haben,

c) nachweislich mit Objektivität und gemäß der Berufsethik arbeiten, insbesondere aufgrund der Einhaltung von Verhaltenskodizes oder der einschlägigen Normen.

(4) Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen stellen sicher, dass die Stellen, die die Prüfungen durchführen, für jede Prüfung einen Prüfbericht anfertigen. Dieser Bericht enthält eine schriftliche Begründung sowie mindestens Folgendes:

a) Name, Anschrift und Kontaktstelle des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine, der geprüft wird, und Zeitraum, auf den sich die Prüfung bezieht,

b) Name und Anschrift der Stelle bzw. der Stellen, die die Prüfung durchführt bzw. durchführen,

c) Interessenerklärung,

d) Beschreibung der konkret geprüften Elemente und der angewandten Methode,

e) Beschreibung und Zusammenfassung der wichtigsten Erkenntnisse aus der Prüfung,

f) Auflistung der Dritten, die im Rahmen der Prüfung konsultiert wurden,

g) Stellungnahme der Prüfer dazu, ob der geprüfte Anbieter der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine den in Absatz 1 genannten Pflichten und Verpflichtungszusagen nachgekommen ist, und zwar entweder „positiv“, „positiv mit Anmerkungen“ oder „negativ“,

h) falls die Stellungnahme nicht „positiv“ ist, operative Empfehlungen für besondere Maßnahmen im Hinblick auf die Einhaltung aller Pflichten und Verpflichtungszusagen und den empfohlenen Zeitrahmen dafür.

(5) War die Stelle, die die Prüfung durchgeführt hat, nicht in der Lage, bestimmte Elemente zu prüfen oder auf der Grundlage ihrer Untersuchungen eine Stellungnahme abzugeben, so muss der Prüfbericht eine Erläuterung der Umstände und der Gründe enthalten, aus denen diese Elemente nicht geprüft werden konnten.

(6) Die Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen, die keinen „positiven“ Prüfbericht erhalten, tragen die an sie gerichteten operativen Empfehlungen gebührend Rechnung und ergreifen die erforderlichen Maßnahmen zu deren Umsetzung. Sie nehmen innerhalb eines Monats nach Erhalt dieser Empfehlungen einen Bericht über die Umsetzung der Prüfergebnisse an, in dem sie diese Maßnahmen darlegen. Falls sie die operativen Empfehlungen nicht umsetzen, begründen sie dies in dem Bericht und legen die alternativen Maßnahmen dar, die sie ergriffen haben, um festgestellte Verstöße zu beheben.

(7) Der Kommission ist dazu befugt, gemäß Artikel 87 delegierte Rechtsakte zu erlassen, um diese Verordnung durch Festlegung der erforderlichen Vorschriften für die Durchführung der Prüfungen gemäß diesem Artikel zu ergänzen, insbesondere in Bezug auf die erforderlichen Vorschriften über die Verfahrensschritte, die Prüfungsmethoden und die Berichtsvorlagen für die gemäß diesem Artikel durchgeführten Prüfungen. In den delegierten Rechtsakten wird etwaigen freiwilligen Prüfungsnormen gemäß Artikel 44 Absatz 1 Buchstabe e Rechnung getragen.

Artikel 38 Empfehlungssysteme

Zusätzlich zu den in Artikel 27 festgelegten Anforderungen legen die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen, die Empfehlungssysteme verwenden, mindestens eine Option für jedes ihrer Empfehlungssysteme vor, die nicht auf Profiling gemäß Artikel 4 Absatz 4 der Verordnung (EU) 2016/679 beruht.

Artikel 39 Zusätzliche Transparenz der Online-Werbung

(1) Die Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen, die Werbung auf ihren Online-Schnittstellen anzeigen, stellen die in Absatz 2 genannten Angaben in einem spezifischen Bereich ihrer Online-Schnittstelle zusammen und machen diese über Anwendungsprogrammierschnittstellen für den gesamten Zeitraum, in dem sie eine Werbung anzeigen, und ein Jahr lang nach der letzten Anzeige der Werbung auf ihren Online-Schnittstellen mithilfe eines durchsuchbaren und verlässlichen Werkzeugs, das mit mehreren Kriterien abgefragt werden kann, öffentlich zugänglich. Sie stellen sicher, dass das Archiv keine personenbezogenen Daten der Nutzer enthält, denen die Werbung angezeigt wurde oder hätte angezeigt werden können, und angemessene Bemühungen unternehmen, um sicherzustellen, dass die Informationen präzise und vollständig sind.

(2) Das Archiv enthält zumindest alle folgenden Angaben:

- a) den Inhalt der Werbung, einschließlich des Namens des Produkts, der Dienstleistung oder der Marke und des Gegenstands der Werbung;
- b) die natürliche oder juristische Person, in deren Namen die Werbung angezeigt wird;
- c) die natürliche oder juristische Person, die für die Werbung bezahlt hat, wenn sich diese Person von der in Buchstabe b genannten Person unterscheidet,
- d) den Zeitraum, in dem die Werbung angezeigt wurde;
- e) ob die Werbung gezielt einer oder mehreren bestimmten Gruppen von Nutzern angezeigt werden sollte, und falls ja, welche Hauptparameter zu diesem Zweck verwendet wurden, einschließlich der wichtigsten Parameter, die gegebenenfalls zum Ausschluss einer oder mehrerer solcher bestimmter Gruppen verwendet werden;
- f) die auf den sehr großen Online-Plattformen gemäß Artikel 26 Absatz 2 veröffentlichte und ermittelte kommerzielle Kommunikation;

g) die Gesamtzahl der erreichten Nutzer und gegebenenfalls aggregierte Zahlen aufgeschlüsselt nach Mitgliedstaat für die Gruppe oder Gruppen von Nutzern, an die die Werbung gezielt gerichtet war.

(3) In Bezug auf Absatz 2 Buchstaben a, b und c darf das Archiv die in diesen Buchstaben genannten Informationen nicht enthalten, wenn ein Anbieter einer sehr großen Online-Plattform oder sehr großen Online-Suchmaschine den Zugang zu einer bestimmten Werbung aufgrund mutmaßlicher Rechtswidrigkeit oder Unvereinbarkeit mit seinen allgemeinen Geschäftsbedingungen entfernt oder gesperrt hat. In diesem Fall enthält das Archiv für die in Rede stehende Werbung die Informationen gemäß Artikel 17 Absatz 3 Buchstaben a bis e bzw. Artikel 9 Absatz 2 Buchstabe a Ziffer i.

Die Kommission kann nach Konsultation des Gremiums, der einschlägigen zugelassenen Forscher gemäß Artikel 40 und der Öffentlichkeit Leitlinien zur Struktur, Organisation und Funktionsweise der in diesem Artikel genannten Archive herausgeben.

Artikel 40 Datenzugang und Kontrolle

(1) Die Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen gewähren dem Koordinator für digitale Dienste am Niederlassungsort oder der Kommission auf deren begründetes Verlangen innerhalb einer darin genannten angemessenen Frist Zugang zu den Daten, die für die Überwachung und Bewertung der Einhaltung dieser Verordnung erforderlich sind.

(2) Die Koordinatoren für digitale Dienste und die Kommission verwenden die Daten, auf die gemäß Absatz 1 zugegriffen wurde, ausschließlich zur Überwachung und Bewertung der Einhaltung dieser Verordnung, und sie berücksichtigen dabei gebührend die Rechte und Interessen der betroffenen Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen und Nutzer, einschließlich des Schutzes personenbezogener Daten, des Schutzes vertraulicher Informationen, insbesondere von Geschäftsgeheimnissen, und der Aufrechterhaltung der Sicherheit ihres Dienstes.

(3) Für die Zwecke des Absatzes 1 erläutern die Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen auf Verlangen des Koordinators für digitale Dienste am Niederlassungsort oder der Kommission die Gestaltung, die Logik, die Funktionsweise und die Tests ihrer algorithmischen Systeme einschließlich ihrer Empfehlungssysteme.

(4) Die Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen gewähren auf begründetes Verlangen des Koordinators für digitale Dienste am Niederlassungsort innerhalb einer darin genannten angemessenen Frist zugelassenen Forschern, die die Anforderungen in Absatz 8 dieses Artikels erfüllen, Zugang zu Daten zum ausschließlichen Zweck der Durchführung von Forschungsarbeiten, die zur Aufspürung, zur Ermittlung und zum Verständnis systemischer Risiken in der Union gemäß Artikel 34 Absatz 1 beitragen, auch in Bezug auf die Bewertung der Angemessenheit, der Wirksamkeit und der Auswirkungen der Risikominderungsmaßnahmen gemäß Artikel 35.

(5) Innerhalb von 15 Tagen nach Eingang eines Verlangens gemäß Absatz 4 können Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen den Koordinator für digitale Dienste am Niederlassungsort ersuchen, das Verlangen zu ändern, wenn sie sich aus einem der beiden folgenden Gründe außerstande sehen, Zugang zu den angeforderten Daten zu gewähren:

a) sie haben keinen Zugriff auf die Daten;

b) die Gewährung des Zugangs zu den Daten führt zu erheblichen Schwachstellen bei der Sicherheit ihres Dienstes oder beim Schutz vertraulicher Informationen, insbesondere von Geschäftsgeheimnissen.

(6) Änderungsanträge nach Absatz 5 müssen Vorschläge für eine oder mehrere Alternativen enthalten, wie der Zugang zu den angeforderten Daten oder zu anderen Daten gewährt werden kann, die für die Zwecke des Verlangens angemessen und ausreichend sind.

Der Koordinator für digitale Dienste am Niederlassungsort entscheidet innerhalb von 15 Tagen über den Änderungsantrag und teilt dem Anbieter der sehr großen Online-Plattformen oder sehr großen Online-Suchmaschine den betreffenden Beschluss sowie das gegebenenfalls geänderte Verlangen mit der neuen Frist für dessen Erfüllung mit.

(7) Die Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen erleichtern und gewähren den Zugang zu Daten gemäß den Absätzen 1 und 4 über geeignete Schnittstellen, die in dem Verlangen angegeben sind, einschließlich Online-Datenbanken oder Anwendungsprogrammierschnittstellen.

(8) Auf hinreichend begründeten Antrag von Forschern erkennt der Koordinator für digitale Dienste am Niederlassungsort solchen Forschern für spezifische im Antrage genannte Forschungsarbeiten den Status von ‚zugelassenen Forschern‘ zu und reicht bei einem Anbieter einer sehr großen Online-Plattform oder sehr großen Online-Suchmaschine ein begründetes Verlangen auf Datenzugang gemäß Absatz 4 ein, sofern die Forscher nachweisen, dass sie alle folgenden Bedingungen erfüllen:

- a) sie sind einer Forschungseinrichtung im Sinne von Artikel 2 Nummer 1 der Richtlinie (EU) 2019/790 angeschlossen;
- b) sie sind unabhängig von kommerziellen Interessen;
- c) ihr Antrag gibt Aufschluss über die Finanzierung der Forschung;
- d) sie sind in der Lage, die mit jedem Verlangen verbundenen besonderen Anforderungen an die Datensicherheit und die Vertraulichkeit einzuhalten und personenbezogene Daten zu schützen, und sie beschreiben in ihrem Verlangen die angemessenen technischen und organisatorischen Maßnahmen, die sie hierzu getroffen haben;
- e) in ihrem Antrag wird nachgewiesen, dass der Zugang zu den Daten und die beantragten Fristen für die Zwecke ihrer Forschungsarbeiten notwendig und verhältnismäßig sind und dass die erwarteten Ergebnisse dieser Forschung zu den in Absatz 4 genannten Zwecken beitragen werden;
- f) die geplanten Forschungstätigkeiten werden zu den in Absatz 4 genannten Zwecken durchgeführt;
- g) sie haben sich dazu verpflichtet, ihre Forschungsergebnisse innerhalb eines angemessenen Zeitraums nach Abschluss der Forschungsarbeiten und unter Berücksichtigung der Rechte und Interessen der Nutzer des betreffenden Dienstes im Einklang mit der Verordnung (EU) 2016/679 kostenlos öffentlich zugänglich zu machen.

Der Koordinator für digitale Dienste am Niederlassungsort unterrichtet die Kommission und das Gremium über den Eingang von Verlangen gemäß diesem Absatz.

(9) Forscher können ihr Verlangen auch beim Koordinator für digitale Dienste des Mitgliedstaats der Forschungsorganisation, der sie angeschlossen sind, einreichen. Nach Eingang des Verlangens gemäß diesem Absatz führt der Koordinator für digitale Dienste eine Anfangsbewertung durch, ob die jeweiligen Forscher alle in Absatz 8 genannten Bedingungen erfüllen. Der jeweilige Koordinator für digitale Dienste übermittelt anschließend das Verlangen zusammen mit den von den jeweiligen Forschern eingereichten Belegen und der Anfangsbewertung an den Koordinator für digitale Dienste am Niederlassungsort. Der Koordinator für digitale Dienste am Niederlassungsort trifft die Entscheidung, ob einem Forscher unverzüglich der Status eines „zugelassenen Forschers“ zuerkannt wird.

Während der bereitgestellten ersten Bewertung gebührend Rechnung zu tragen ist, liegt die endgültige Entscheidung über die Zuerkennung des Status eines „zugelassenen Forschers“ gemäß Absatz 8 in der Zuständigkeit des Koordinators für digitale Dienste am Niederlassungsort.

(10) Der Koordinator für digitale Dienste, der den Status eines zugelassenen Forschers zuerkennt und bei Anbietern sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen das begründete Verlangen auf Datenzugang zugunsten eines zugelassenen Forschers eingereicht hat, trifft eine Entscheidung über die Beendigung des Zugangs, wenn er nach einer Untersuchung von sich aus oder auf der Grundlage von Informationen Dritter feststellt, dass der zugelassene Forscher die in Absatz 8 genannten Bedingungen nicht mehr erfüllt, und unterrichtet den betroffenen Anbieter der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine über die Entscheidung. Vor der Beendigung des Zugangs erteilt der Koordinator für digitale Dienste dem zugelassenen Forscher die Gelegenheit, zu den Untersuchungsergebnissen und zu der Absicht, den Zugang zu beenden, Stellung zu nehmen.

(11) Die Koordinatoren für digitale Dienste am Niederlassungsort teilen dem Gremium die Namen und Kontaktangaben der natürlichen Personen oder Einrichtungen, denen sie gemäß Absatz 8 den Status eines

„zugelassenen Forschers“ zuerkannt haben, sowie den Zweck der Forschungsarbeiten, für die der Antrag gestellt wurde, mit oder sie übermitteln dem Gremium diese Informationen, wenn der Datenzugang gemäß Absatz 10 beendet wurde.

(12) Die Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen gewähren unverzüglich Zugang zu Daten, einschließlich – soweit dies technisch möglich ist – zu Daten in Echtzeit vorausgesetzt, die Daten sind Forschern, auch Forschern, die mit gemeinnützigen Einrichtungen, Organisationen und Vereinigungen verbunden sind, die die in Absatz 8 Buchstaben b, c, d und e genannten Bedingungen erfüllen und die Daten ausschließlich zu Forschungszwecken verwenden, die zur Aufdeckung, Identifizierung und zum Verständnis systemischer Risiken in der Union gemäß Artikel 34 Absatz 1 beitragen, über ihre Online-Schnittstelle öffentlich zugänglich.

(13) Die Kommission erlässt nach Anhörung des Gremiums delegierte Rechtsakte zur Ergänzung dieser Verordnung zur Festlegung der technischen Bedingungen, unter denen die Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchdienste Daten gemäß den Absätzen 1 und 4 zur Verfügung stellen müssen, und der Zwecke, für die die Daten verwendet werden dürfen. In diesen delegierten Rechtsakten werden die besonderen Bedingungen festgelegt, nach denen eine solche Datenweitergabe an Forscher im Einklang mit der Verordnung (EU) 2016/679 erfolgen darf und die einschlägigen objektiven Indikatoren sowie die Verfahren und erforderlichenfalls die unabhängigen Beratungsmechanismen zur Unterstützung der Datenweitergabe, wobei die Rechte und Interessen der Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen und der Nutzer zu berücksichtigen sind, einschließlich des Schutzes vertraulicher Informationen, insbesondere von Geschäftsgeheimnissen, und der Aufrechterhaltung der Sicherheit ihres Dienstes.

Artikel 41 Compliance-Abteilung

(1) Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen richten eine Compliance-Abteilung ein, die unabhängig von ihren operativen Abteilungen ist und aus einem oder mehreren Compliance-Beauftragten besteht, einschließlich des Leiters der Compliance-Abteilung. Diese Compliance-Abteilung verfügt über ausreichend Autorität, Befugnisse und Ressourcen sowie über Zugang zum Leitungsorgan des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine, um die Einhaltung dieser Verordnung durch den betreffenden Anbieter zu überwachen.

(2) Das Leitungsorgan des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine stellt sicher, dass die Compliance-Beauftragten über die zur Erfüllung der in Absatz 3 genannten Aufgaben erforderlichen beruflichen Qualifikationen, Kenntnisse, Erfahrungen und Fähigkeiten verfügen.

Das Leitungsorgan des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine stellt sicher, dass es sich bei dem Leiter der Compliance-Abteilung um eine unabhängige Führungskraft handelt, die eigens für die Compliance-Abteilung zuständig ist.

Der Leiter der Compliance-Abteilung untersteht direkt dem Leitungsorgan des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine und kann Bedenken äußern und dieses Organ warnen, falls in Artikel 34 genannte Risiken oder die Nichteinhaltung dieser Verordnung den Anbieter der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine betreffen oder betreffen könnten, unbeschadet der Zuständigkeiten des Leitungsorgans in seinen Aufsichts- und Leitungsfunktionen.

Der Leiter der Compliance-Abteilung darf nicht ohne vorherige Zustimmung des Leitungsorgans des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine abgelöst werden.

(3) Compliance-Beauftragte haben folgende Aufgaben:

- a) Zusammenarbeit mit dem Koordinator für digitale Dienste am Niederlassungsort und mit der Kommission für die Zwecke dieser Verordnung;
- b) Gewährleistung, dass alle in Artikel 34 genannten Risiken ermittelt und ordnungsgemäß gemeldet werden, und dass angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen gemäß Artikel 35 ergriffen werden;

- c) Organisation und Beaufsichtigung der Tätigkeiten des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine im Zusammenhang mit der unabhängigen Prüfung gemäß Artikel 37;
- d) Information und Beratung des Managements und der Mitarbeiter des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine über die einschlägigen Verpflichtungen aus dieser Verordnung;
- e) Überwachung, dass der Anbieter der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine seinen Verpflichtungen aus dieser Verordnung nachkommt;
- f) gegebenenfalls Überwachung der Einhaltung der Verpflichtungszusagen, die der Anbieter der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine im Rahmen der Verhaltenskodizes gemäß den Artikeln 45 und 46 oder der Krisenprotokolle gemäß Artikel 48 gemacht hat.

(4) Anbieter sehr großer Online-Plattform oder sehr großer Online-Suchmaschinen teilen dem Koordinator für digitale Dienste am Niederlassungsort und der Kommission die Namen und die Kontaktangaben des Leiters der Compliance-Abteilung mit.

(5) Das Leitungsorgan des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine übernimmt die Festlegung, Beaufsichtigung und Haftung der bzw. für die Umsetzung der Unternehmensführungsregelungen des Anbieters, die für die Unabhängigkeit der Compliance-Abteilung sorgen, einschließlich der Aufgabenverteilung innerhalb der Organisation des Anbieters der sehr großen Online-Plattform oder sehr großen Online-Suchmaschine, der Vermeidung von Interessenkonflikten und des verantwortungsvollen Umgangs mit den gemäß Artikel 34 ermittelten systemischen Risiken.

(6) Das Leitungsorgan billigt und überprüft regelmäßig, mindestens jedoch einmal jährlich, die Strategien und Maßnahmen für das Ansehen, das Management, die Überwachung und die Minderung der gemäß Artikel 34 ermittelten Risiken, denen die sehr große Online-Plattform oder sehr großen Online-Suchmaschine ausgesetzt ist oder ausgesetzt sein könnte.

(7) Das Leitungsorgan widmet der Prüfung der mit dem Risikomanagement verbundenen Maßnahmen ausreichend Zeit. Es beteiligt sich aktiv an den Entscheidungen im Zusammenhang mit dem Risikomanagement und sorgt dafür, dass für das Management der gemäß Artikel 34 ermittelten Risiken angemessene Ressourcen zugewiesen werden.

Artikel 42 Transparenzberichtspflichten

(1) Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen veröffentlichen spätestens zwei Monate nach dem in Artikel 33 Absatz 6 Unterabsatz 2 genannten Anwendungsbeginn und danach mindestens alle sechs Monate die in Artikel 15 genannten Berichte.

(2) Die von Anbietern sehr großer Online-Suchmaschinen veröffentlichten Berichte gemäß Absatz 1 dieses Artikels enthalten zusätzlich zu den in Artikel 15 und Artikel 24 Absatz 1 genannten Informationen folgende Angaben:

- a) die personellen Ressourcen, die der Anbieter einer sehr großen Online-Plattform für die Moderation von Inhalten in Bezug auf den in der Union angebotenen Dienst – aufgeschlüsselt nach jeder einschlägigen Amtssprache der Mitgliedstaaten – einsetzt, einschließlich für die Einhaltung der Verpflichtungen gemäß der Artikel 16 und 22 sowie für die Einhaltung der Verpflichtungen gemäß Artikel 20;
- b) die Qualifikationen und Sprachkenntnisse der Personen, die die unter Buchstabe a genannten Tätigkeiten durchführen, sowie die Schulung und Unterstützung dieses Personals;
- c) die Indikatoren für die Genauigkeit und damit zusammenhängende Informationen gemäß Artikel 15 Absatz 1 Buchstabe e, aufgeschlüsselt nach jeder Amtssprache der Mitgliedstaaten.

Die Berichte werden mindestens in einer der Amtssprachen der Mitgliedstaaten veröffentlicht.

(3) Zusätzlich zu den in Artikel 24 Absatz 2 genannten Informationen nehmen Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen die durchschnittliche monatliche Zahl der Nutzer für jeden Mitgliedstaat in die in Absatz 1 dieses Artikels genannten Berichte auf.

(4) Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen übermitteln dem Koordinator für digitale Dienste am Niederlassungsort und der Kommission spätestens drei Monate nach Eingang des Prüfberichts gemäß Artikel 37 Absatz 4 unverzüglich nach Abschluss folgende Unterlagen und machen sie öffentlich zugänglich:

- a) einen Bericht über die Ergebnisse der Risikobewertung gemäß Artikel 34,
- b) die gemäß Artikel 35 Absatz 1 getroffenen besonderen Abhilfemaßnahmen,
- c) den in Artikel 37 Absatz 4 genannten Prüfbericht,
- d) den in Artikel 37 Absatz 6 genannten Bericht über die Umsetzung der Prüfergebnisse,
- e) gegebenenfalls Informationen über die Konsultationen, die der Anbieter zur Unterstützung der Risikobewertungen und der Gestaltung der Risikominderungsmaßnahmen durchgeführt hat.

(5) Ist ein Anbieter einer sehr großen Online-Plattform oder sehr großen Online-Suchmaschine der Auffassung, dass die Veröffentlichung von Informationen gemäß Absatz 4 zur Offenlegung vertraulicher Informationen dieses Anbieters oder der Nutzer führen, erhebliche Schwachstellen für die Sicherheit seines Dienstes verursachen, die öffentliche Sicherheit beeinträchtigen oder Nutzern schaden könnte, so kann der Anbieter diese Informationen aus den öffentlich zugänglichen Berichten entfernen. In diesem Fall übermittelt der Anbieter dem Koordinator für digitale Dienste am Niederlassungsort und der Kommission die vollständigen Berichte zusammen mit einer Begründung für die Entfernung der Informationen aus den öffentlich zugänglichen Berichten.

Artikel 43 Aufsichtsgebühren

(1) Die Kommission erhebt von den Anbietern sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen bei ihrer Benennung gemäß Artikel 33 eine jährliche Aufsichtsgebühr.

(2) Der Gesamtbetrag der jährlichen Aufsichtsgebühren deckt die geschätzten Kosten, die der Kommission im Zusammenhang mit ihren Aufsichtsaufgaben im Rahmen dieser Verordnung entstehen, insbesondere die Kosten im Zusammenhang mit der Benennung gemäß Artikel 33, der Einrichtung, der Pflege und dem Betrieb der Datenbank gemäß Artikel 24 Absatz 5 und dem Informationsaustauschsystem gemäß Artikel 85, den Befassungen gemäß Artikel 59, der Unterstützung des Ausschusses gemäß Artikel 62 und den Aufsichtsaufgaben gemäß Artikel 56 und Kapitel IV Abschnitt 4.

(3) Anbietern sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen wird jährlich eine Aufsichtsgebühr für jeden Dienst berechnet, für den sie gemäß Artikel 33 benannt wurden.

Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Höhe der jährlichen Aufsichtsgebühr für jeden Anbieter einer sehr großen Online-Plattform oder einer sehr großen Online-Suchmaschine. Beim Erlass dieser Durchführungsrechtsakte wendet die Kommission die in dem in Absatz 4 des vorliegenden Artikels genannten delegierten Rechtsakt festgelegte Methodik an und beachtet die in Absatz 5 des vorliegenden Artikels genannten Grundsätze. Diese Durchführungsrechtsakte werden nach dem in Artikel 88 genannten Beratungsverfahren erlassen.

(4) Die Kommission erlässt gemäß Artikel 87 delegierte Rechtsakte und legt die detaillierte Methodik und entsprechende Verfahren für Folgendes fest:

- a) die Festlegung der Kosten gemäß Absatz 2;
- b) die Festlegung der einzelnen jährlichen Aufsichtsgebühren gemäß Absatz 5 Buchstaben b und c;
- c) die Festlegung des maximalen Gesamtgrenzwerts gemäß Absatz 5 Buchstabe c; und
- d) die für die Durchführung der Zahlung erforderlichen Einzelheiten.

Beim Erlass dieser delegierten Rechtsakte beachtet die Kommission die in Absatz 5 des vorliegenden Artikels genannten Grundsätze.

(5) Der Durchführungsrechtsakt gemäß Absatz 3 und der delegierte Rechtsakt gemäß Absatz 4 entsprechen den folgenden Grundsätzen:

- a) bei der Schätzung des Gesamtbetrags der jährlichen Aufsichtsgebühr werden die im Vorjahr angefallenen Kosten berücksichtigt;
- b) die jährliche Aufsichtsgebühr steht im Verhältnis zur durchschnittlichen monatlichen Zahl der aktiven Nutzer in der Union jeder gemäß Artikel 33 benannten sehr großen Online-Plattform oder jeder sehr großen Online-Suchmaschine;
- c) der Gesamtbetrag der jährlichen Aufsichtsgebühr, die einem bestimmten Anbieter einer sehr großen Online-Plattform oder einer sehr großen Suchmaschine in Rechnung gestellt wird, darf in keinem Fall 0,05 % seiner weltweiten Jahresnettoeinnahmen im vorangegangenen Geschäftsjahr übersteigen.

(6) Die einzelnen jährlichen Aufsichtsgebühren, die gemäß Absatz 1 in Rechnung gestellt werden, stellen externe zweckgebundene Einnahmen im Sinne von Artikel 21 Absatz 5 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates [\(41\)](#) dar.

(7) Die Kommission erstattet dem Europäischen Parlament und dem Rat jährlich Bericht über den Gesamtbetrag der Kosten, die für die Erfüllung der Aufgaben gemäß dieser Verordnung entstanden sind, und über den Gesamtbetrag der einzelnen jährlichen Aufsichtsgebühren, die im Vorjahr erhoben wurden.

Digital Markets Act – VO /EU 2022/1925

Artikel 1 Gegenstand und Anwendungsbereich

(1) Zweck dieser Verordnung ist es, zum reibungslosen Funktionieren des Binnenmarkts beizutragen, indem harmonisierte Vorschriften festgelegt werden, die in der gesamten Union zum Nutzen von gewerblichen Nutzern und Endnutzern für alle Unternehmen bestreitbare und faire Märkte im digitalen Sektor, auf denen Torwächter tätig sind, gewährleisten.

(2) Diese Verordnung gilt für zentrale Plattformdienste, die Torwächter für in der Union niedergelassene gewerbliche Nutzer oder in der Union niedergelassene oder aufhältige Endnutzer bereitstellen oder anbieten, ungeachtet des Niederlassungsorts und Standorts der Torwächter und ungeachtet des sonstigen auf die Erbringung von Dienstleistungen anwendbaren Rechts.

(3) Diese Verordnung gilt nicht für Märkte im Zusammenhang mit

- a) elektronischen Kommunikationsnetzen im Sinne des Artikels 2 Nummer 1 der Richtlinie (EU) 2018/1972;
- b) elektronischen Kommunikationsdiensten im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972, ausgenommen nummernunabhängige interpersonelle Kommunikationsdienste.

(4) Was interpersonelle Kommunikationsdienste im Sinne des Artikels 2 Nummer 5 der Richtlinie (EU) 2018/1972 betrifft, so berührt diese Verordnung nicht die Befugnisse und Zuständigkeiten, die den nationalen Regulierungsbehörden und anderen zuständigen Behörden nach Artikel 61 der genannten Richtlinie übertragen werden.

(5) Um eine Fragmentierung des Binnenmarkts zu vermeiden, erlegen die Mitgliedstaaten Torwächtern keine weiteren Verpflichtungen im Wege von Rechts- oder Verwaltungsvorschriften auf, um bestreitbare und faire Märkte zu gewährleisten. Diese Verordnung hindert die Mitgliedstaaten nicht daran, Unternehmen – einschließlich solcher, die zentrale Plattformdienste bereitstellen – für Angelegenheiten, die nicht in den Anwendungsbereich dieser Verordnung fallen, Verpflichtungen aufzuerlegen, sofern diese Verpflichtungen mit dem Unionsrecht vereinbar sind und nicht darauf zurückzuführen sind, dass die betreffenden Unternehmen den Status eines Torwächters im Sinne dieser Verordnung haben.

(6) Diese Verordnung berührt nicht die Anwendung der Artikel 101 und 102 AEUV. Sie lässt auch die Anwendung der folgenden Vorschriften unberührt:

- a) nationaler Wettbewerbsvorschriften zum Verbot von wettbewerbswidrigen Vereinbarungen, Beschlüssen von Unternehmensvereinigungen, aufeinander abgestimmten Verhaltensweisen und der missbräuchlichen Ausnutzung einer beherrschenden Stellung,
- b) nationaler Wettbewerbsvorschriften, mit denen andere Formen einseitiger Verhaltensweisen verboten werden, soweit sie auf andere Unternehmen als Torwächter angewandt werden oder Torwächtern damit weitere Verpflichtungen auferlegt werden, und
- c) der Verordnung (EG) Nr. 139/2004 des Rates und nationaler Fusionskontrollvorschriften.

(7) Die nationalen Behörden erlassen keine Entscheidungen, die einem von der Kommission nach dieser Verordnung erlassenen Beschluss zuwiderlaufen. Die Kommission und die Mitgliedstaaten arbeiten eng zusammen und koordinieren ihre Durchsetzungsmaßnahmen auf der Grundlage der in den Artikeln 37 und 38 genannten Grundsätze.

Artikel 2 Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Torwächter“ ein Unternehmen, das zentrale Plattformdienste bereitstellt und nach Artikel 3 benannt worden ist;
2. „zentraler Plattformdienst“ die folgenden Dienste:
 - a) Online-Vermittlungsdienste,
 - b) Online-Suchmaschinen,
 - c) Online-Dienste sozialer Netzwerke,
 - d) Video-Sharing-Plattform-Dienste,
 - e) nummernunabhängige interpersonelle Kommunikationsdienste,
 - f) Betriebssysteme,
 - g) Webbrowser,
 - h) virtuelle Assistenten,
 - i) Cloud-Computing-Dienste,
 - j) Online-Werbedienste, einschließlich Werbenetzwerken, Werbebörsen und sonstiger Werbevermittlungsdienste, die von einem Unternehmen, das einen der unter den Buchstaben a bis i genannten zentralen Plattformdienste bereitstellt, bereitgestellt werden;
3. „Dienst der Informationsgesellschaft“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535;
4. „digitaler Sektor“ den Sektor der Produkte und Dienstleistungen, die durch Dienste der Informationsgesellschaft bereitgestellt werden;
5. „Online-Vermittlungsdienste“ Online-Vermittlungsdienste im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2019/1150;
6. „Online-Suchmaschine“ eine Online-Suchmaschine im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150;
7. „Online-Dienst eines sozialen Netzwerks“ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Unterhaltungen, Beiträge, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und andere Nutzer und Inhalte entdecken können;
8. „Video-Sharing-Plattform-Dienst“ einen Video-Sharing-Plattform-Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe aa der Richtlinie 2010/13/EU;

9. „nummernunabhängiger interpersoneller Kommunikationsdienst“ einen nummernunabhängigen interpersonellen Kommunikationsdienst im Sinne des Artikels 2 Nummer 7 der Richtlinie (EU) 2018/1972;
10. „Betriebssystem“ eine Systemsoftware, die die Grundfunktionen der Hardware oder Software steuert und die Ausführung von Software-Anwendungen ermöglicht;
11. „Webbrowser“ eine Software-Anwendung, die Endnutzern den Zugriff auf und die Interaktion mit Web-Inhalten ermöglicht, die auf Servern gehostet werden, welche mit Netzwerken wie dem Internet verbunden sind, einschließlich eigenständiger Webbrowser sowie in Software integrierter oder eingebetteter oder vergleichbarer Webbrowser;
12. „virtueller Assistent“ eine Software, die Aufträge, Aufgaben oder Fragen verarbeiten kann, auch aufgrund von Eingaben in Ton-, Bild- und Schriftform, Gesten oder Bewegungen, und die auf der Grundlage dieser Aufträge, Aufgaben oder Fragen den Zugang zu anderen Diensten ermöglicht oder angeschlossene physische Geräte steuert;
13. „Cloud-Computing-Dienst“ einen Cloud-Computing-Dienst im Sinne des Artikels 4 Nummer 19 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates [\(24\)](#);
14. „Geschäfte für Software-Anwendungen“ Online-Vermittlungsdienste, durch die in erster Linie Software-Anwendungen als Produkt oder Dienstleistung vermittelt werden;
15. „Software-Anwendung“ ein digitales Produkt oder eine digitale Dienstleistung, das bzw. die über ein Betriebssystem genutzt wird;
16. „Zahlungsdienst“ einen Zahlungsdienst im Sinne des Artikels 4 Nummer 3 der Richtlinie (EU) 2015/2366;
17. „technischer Dienst zur Unterstützung von Zahlungsdiensten“ einen Dienst im Sinne des Artikels 3 Buchstabe j der Richtlinie (EU) 2015/2366;
18. „Zahlungsdienst für in der Software-Anwendung integrierte Käufe“ eine Software-Anwendung, einen Dienst oder eine Benutzeroberfläche, die den Kauf digitaler Inhalte oder digitaler Dienste innerhalb einer Software-Anwendung, einschließlich Inhalten, Abonnements, Merkmalen oder Funktionen, und die Zahlungen für solche Käufe ermöglicht;
19. „Identifizierungsdienst“ einen Dienst, der zusammen mit oder zur Unterstützung von zentralen Plattformdiensten erbracht wird und unabhängig von der verwendeten Technologie eine Überprüfung der Identität von Endnutzern oder gewerblichen Nutzern ermöglicht;
20. „Endnutzer“ eine natürliche oder juristische Person, die zentrale Plattformdienste nutzt und nicht als gewerblicher Nutzer auftritt;
21. „gewerblicher Nutzer“ eine natürliche oder juristische Person, die im Rahmen einer geschäftlichen oder beruflichen Tätigkeit zentrale Plattformdienste zum Zweck oder im Zuge der Bereitstellung von Waren oder Dienstleistungen für Endnutzer nutzt;
22. „Ranking“ die relative Hervorhebung von Waren und Dienstleistungen, die über Online-Vermittlungsdienste, Online-Dienste sozialer Netzwerke, Video-Sharing-Plattform-Dienste oder virtuelle Assistenten angeboten werden, oder die Relevanz, die den Suchergebnissen von Online-Suchmaschinen mittels entsprechender Darstellung, Organisation oder Kommunikation durch die Unternehmen, die Online-Vermittlungsdienste, Online-Dienste sozialer Netzwerke, Video-Sharing-Plattform-Dienste, virtuelle Assistenten oder Online-Suchmaschinen anbieten, zugemessen wird, unabhängig von den für diese Darstellung, Organisation oder Kommunikation verwendeten technischen Mitteln und unabhängig davon, ob nur ein einziges Ergebnis dargestellt oder kommuniziert wird;
23. „Suchergebnisse“ alle Informationen in beliebigem Format, darunter in Text-, grafischer, gesprochener oder sonstiger Form, die als Antwort auf eine Suchanfrage ausgegeben werden und sich auf diese beziehen, unabhängig davon, ob es sich bei den ausgegebenen Informationen um ein bezahltes oder ein unbezahltes Ergebnis, eine direkte Antwort oder ein Produkt, eine Dienstleistung oder eine Information handelt, das bzw.

die in Verbindung mit den organischen Ergebnissen angeboten oder zusammen mit diesen angezeigt wird oder teilweise oder vollständig in diese eingebettet ist;

24. „Daten“ jegliche digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jegliche Zusammenstellung solcher Handlungen, Tatsachen oder Informationen, auch in Form von Ton-, Bild- oder audiovisuellem Material;
25. „personenbezogene Daten“ personenbezogene Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679;
26. „nicht personenbezogene Daten“ Daten, bei denen es sich nicht um personenbezogene Daten handelt;
27. „Unternehmen“ eine Einheit, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung, einschließlich aller verbundenen Unternehmen, die durch die unmittelbare oder mittelbare Kontrolle eines Unternehmens durch ein anderes Unternehmen eine Gruppe bilden;
28. „Kontrolle“ die Möglichkeit, im Sinne des Artikels 3 Absatz 2 der Verordnung (EG) Nr. 139/2004 bestimmenden Einfluss auf ein Unternehmen auszuüben;
29. „Interoperabilität“ die Fähigkeit, Informationen auszutauschen und die über Schnittstellen oder andere Lösungen ausgetauschten Informationen beiderseitig zu nutzen, sodass alle Hardware- oder Softwarekomponenten mit anderer Hardware und Software auf die vorgesehene Weise zusammenwirken und bei Nutzern auf die vorgesehene Weise funktionieren;
30. „Umsatz“ den von einem Unternehmen erzielten Umsatz im Sinne des Artikels 5 Absatz 1 der Verordnung (EG) Nr. 139/2004;
31. „Profiling“ ein Profiling im Sinne des Artikels 4 Nummer 4 der Verordnung (EU) 2016/679;
32. „Einwilligung“ eine Einwilligung im Sinne des Artikels 4 Nummer 11 der Verordnung (EU) 2016/679;
33. „nationales Gericht“ ein Gericht eines Mitgliedstaats im Sinne des Artikels 267 AEUV.

KAPITEL II TORWÄCHTER

Artikel 3 Benennung von Torwächtern

(1) Ein Unternehmen wird als Torwächter benannt, wenn es

- a) erheblichen Einfluss auf den Binnenmarkt hat,
- b) einen zentralen Plattformdienst bereitstellt, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient, und
- c) hinsichtlich seiner Tätigkeiten eine gefestigte und dauerhafte Position innehat oder absehbar ist, dass es eine solche Position in naher Zukunft erlangen wird.

(2) Es wird davon ausgegangen, dass ein Unternehmen die jeweiligen Anforderungen des Absatzes 1 erfüllt, wenn es

- a) in Bezug auf Absatz 1 Buchstabe a in jedem der vergangenen drei Geschäftsjahre in der Union einen Jahresumsatz von mindestens 7,5 Mrd. EUR erzielt hat oder wenn seine durchschnittliche Marktkapitalisierung oder sein entsprechender Marktwert im vergangenen Geschäftsjahr mindestens 75 Mrd. EUR betrug und es in mindestens drei Mitgliedstaaten denselben zentralen Plattformdienst bereitstellt;
- b) in Bezug auf Absatz 1 Buchstabe b einen zentralen Plattformdienst bereitstellt, der im vergangenen Geschäftsjahr mindestens 45 Millionen in der Union niedergelassene oder aufhältige monatlich aktive Endnutzer und mindestens 10 000 in der Union niedergelassene jährlich aktive gewerbliche Nutzer hatte, wobei die Ermittlung und Berechnung gemäß der Methode und den Indikatoren im Anhang erfolgt;
- c) in Bezug auf Absatz 1 Buchstabe c die unter Buchstabe b des vorliegenden Absatzes genannten Schwellenwerte in jedem der vergangenen drei Geschäftsjahre erreicht hat.

(3) Wenn ein Unternehmen, das zentrale Plattformdienste bereitstellt, alle in Absatz 2 genannten Schwellenwerte erreicht, teilt es dies der Kommission unverzüglich, in jedem Fall aber innerhalb von zwei Monaten nach Erreichen der Schwellenwerte mit und übermittelt ihr die in Absatz 2 genannten einschlägigen Angaben. Die entsprechende Mitteilung muss die in Absatz 2 genannten einschlägigen Angaben für jeden zentralen Plattformdienst des Unternehmens enthalten, der die in Absatz 2 Buchstabe b genannten Schwellenwerte erreicht. Erreicht ein weiterer zentraler Plattformdienst, der von dem zuvor als Torwächter benannten Unternehmen erbracht wird, die in Absatz 2 Buchstaben b und c genannten Schwellenwerte, so teilt das Unternehmen dies der Kommission innerhalb von zwei Monaten nach Erreichen dieser Schwellenwerte mit.

Versäumt es das Unternehmen, das den zentralen Plattformdienst bereitstellt, die Kommission gemäß Unterabsatz 1 des vorliegenden Absatzes zu benachrichtigen und innerhalb der von der Kommission in dem Auskunftsverlangen gemäß Artikel 21 gesetzten Frist alle einschlägigen Angaben zu übermitteln, die die Kommission benötigt, um das betroffene Unternehmen gemäß Absatz 4 des vorliegenden Artikels als Torwächter zu benennen, so ist die Kommission dennoch berechtigt, das Unternehmen auf der Grundlage der ihr vorliegenden Angaben als Torwächter zu benennen.

Kommt das Unternehmen, das zentrale Plattformdienste bereitstellt, dem Auskunftsverlangen gemäß Unterabsatz 2 des vorliegenden Absatzes nach oder werden die Informationen übermittelt nachdem die in jenem Unterabsatz genannte Frist abgelaufen ist, so wendet die Kommission das Verfahren nach Absatz 4 an.

(4) Die Kommission benennt ein Unternehmen, das zentrale Plattformdienste bereitstellt und alle in Absatz 2 genannten Schwellenwerte erreicht, unverzüglich und spätestens innerhalb von 45 Arbeitstagen nach Erhalt der vollständigen Angaben nach Absatz 3 als Torwächter.

(5) Das Unternehmen, das zentrale Plattformdienste bereitstellt, kann im Rahmen seiner Mitteilung hinreichend substantiierte Argumente dafür vorbringen, dass es in Anbetracht der Umstände, unter denen der betreffende zentrale Plattformdienst bereitgestellt wird, die in Absatz 1 aufgeführten Anforderungen ausnahmsweise nicht erfüllt, obwohl es alle in Absatz 2 genannten Schwellenwerte erreicht.

Ist die Kommission der Auffassung, dass die von dem Unternehmen, das zentrale Plattformdienste bereitstellt, gemäß Unterabsatz 1 vorgebrachten Argumente nicht hinreichend substantiiert sind, weil sie die Vermutungen nach Absatz 2 dieses Artikels nicht eindeutig entkräften, so kann sie diese Argumente innerhalb der in Absatz 4 genannten Frist zurückweisen, ohne das Verfahren nach Artikel 17 Absatz 3 anzuwenden.

Bringt das Unternehmen, das zentrale Plattformdienste bereitstellt, solche hinreichend substantiierten Argumente vor, die die Vermutungen nach Absatz 2 des vorliegenden Artikels eindeutig entkräften, so kann die Kommission ungeachtet des Unterabsatzes 1 des vorliegenden Absatzes innerhalb der in Absatz 4 dieses Artikels genannten Frist das Verfahren nach Artikel 17 Absatz 3 eröffnen.

Kommt die Kommission zu dem Schluss, dass das Unternehmen, das zentrale Plattformdienste bereitstellt, nicht nachweisen konnte, dass die von ihm erbrachten einschlägigen zentralen Plattformdienste die Anforderungen des Absatzes 1 des vorliegenden Artikels nicht erfüllen, so benennt sie dieses Unternehmen gemäß dem Verfahren nach Artikel 17 Absatz 3 als Torwächter.

(6) Der Kommission wird gemäß Artikel 49 die Befugnis übertragen, delegierte Rechtsakte zu erlassen, um diese Verordnung durch Festlegung der Methode zu ergänzen, anhand deren bestimmt wird, ob die in Absatz 2 des vorliegenden Artikels genannten quantitativen Schwellenwerte erreicht sind, und um diese Methode bei Bedarf regelmäßig an Marktentwicklungen und technologische Entwicklungen anzupassen.

(7) Der Kommission wird die Befugnis übertragen, gemäß Artikel 49 delegierte Rechtsakte zu erlassen, um diese Verordnung durch Aktualisierung der Methode und der Liste der Indikatoren im Anhang zu ändern.

(8) Die Kommission benennt jedes Unternehmen, das zentrale Plattformdienste bereitstellt und sämtliche in Absatz 1 des vorliegenden Artikels genannten Anforderungen erfüllt, aber nicht jeden der in Absatz 2 des vorliegenden Artikels genannten Schwellenwerte erreicht, nach dem Verfahren des Artikels 17 als Torwächter.

Dafür berücksichtigt die Kommission einige oder alle der folgenden Aspekte, soweit sie für das betreffende Unternehmen, das zentrale Plattformdienste bereitstellt, relevant sind:

- a) die Größe dieses Unternehmens, einschließlich seines Umsatzes, seiner Marktkapitalisierung, seiner Tätigkeiten und seiner Position,
- b) die Zahl der gewerblichen Nutzer, die den zentralen Plattformdienst nutzen, um Endnutzer zu erreichen, und die Zahl der Endnutzer,
- c) Netzwerkeffekte und Datenvorteile, insbesondere im Zusammenhang mit dem Zugang des Unternehmens zu personenbezogenen und nicht personenbezogenen Daten und deren Erhebung sowie Analysefähigkeiten,
- d) etwaige Skalen- und Verbundeffekte, von denen das Unternehmen profitiert, auch in Bezug auf Daten und gegebenenfalls auf seine Tätigkeiten außerhalb der Union,
- e) die Bindung von gewerblichen Nutzern und Endnutzern, einschließlich Kosten für einen Wechsel und Verhaltensverzerrungen, die die Fähigkeit von gewerblichen Nutzern und Endnutzern zum Wechsel oder zur Parallelverwendung mehrerer Dienste einschränken,
- f) eine konglomeratsartige Unternehmensstruktur oder vertikale Integration des Unternehmens, die es ihm beispielsweise ermöglicht, Quersubventionen vorzunehmen, Daten aus verschiedenen Quellen zusammenzuführen oder seine Position zu seinem Vorteil zu nutzen, oder
- g) sonstige strukturelle Geschäfts- oder Dienstmerkmale.

Bei ihrer Bewertung nach diesem Absatz trägt die Kommission auch der absehbaren Entwicklung in Bezug auf die in Unterabsatz 2 aufgeführten Aspekte Rechnung, einschließlich etwaiger geplanter Zusammenschlüsse, an denen ein weiteres Unternehmen beteiligt ist, das zentrale Plattformdienste oder andere Dienste im digitalen Sektor bereitstellt oder die Erhebung von Daten ermöglicht.

Wenn ein Unternehmen, das einen zentralen Plattformdienst bereitstellt und die in Absatz 2 genannten quantitativen Schwellenwerte nicht erreicht, den von der Kommission angeordneten Untersuchungsmaßnahmen nicht hinreichend nachkommt und dieser Verstoß andauert, nachdem das Unternehmen aufgefordert wurde, den Maßnahmen innerhalb einer angemessenen Frist nachzukommen und dazu Stellung zu nehmen, darf die Kommission das Unternehmen auf der Grundlage der ihr vorliegenden Informationen als Torwächter benennen.

(9) Bei jedem Unternehmen, das gemäß Absatz 4 oder 8 als Torwächter benannt wurde, führt die Kommission im Benennungsbeschluss die einschlägigen zentralen Plattformdienste auf, die von dem Unternehmen bereitgestellt werden und für sich genommen gemäß Absatz 1 Buchstabe b gewerblichen Nutzern als wichtiger Zugangstor zu Endnutzern dienen.

(10) Der Torwächter muss die in den Artikeln 5, 6 und 7 genannten Verpflichtungen spätestens sechs Monate, nachdem einer seiner zentralen Plattformdienste im Benennungsbeschluss nach Absatz 9 des vorliegenden Artikels aufgeführt wurde, erfüllen.

Artikel 4 Überprüfung des Torwächter-Status

(1) Die Kommission kann auf Antrag oder von Amts wegen jederzeit einen nach Artikel 3 erlassenen Benennungsbeschluss überprüfen, ändern oder aufheben,

- a) wenn sich der Sachverhalt, auf den sich der Benennungsbeschluss stützte, in einem wesentlichen Punkt geändert hat oder
- b) wenn der Benennungsbeschluss auf unvollständigen, unrichtigen oder irreführenden Angaben beruhte.

(2) Die Kommission überprüft regelmäßig, mindestens jedoch alle drei Jahre, ob die Torwächter die in Artikel 3 Absatz 1 genannten Anforderungen nach wie vor erfüllen. Diese Überprüfung prüft, ob die Liste der zentralen Plattformdienste des Torwächters, die jeweils für sich genommen gemäß Artikel 3 Absatz 1 Buchstabe b gewerblichen Nutzern als wichtiger Zugangstor zu Endnutzern dienen, geändert werden muss. Diese Überprüfungen haben keine aufschiebende Wirkung auf die Verpflichtungen des Torwächters.

Die Kommission überprüft außerdem mindestens einmal jährlich, ob neue Unternehmen, die zentrale Plattformdienste bereitstellen, die genannten Anforderungen erfüllen.

Stellt die Kommission anhand der Überprüfungen nach Unterabsatz 1 fest, dass sich der Sachverhalt, auf den sich die Benennung der Unternehmen, die zentrale Plattformdienste bereitstellen, als Torwächter stützte, geändert hat, so erlässt sie einen Beschluss zur Bestätigung, Änderung oder Aufhebung des Benennungsbeschlusses.

(3) Die Kommission veröffentlicht und aktualisiert laufend eine Liste der Torwächter und die Liste der zentralen Plattformdienste, in Bezug auf welche die Torwächter die in Kapitel III genannten Verpflichtungen einhalten müssen.

KAPITEL III UNFAIRE ODER DIE BESTREITBARKEIT BESCHRÄNKENDE PRAKTIKEN VON TORWÄCHTERN

Artikel 5 Verpflichtungen von Torwächtern

(1) Der Torwächter hält alle Verpflichtungen nach diesem Artikel in Bezug auf jeden seiner zentralen Plattformdienste ein, die im Benennungsbeschluss nach Artikel 3 Absatz 9 aufgeführt sind.

(2) Der Torwächter darf

- a) personenbezogene Daten von Endnutzern, die Dienste Dritter nutzen, welche zentrale Plattformdienste des Torwächters in Anspruch nehmen, nicht zum Zweck des Betriebs von Online-Werbediensten verarbeiten,
- b) personenbezogene Daten aus dem betreffenden zentralen Plattformdienst nicht mit personenbezogenen Daten aus weiteren zentralen Plattformdiensten oder aus anderen vom Torwächter bereitgestellten Diensten oder mit personenbezogenen Daten aus Diensten Dritter zusammenführen,
- c) personenbezogene Daten aus dem betreffenden zentralen Plattformdienst nicht in anderen vom Torwächter getrennt bereitgestellten Diensten, einschließlich anderer zentraler Plattformdienste, weiterverwenden und umgekehrt und
- d) Endnutzer nicht in anderen Diensten des Torwächters anmelden, um personenbezogene Daten zusammenzuführen,

außer wenn dem Endnutzer die spezifische Wahl gegeben wurde und er im Sinne des Artikels 4 Nummer 11 und des Artikels 7 der Verordnung (EU) 2016/679 eingewilligt hat.

Wurde die für die Zwecke des Unterabsatz 1 gegebene Einwilligung vom Endnutzer verweigert oder widerrufen, so darf der Torwächter sein Ersuchen um Einwilligung für denselben Zweck innerhalb eines Jahres nicht mehr als einmal wiederholen.

Dieser Absatz berührt nicht die Möglichkeit des Torwächters, sich gegebenenfalls auf Artikel 6 Absatz 1 Buchstaben c, d und e der Verordnung (EU) 2016/679 zu berufen.

(3) Der Torwächter darf die gewerbliche Nutzer nicht daran hindern, Endnutzern dieselben Produkte oder Dienstleistungen über Online-Vermittlungsdienste Dritter oder über ihre eigenen direkten Online-Vertriebskanäle zu anderen Preisen oder Bedingungen anzubieten als über die Online-Vermittlungsdienste des Torwächters.

(4) Der Torwächter gibt gewerblichen Nutzern die Möglichkeit, Angebote gegenüber Endnutzern, die über seinen zentralen Plattformdienst oder über andere Kanäle akquiriert wurden, kostenlos zu kommunizieren und zu bewerben – auch zu anderen Bedingungen – und mit diesen Endnutzern Verträge zu schließen, unabhängig davon, ob sie zu diesem Zweck die zentralen Plattformdienste des Torwächters nutzen.

(5) Der Torwächter gibt Endnutzern die Möglichkeit, über seine zentralen Plattformdienste durch Nutzung der Software-Anwendung eines gewerblichen Nutzers auf Inhalte, Abonnements, Funktionen oder andere Elemente zuzugreifen und diese zu nutzen, auch wenn diese Endnutzer diese Elemente bei dem betreffenden gewerblichen Nutzer ohne Nutzung der zentralen Plattformdienste des Torwächters erworben haben.

(6) Der Torwächter darf gewerbliche Nutzer oder Endnutzer nicht direkt oder indirekt daran hindern, einer zuständigen Behörde, einschließlich nationaler Gerichte, eine etwaige Nichteinhaltung des einschlägigen Unionsrechts oder nationalen Rechts durch den Torwächter im Zusammenhang mit den Praktiken des Torwächters mitzuteilen, oder sie in dieser Hinsicht einschränken. Dies berührt nicht das Recht von

gewerblichen Nutzern und Torwächtern, in ihren Vereinbarungen die Nutzungsbedingungen von Mechanismen für die Behandlung von rechtmäßigen Beschwerden festzulegen.

(7) Der Torwächter darf von Endnutzern oder gewerblichen Nutzern nicht verlangen, dass sie einen Identifizierungsdienst, eine Webbrowser-Engine oder einen Zahlungsdienst, oder technische Dienste zur Unterstützung der Erbringung von Zahlungsdiensten, beispielsweise Zahlungssysteme für in der Software-Anwendung integrierte Käufe, des Torwächters im Zusammenhang mit Diensten, die von den gewerblichen Nutzern, die zentrale Plattformdienste des Torwächters nutzen, erbracht werden, nutzen bzw. – im Falle von gewerblichen Nutzern – nutzen, anbieten oder mit ihnen interoperieren.

(8) Der Torwächter darf von gewerblichen Nutzern oder Endnutzern nicht verlangen, dass sie weitere zentrale Plattformdienste, die im Benennungsbeschluss nach Artikel 3 Absatz 9 aufgeführt sind oder die die in Artikel 3 Absatz 2 Buchstabe b genannten Schwellenwerte erreichen, abonnieren oder sich bei diesen registrieren, um gemäß dem genannten Artikel aufgeführte zentrale Plattformdienste des Torwächters nutzen, darauf zugreifen, sich bei diesen anmelden oder sich bei diesen registrieren zu können.

(9) Der Torwächter gibt jedem Werbetreibenden, für den er Online-Werbedienste erbringt, oder von Werbetreibenden bevollmächtigten Dritten auf Anfrage des Werbetreibenden hin täglich kostenlos Auskunft über jede vom Werbetreibenden geschaltete Anzeige, und zwar über

- a) die vom Werbetreibenden gezahlten Preise und Gebühren, einschließlich etwaiger Abzüge und Aufschläge, für jede der vom Torwächter bereitgestellten einschlägigen Online-Werbedienste,
- b) die vom Herausgeber erhaltene Vergütung, einschließlich etwaiger Abzüge und Aufschläge, vorbehaltlich der Zustimmung des Herausgebers, und
- c) die Kennzahlen, anhand deren die einzelnen Preise, Gebühren und Vergütungen berechnet werden.

Stimmt ein Herausgeber der Weitergabe von Informationen über die erhaltene Vergütung gemäß Unterabsatz 1 Buchstabe b nicht zu, so gibt der Torwächter jedem Werbetreibenden kostenlos Auskunft über die durchschnittliche tägliche Vergütung, die dieser Herausgeber für die betreffenden Anzeigen erhält, einschließlich etwaiger Abzüge und Aufschläge.

(10) Der Torwächter gibt jedem Herausgeber, für den er Online-Werbedienste erbringt, oder von Herausgebern bevollmächtigten Dritten auf Anfrage des Herausgebers hin täglich kostenlos Auskunft über jede auf dem Inventar des Herausgebers angezeigte Anzeige, und zwar über

- a) die vom Herausgeber erhaltene Vergütung und die von ihm gezahlten Gebühren, einschließlich etwaiger Abzüge und Aufschläge, für jede der vom Torwächter bereitgestellten einschlägigen Online-Werbedienste,
- b) den vom Werbetreibendem gezahlten Preis, einschließlich etwaiger Abzüge und Aufschläge, vorbehaltlich der Zustimmung des Werbetreibenden, und
- c) die Kennzahlen, anhand dessen die einzelnen Preise und Vergütungen berechnet werden.

Stimmt ein Werbetreibender der Weitergabe von Informationen nicht zu, so gibt der Torwächter jedem Herausgeber kostenlos Auskunft über den durchschnittlichen täglichen Preis, den dieser Werbetreibende für die betreffenden Anzeigen zahlt, einschließlich etwaiger Abzüge und Aufschläge.

Artikel 6 Verpflichtungen von Torwächtern, die möglicherweise noch durch Artikel 8 näher ausgeführt werden

(1) Der Torwächter hält alle Verpflichtungen nach diesem Artikel in Bezug auf jeden seiner zentralen Plattformdienste ein, die im Benennungsbeschluss nach Artikel 3 Absatz 9 aufgeführt sind.

(2) Der Torwächter darf im Wettbewerb mit gewerblichen Nutzern keine nicht öffentlich zugänglichen Daten verwenden, die von diesen gewerblichen Nutzern im Zusammenhang mit der Nutzung der betreffenden zentralen Plattformdienste oder der zusammen mit den betreffenden zentralen Plattformdiensten oder zu deren Unterstützung erbrachten Dienste generiert oder bereitgestellt werden, einschließlich der von den Kunden dieser gewerblichen Nutzer generierten oder bereitgestellten Daten.

Für die Zwecke des Unterabsatzes 1 umfassen die nicht öffentlich zugänglichen Daten alle von gewerblichen Nutzern generierten aggregierten und nichtaggregierten Daten, die aus den kommerziellen Tätigkeiten

gewerblicher Nutzer oder ihrer Kunden auf den betreffenden zentralen Plattformdiensten oder auf Diensten, die zusammen mit den betreffenden zentralen Plattformdiensten des Torwächters oder zu deren Unterstützung erbracht werden, abgeleitet oder durch diese erhoben werden können, einschließlich Klick-, Anfrage-, Ansichts- und Sprachdaten.

(3) Der Torwächter gestattet es Endnutzern und ermöglicht es ihnen technisch, Software-Anwendungen auf dem Betriebssystem des Torwächters auf einfache Weise zu deinstallieren; dies gilt unbeschadet der Möglichkeit des Torwächters, die Deinstallation von Software-Anwendungen zu beschränken, die für das Funktionieren des Betriebssystems oder des Geräts unabdingbar sind und die aus technischen Gründen nicht von Dritten eigenständig angeboten werden können.

Der Torwächter gestattet es Endnutzern und ermöglicht es ihnen technisch, Standardeinstellungen des Betriebssystems, virtuellen Assistenten und Webbrowsers des Torwächters, die Endnutzer zu vom Torwächter angebotenen Produkten oder Dienstleistungen leiten oder lenken, auf einfache Weise zu ändern. Dazu gehört, dass Endnutzer bei der ersten Nutzung einer Online-Suchmaschine, eines virtuellen Assistenten oder eines Webbrowsers des Torwächters, die bzw. der im Benennungsbeschluss nach Artikel 3 Absatz 9 aufgeführt sind, aufgefordert werden, aus einer Liste der wesentlichen verfügbaren Diensteanbieter die Online-Suchmaschine, den virtuellen Assistenten oder den Webbrowser, auf die bzw. den das Betriebssystem des Torwächters Nutzer standardmäßig leitet oder lenkt, sowie die Online-Suchmaschine, auf die der virtuelle Assistent und der Webbrowser des Torwächters Nutzer standardmäßig leitet oder lenkt, auszuwählen.

(4) Der Torwächter gestattet es und ermöglicht es technisch, Software-Anwendungen Dritter und von Dritten betriebene Geschäfte für Software-Anwendungen, die sein Betriebssystem nutzen oder mit diesem interoperieren, zu installieren und effektiv zu nutzen und auf diese Software-Anwendungen bzw. Geschäfte für Software-Anwendungen auf anderem Wege als über die betreffenden zentralen Plattformdienste des Torwächters zuzugreifen. Der Torwächter darf gegebenenfalls nicht verhindern, dass die heruntergeladenen Software-Anwendungen Dritter oder von Dritten betriebenen Geschäfte für Software-Anwendungen Endnutzer auffordern, zu entscheiden, ob sie die heruntergeladene Software-Anwendung oder das heruntergeladene Geschäft für Software-Anwendungen als Standard festlegen wollen. Der Torwächter muss es Endnutzern, die beschließen, die heruntergeladene Software-Anwendung oder das heruntergeladene Geschäft für Software-Anwendungen als Standard festzulegen, technisch ermöglichen, diese Änderung auf einfache Weise vorzunehmen.

Der Torwächter wird nicht daran gehindert, Maßnahmen zu ergreifen, soweit sie unbedingt erforderlich und angemessen sind, um sicherzustellen, dass Software-Anwendungen Dritter oder von Dritten betriebene Geschäfte für Software-Anwendungen die Integrität der vom Torwächter bereitgestellten Hardware oder des vom Torwächter bereitgestellten Betriebssystems nicht gefährden, sofern die Maßnahmen vom Torwächter hinreichend begründet werden.

Darüber hinaus wird der Torwächter nicht daran gehindert, Maßnahmen und Einstellungen, die keine Standardeinstellungen sind, vorzunehmen, soweit sie unbedingt erforderlich und angemessen sind, die es Endnutzern ermöglichen, die Sicherheit in Bezug auf Software-Anwendungen Dritter oder von Dritten betriebene Geschäfte für Software-Anwendungen wirksam zu schützen, sofern die Maßnahmen und Einstellungen keine Standardeinstellungen sind und vom Torwächter hinreichend begründet werden.

(5) Der Torwächter darf von ihm selbst angebotene Dienstleistungen und Produkte beim Ranking sowie bei der damit verbundenen Indexierung und dem damit verbundenen Auffinden gegenüber ähnlichen Dienstleistungen oder Produkten eines Dritten nicht bevorzugen. Der Torwächter muss das Ranking anhand transparenter, fairer und diskriminierungsfreier Bedingungen vornehmen.

(6) Der Torwächter darf die Möglichkeiten der Endnutzer, zwischen verschiedenen Software-Anwendungen und Diensten, auf die über die zentralen Plattformdienste des Torwächters zugegriffen wird, zu wechseln oder solche zu abonnieren, weder technisch noch anderweitig beschränken; dies gilt auch für die Wahl der Internetzugangsdienste für Endnutzer.

(7) Der Torwächter ermöglicht Diensteanbietern und Anbietern von Hardware kostenlos wirksame Interoperabilität mit – und Zugang für Zwecke der Interoperabilität zu – denselben über das Betriebssystem oder den virtuellen Assistenten, das bzw. der im Benennungsbeschluss nach Artikel 3 Absatz 9 aufgeführt ist, zugegriffenen oder gesteuerten Hardware- und Software-Funktionen, die für die vom Torwächter

bereitgestellten Dienste oder die von ihm bereitgestellte Hardware zur Verfügung stehen. Darüber hinaus ermöglicht der Torwächter gewerblichen Nutzern und alternativen Anbietern von Diensten, die zusammen mit zentralen Plattformdiensten oder zu deren Unterstützung erbracht werden, kostenlos wirksame Interoperabilität mit – und Zugang für Zwecke der Interoperabilität zu – denselben Betriebssystem-, Hardware- oder Software-Funktionen, die der Torwächter bei der Erbringung solcher Dienste zur Verfügung hat oder verwendet, unabhängig davon, ob die Funktionen Teil des Betriebssystems sind.

Der Torwächter wird nicht daran gehindert, unbedingt erforderliche und angemessene Maßnahmen zu ergreifen, um sicherzustellen, dass die Integrität des Betriebssystems, des virtuellen Assistenten, der Hardware oder der Software-Funktionen, die vom Torwächter bereitgestellt werden, durch Interoperabilität nicht beeinträchtigt werden, sofern der Torwächter solche Maßnahmen hinreichend begründet.

(8) Der Torwächter gewährt Werbetreibenden und Herausgebern sowie von Werbetreibenden und Herausgebern beauftragten Dritten auf ihren Antrag hin kostenlos Zugang zu seinen Instrumenten zur Leistungsmessung und zu den Daten, die sie benötigen, um ihre eigene unabhängige Überprüfung des Werbeinventars vorzunehmen, einschließlich aggregierter und nichtaggregierter Daten. Diese Daten werden so bereitgestellt, dass Werbetreibende und Herausgeber ihre eigenen Überprüfungs- und Messinstrumente einsetzen können, um die Leistung der von den Torwächtern bereitgestellten zentralen Plattformdienste zu bewerten.

(9) Der Torwächter ermöglicht Endnutzern und von ihnen beauftragten Dritten auf ihren Antrag hin kostenlos die effektive Übertragbarkeit der Daten, die vom Endnutzer bereitgestellt oder durch die Tätigkeit des Endnutzers im Zusammenhang mit der Nutzung des betreffenden zentralen Plattformdienstes generiert werden, auch indem kostenlos Instrumente bereitgestellt werden, die die effektive Nutzung dieser Datenübertragbarkeit erleichtern, und indem unter anderem ein permanenter Echtzeitzugang zu diesen Daten gewährleistet wird.

(10) Der Torwächter gewährt gewerblichen Nutzern und von einem gewerblichen Nutzer zugelassenen Dritten auf ihren Antrag hin kostenlos einen effektiven, hochwertigen und permanenten Echtzeitzugang zu aggregierten und nichtaggregierten Daten, einschließlich personenbezogener Daten, die im Zusammenhang mit der Nutzung der betreffenden zentralen Plattformdienste oder von Diensten, die zusammen mit den betreffenden zentralen Plattformdiensten oder zu deren Unterstützung erbracht werden, durch diese gewerblichen Nutzer und die Endnutzer, die die Produkte oder Dienstleistungen dieser gewerblichen Nutzer in Anspruch nehmen, bereitgestellt oder generiert werden, und ermöglicht die Nutzung solcher Daten. In Bezug auf personenbezogene Daten darf der Torwächter diesen Zugang zu den und die Nutzung von personenbezogenen Daten nur dann gewähren bzw. ermöglichen, wenn sie unmittelbar mit der Nutzung der vom betreffenden gewerblichen Nutzer über den betreffenden zentralen Plattformdienst angebotenen Produkte oder Dienstleistungen durch die Endnutzer im Zusammenhang stehen und sofern die Endnutzer einer solchen Weitergabe durch eine Einwilligung zustimmt.

(11) Der Torwächter gewährt Drittunternehmen, die Online-Suchmaschinen bereitstellen, auf ihren Antrag hin zu fairen, zumutbaren und diskriminierungsfreien Bedingungen Zugang zu Ranking-, Anfrage-, Klick- und Ansichtsdaten in Bezug auf unbezahlte und bezahlte Suchergebnisse, die von Endnutzern über seine Online-Suchmaschinen generiert werden. Alle derartigen Anfrage-, Klick- und Ansichtsdaten, bei denen es sich um personenbezogene Daten handelt, werden anonymisiert.

(12) Der Torwächter wendet für den Zugang gewerblicher Nutzer zu seinen im Benennungsbeschluss nach Artikel 3 Absatz 9 aufgeführten Geschäften für Software-Anwendungen, Online-Suchmaschinen und Online-Diensten sozialer Netzwerke faire, zumutbare und diskriminierungsfreie allgemeine Bedingungen an.

Zu diesem Zweck veröffentlicht der Torwächter allgemeine Zugangsbedingungen, einschließlich eines alternativen Streitbeilegungsmechanismus.

Die Kommission prüft, ob die veröffentlichten allgemeinen Zugangsbedingungen dem vorliegenden Absatz entsprechen.

(13) Die allgemeinen Bedingungen des Torwächters für die Kündigung eines zentralen Plattformdienstes dürfen nicht unverhältnismäßig sein. Der Torwächter stellt sicher, dass die Kündigungsbedingungen ohne übermäßige Schwierigkeiten eingehalten werden können.

Artikel 7 Verpflichtung von Torwächtern zur Interoperabilität nummernunabhängiger interpersoneller Kommunikationsdienste

(1) Erbringt ein Torwächter nummernunabhängige interpersonelle Kommunikationsdienste, die im Benennungsbeschluss nach Artikel 3 Absatz 9 aufgeführt sind, so sorgt er für die Interoperabilität der grundlegenden Funktionen seiner nummernunabhängigen interpersonellen Kommunikationsdienste mit den nummernunabhängigen interpersonellen Kommunikationsdiensten anderer Anbieter, die solche Dienste in der Union anbieten oder anzubieten beabsichtigen, indem er auf Antrag kostenlos die im Sinne der Interoperabilität erforderlichen technischen Schnittstellen oder ähnliche Lösungen bereitstellt.

(2) Der Torwächter sorgt, wenn er diese Funktionen für die eigenen Endnutzer selbst bereitstellt, zumindest für die Interoperabilität der folgenden grundlegenden Funktionen nach Absatz 1:

a) im Anschluss an die Aufführung im Benennungsbeschluss nach Artikel 3 Absatz 9:

- i) Ende-zu-Ende-Textnachrichten zwischen zwei einzelnen Endnutzern;
- ii) Austausch von Bildern, Sprachnachrichten, Videos und anderen angehängten Dateien bei der Ende-zu-Ende-Kommunikation zwischen zwei einzelnen Endnutzern;

b) innerhalb von zwei Jahren nach der Benennung:

- i) Ende-zu-Ende-Textnachrichten innerhalb von Gruppen einzelner Endnutzer;
- ii) Austausch von Bildern, Sprachnachrichten, Videos und anderen angehängten Dateien bei der Ende-zu-Ende-Kommunikation zwischen einer Gruppenunterhaltung und einem einzelnen Endnutzer;

c) innerhalb von vier Jahren nach der Benennung:

- i) Ende-zu-Ende-Sprachanrufe zwischen zwei einzelnen Endnutzern;
- ii) Ende-zu-Ende-Videoanrufe zwischen zwei einzelnen Endnutzern;
- iii) Ende-zu-Ende-Sprachanrufe zwischen einer Gruppenunterhaltung und einem einzelnen Endnutzer;
- iv) Ende-zu-Ende-Videoanrufe zwischen einer Gruppenunterhaltung und einem einzelnen Endnutzer.

(3) Das Sicherheitsniveau, gegebenenfalls einschließlich der Ende-zu-Ende-Verschlüsselung, das der Torwächter seinen eigenen Endnutzern bietet, muss bei allen interoperablen Diensten beibehalten werden.

(4) Der Torwächter veröffentlicht ein Referenzangebot mit den technischen Einzelheiten und allgemeinen Bedingungen für die Interoperabilität mit seinen nummernunabhängigen interpersonellen Kommunikationsdiensten, einschließlich der erforderlichen Einzelheiten zum Sicherheitsniveau und zur Ende-zu-Ende-Verschlüsselung. Der Torwächter veröffentlicht dieses Referenzangebot innerhalb der in Artikel 3 Absatz 10 festgelegten Frist und aktualisiert es erforderlichenfalls.

(5) Nach der Veröffentlichung des Referenzangebots gemäß Absatz 4 kann jeder Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste, der solche Dienste in der Union anbietet oder anzubieten beabsichtigt, Interoperabilität mit den vom Torwächter erbrachten nummernunabhängigen interpersonellen Kommunikationsdiensten beantragen. Ein solcher Antrag kann sich auf einige oder alle der in Absatz 2 aufgeführten grundlegenden Funktionen erstrecken. Der Torwächter kommt jedem zumutbaren Antrag auf Interoperabilität innerhalb von drei Monaten nach Eingang des Antrags nach, indem er die beantragten grundlegenden Funktionen bereitstellt.

(6) Die Kommission kann die Fristen für die Einhaltung der Verpflichtungen nach Absatz 2 oder 5 auf begründeten Antrag des Torwächters ausnahmsweise verlängern, wenn der Torwächter nachweist, dass dies zur Gewährleistung wirksamer Interoperabilität und zur Aufrechterhaltung des erforderlichen Sicherheitsniveaus, gegebenenfalls einschließlich Ende-zu-Ende-Verschlüsselung, erforderlich ist.

(7) Den Endnutzern der nummernunabhängigen interpersonellen Kommunikationsdienste des Torwächters und des antragstellenden Anbieters nummernunabhängiger interpersoneller Kommunikationsdienste bleibt

freigestellt, ob sie sich für die Nutzung der interoperablen grundlegenden Funktionen, die der Torwächter gemäß Absatz 1 bereitstellen kann, entscheiden.

(8) Nur diejenigen personenbezogenen Daten von Endnutzern, die für wirksame Interoperabilität unbedingt erforderlich sind, werden vom Torwächter erhoben und mit dem Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste, der einen Antrag auf Interoperabilität stellt, ausgetauscht. Bei der Erhebung und dem Austausch der personenbezogenen Daten von Endnutzern sind die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG vollumfänglich einzuhalten.

(9) Der Torwächter wird nicht daran gehindert, Maßnahmen zu ergreifen, um sicherzustellen, dass Dritte, die nummernunabhängige interpersonelle Kommunikationsdienste erbringen und Interoperabilität beantragen, die Integrität, die Sicherheit und den Schutz der Privatsphäre seiner Dienste nicht gefährden, sofern diese Maßnahmen unbedingt erforderlich und angemessen sind und vom Torwächter hinreichend begründet werden.

Artikel 8 Einhaltung der Verpflichtungen durch Torwächter

(1) Der Torwächter hat die Einhaltung der Verpflichtungen aus den Artikeln 5, 6 und 7 dieser Verordnung sicherzustellen und weist diese nach. Die Maßnahmen, die der Torwächter ergreift, um die Einhaltung der genannten Artikel sicherzustellen, müssen dazu führen, dass die Zielsetzungen dieser Verordnung und der jeweiligen Verpflichtung wirksam erreicht werden. Der Torwächter stellt sicher, dass diese Maßnahmen im Einklang mit dem anwendbaren Recht, insbesondere der Verordnung (EU) 2016/679, der Richtlinie 2002/58/EG, den Rechtsvorschriften in Bezug auf Cybersicherheit, Verbraucherschutz, Produktsicherheit sowie den Anforderungen an die Barrierefreiheit durchgeführt werden.

(2) Die Kommission kann von Amts wegen oder auf Antrag des Torwächters gemäß Absatz 3 des vorliegenden Artikels ein Verfahren nach Artikel 20 einleiten.

Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Maßnahmen festgelegt werden, die der betreffende Torwächter zu ergreifen hat, um den Verpflichtungen aus Artikel 6 und 7 wirksam nachzukommen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 50 Absatz 2 genannten Beratungsverfahren erlassen innerhalb von sechs Monaten nach Einleitung des Verfahrens nach Artikel 20.

Leitet die Kommission von Amts wegen ein Verfahren wegen Umgehung nach Artikel 13 ein, so können diese Maßnahmen die Verpflichtungen aus den Artikeln 5, 6 und 7 betreffen.

(3) Ein Torwächter kann die Kommission ersuchen, ein Verfahren einzuleiten, um festzustellen, ob das Ziel der betreffenden Verpflichtung durch die Maßnahmen, die der Torwächter zur Gewährleistung der Einhaltung der Artikel 6 und 7 zu ergreifen beabsichtigt oder ergriffen hat, in Anbetracht der besonderen Umstände des Torwächters wirksam erreicht wird. Die Kommission entscheidet nach eigenem Ermessen über die Einleitung eines solchen Verfahrens, unter Wahrung der Grundsätze der Gleichbehandlung, der Verhältnismäßigkeit und der guten Verwaltungspraxis.

Der Torwächter fügt seinem Ersuchen einen mit Gründen versehenen Schriftsatz bei, in dem er die Maßnahmen erläutert, die er zu ergreifen beabsichtigt oder ergriffen hat. Darüber hinaus stellt der Torwächter eine nichtvertrauliche Fassung seines mit Gründen versehenen Schriftsatzes zur Verfügung, die gemäß Absatz 6 an Dritte weitergegeben werden kann.

(4) Die Absätze 2 und 3 des vorliegenden Artikels lassen die Befugnisse der Kommission nach den Artikeln 29, 30 und 31 unberührt.

(5) Im Hinblick auf den Erlass eines Beschlusses nach Absatz 2 gibt die Kommission dem Torwächter innerhalb von drei Monaten nach Einleitung des Verfahrens nach Artikel 20 ihre vorläufige Beurteilung bekannt. In dieser vorläufigen Beurteilung erläutert die Kommission, welche Maßnahmen sie zu ergreifen beabsichtigt bzw. der betreffende Torwächter ihrer Ansicht nach ergreifen sollte, um der vorläufigen Beurteilung wirksam Rechnung zu tragen.

(6) Um interessierten Dritten wirksam Gelegenheit zur Stellungnahme zu geben, veröffentlicht die Kommission bei Mitteilung ihrer vorläufigen Beurteilung an den Torwächter nach Absatz 5 oder so bald wie möglich danach eine nichtvertrauliche Zusammenfassung des Falls und der Maßnahmen, die sie zu ergreifen beabsichtigt oder

die der betreffende Torwächter ihrer Ansicht nach ergreifen sollte. Die Kommission legt für die Abgabe der Stellungnahmen einen angemessenen Zeitraum fest.

(7) Bei der Festlegung der Maßnahmen nach Absatz 2 stellt die Kommission sicher, dass die Ziele dieser Verordnung und der betreffenden Verpflichtung durch diese Maßnahmen wirksam erreicht werden und die Maßnahmen in Anbetracht der besonderen Umstände des Torwächters und der betreffenden Dienstleistung verhältnismäßig sind.

(8) Für die Zwecke der Festlegung der Verpflichtungen nach Artikel 6 Absätze 11 und 12 prüft die Kommission auch, ob die beabsichtigten bzw. durchgeführten Maßnahmen sicherstellen, dass kein Ungleichgewicht zwischen den Rechten und Pflichten der gewerblichen Nutzer mehr besteht und dass die Maßnahmen dem Torwächter keinen Vorteil verschaffen, der in Anbetracht seiner Dienstleistung für die gewerblichen Nutzer unverhältnismäßig wäre.

(9) Bei Verfahren nach Absatz 2 kann die Kommission auf Antrag oder von Amts wegen beschließen, das Verfahren wieder aufzunehmen, wenn

- a) sich der Sachverhalt, auf den sich der Beschluss stützte, in einem wesentlichen Punkt geändert hat oder
- b) der Beschluss auf unvollständigen, unrichtigen oder irreführenden Angaben beruhte oder
- c) die im Beschluss genannten Maßnahmen nicht wirksam sind.

GG - Grundgesetz für die Bundesrepublik Deutschland

I. Die Grundrechte

Art 1

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Art 2

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Art 5

(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

(2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.

(3) Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung.

Art 10

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes

oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Art 13

(1) Die Wohnung ist unverletzlich.

(2) Durchsuchungen dürfen nur durch den Richter, bei Gefahr im Verzuge auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden.

(3) Begründen bestimmte Tatsachen den Verdacht, daß jemand eine durch Gesetz einzeln bestimmte besonders schwere Straftat begangen hat, so dürfen zur Verfolgung der Tat auf Grund richterlicher Anordnung technische Mittel zur akustischen Überwachung von Wohnungen, in denen der Beschuldigte sich vermutlich aufhält, eingesetzt werden, wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre. Die Maßnahme ist zu befristen. Die Anordnung erfolgt durch einen mit drei Richtern besetzten Spruchkörper. Bei Gefahr im Verzuge kann sie auch durch einen einzelnen Richter getroffen werden.

(4) Zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, dürfen technische Mittel zur Überwachung von Wohnungen nur auf Grund richterlicher Anordnung eingesetzt werden. Bei Gefahr im Verzuge kann die Maßnahme auch durch eine andere gesetzlich bestimmte Stelle angeordnet werden; eine richterliche Entscheidung ist unverzüglich nachzuholen.

(5) Sind technische Mittel ausschließlich zum Schutze der bei einem Einsatz in Wohnungen tätigen Personen vorgesehen, kann die Maßnahme durch eine gesetzlich bestimmte Stelle angeordnet werden. Eine anderweitige Verwertung der hierbei erlangten Erkenntnisse ist nur zum Zwecke der Strafverfolgung oder der Gefahrenabwehr und nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzuge ist die richterliche Entscheidung unverzüglich nachzuholen.

(6) Die Bundesregierung unterrichtet den Bundestag jährlich über den nach Absatz 3 sowie über den im Zuständigkeitsbereich des Bundes nach Absatz 4 und, soweit richterlich überprüfungsbedürftig, nach Absatz 5 erfolgten Einsatz technischer Mittel. Ein vom Bundestag gewähltes Gremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. Die Länder gewährleisten eine gleichwertige parlamentarische Kontrolle.

(7) Eingriffe und Beschränkungen dürfen im übrigen nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, auf Grund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere zur Behebung der Raumnot, zur Bekämpfung von Seuchengefahr oder zum Schutze gefährdeter Jugendlicher vorgenommen werden.

Art 14

(1) Das Eigentum und das Erbrecht werden gewährleistet. Inhalt und Schranken werden durch die Gesetze bestimmt.

(2) Eigentum verpflichtet. Sein Gebrauch soll zugleich dem Wohle der Allgemeinheit dienen.

(3) Eine Enteignung ist nur zum Wohle der Allgemeinheit zulässig. Sie darf nur durch Gesetz oder auf Grund eines Gesetzes erfolgen, das Art und Ausmaß der Entschädigung regelt. Die Entschädigung ist unter gerechter Abwägung der Interessen der Allgemeinheit und der Beteiligten zu bestimmen. Wegen der Höhe der Entschädigung steht im Streitfalle der Rechtsweg vor den ordentlichen Gerichten offen.

Art 87f

(1) Nach Maßgabe eines Bundesgesetzes, das der Zustimmung des Bundesrates bedarf, gewährleistet der Bund im Bereich des Postwesens und der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen.

(2) Dienstleistungen im Sinne des Absatzes 1 werden als privatwirtschaftliche Tätigkeiten durch die aus dem Sondervermögen Deutsche Bundespost hervorgegangenen Unternehmen und durch andere private Anbieter erbracht. Hoheitsaufgaben im Bereich des Postwesens und der Telekommunikation werden in bundeseigener Verwaltung ausgeführt.

(3) Unbeschadet des Absatzes 2 Satz 2 führt der Bund in der Rechtsform einer bundesunmittelbaren Anstalt des öffentlichen Rechts einzelne Aufgaben in Bezug auf die aus dem Sondervermögen Deutsche Bundespost hervorgegangenen Unternehmen nach Maßgabe eines Bundesgesetzes aus.

TKG – Telekommunikationsgesetz

Teil 1 Allgemeine Vorschriften

§ 1 Zweck des Gesetzes, Anwendungsbereich

(1) Zweck dieses Gesetzes ist es, durch technologie neutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten.

(2) Diesem Gesetz unterliegen alle Unternehmen oder Personen, die im Geltungsbereich dieses Gesetzes Telekommunikationsnetze oder Telekommunikationsanlagen betreiben oder Telekommunikationsdienste erbringen sowie die weiteren, nach diesem Gesetz Berechtigten und Verpflichteten.

§ 2 Ziele und Grundsätze der Regulierung

(1) Die Regulierung der Telekommunikation ist eine hoheitliche Aufgabe des Bundes.

(2) Ziele der Regulierung sind

1. die Sicherstellung der Konnektivität sowie die Förderung des Zugangs zu und der Nutzung von Netzen mit sehr hoher Kapazität durch alle Bürger und Unternehmen,

2. die Sicherstellung eines chancengleichen Wettbewerbs und die Förderung nachhaltig wettbewerbsorientierter Märkte der Telekommunikation im Bereich der Telekommunikationsdienste und -netze – einschließlich eines effizienten infrastrukturasierten Wettbewerbs – sowie der zugehörigen Einrichtungen und Dienste, auch in der Fläche,

3. die Wahrung der Nutzer-, insbesondere der Verbraucherinteressen auf dem Gebiet der Telekommunikation; die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn (Bundesnetzagentur) und andere nach diesem Gesetz zuständige Behörden fördern die Interessen der Nutzer, indem sie

a) die Konnektivität, die breite Verfügbarkeit sowie den beschleunigten Ausbau von Netzen mit sehr hoher Kapazität wie auch von Telekommunikationsdiensten sicherstellen und deren Nutzung fördern,

b) auf größtmögliche Vorteile der Nutzer in Bezug auf Auswahl, Preise und Qualität auf der Grundlage eines wirksamen Wettbewerbs hinwirken,

c) die Interessen der öffentlichen Sicherheit wahren und die Sicherheit der Netze und Dienste gewährleisten,

d) gleichwertige Lebensverhältnisse in städtischen und ländlichen Räumen sowie ein hohes gemeinsames Schutzniveau für die Endnutzer sicherstellen und die Bedürfnisse – wie beispielsweise erschwingliche Preise – bestimmter gesellschaftlicher Gruppen, insbesondere von Endnutzern mit Behinderungen, älteren Endnutzern und Endnutzern mit besonderen sozialen Bedürfnissen, sowie die Wahlmöglichkeiten und den gleichwertigen Zugang für Endnutzer mit Behinderungen berücksichtigen,

e) sicherstellen, dass im Bereich der Telekommunikation keine Wettbewerbsverzerrungen oder -beschränkungen bestehen,

4. die Förderung der Entwicklung des Binnenmarktes der Europäischen Union, indem die Bundesnetzagentur und andere nach diesem Gesetz zuständige Behörden verbleibende Hindernisse für Investitionen in Telekommunikationsnetze, Telekommunikationsdienste, zugehörige Einrichtungen und zugehörige Dienste sowie für deren Bereitstellung in der gesamten Europäischen Union abbauen helfen und die Schaffung konvergierender Bedingungen hierfür erleichtern, gemeinsame Regeln und vorhersehbare Regulierungskonzepte entwickeln und ferner offene Innovationen, den Aufbau und die Entwicklung transeuropäischer Netze, die Bereitstellung, Verfügbarkeit und Interoperabilität europaweiter Dienste und die durchgehende Konnektivität fördern,

5. die Sicherstellung einer effizienten und störungsfreien Nutzung von Frequenzen, auch unter Berücksichtigung der Belange des Rundfunks.

(3) Die Bundesnetzagentur und andere nach diesem Gesetz zuständige Behörden wenden bei der Verfolgung der in Absatz 2 festgelegten Ziele objektive, transparente, nichtdiskriminierende und verhältnismäßige Regulierungsgrundsätze an, indem sie unter anderem

1. die Vorhersehbarkeit der Regulierung dadurch fördern, dass sie über angemessene Überprüfungszeiträume und im Wege der Zusammenarbeit untereinander, mit dem GEREK, mit der Gruppe für Frequenzpolitik und mit der Kommission ein einheitliches Regulierungskonzept wahren,

2. gewährleisten, dass Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten unter vergleichbaren Umständen nicht diskriminiert werden,

3. das Unionsrecht in technologieutraler Weise anwenden, soweit dies mit der Erfüllung der Ziele des Absatzes 2 vereinbar ist,

4. effiziente Investitionen und Innovationen im Bereich neuer und verbesserter Infrastrukturen auch dadurch fördern, dass sie dafür sorgen, dass bei jeglicher Zugangsverpflichtung dem Risiko der investierenden Unternehmen gebührend Rechnung getragen wird und dass sie verschiedene kommerzielle Vereinbarungen zur Diversifizierung des Investitionsrisikos zwischen Investoren untereinander sowie zwischen Investoren und Zugangsnachfragern zulassen, während sie gleichzeitig gewährleisten, dass der Wettbewerb auf dem Markt und der Grundsatz der Nichtdiskriminierung gewahrt werden,

5. die vielfältigen Bedingungen im Zusammenhang mit Infrastrukturen, Wettbewerb, Gegebenheiten der Endnutzer und insbesondere der Verbraucher, die in den verschiedenen geografischen Gebieten innerhalb der Bundesrepublik Deutschland vorhanden sind, gebührend berücksichtigen und

6. regulatorische Vorabverpflichtungen nur dann auferlegen, wenn es keinen wirksamen und nachhaltigen Wettbewerb im Interesse der Endnutzer gibt und gewährleisten, dass diese Verpflichtungen gelockert oder aufgehoben werden, sobald es einen solchen Wettbewerb gibt.

(4) Die Vorschriften des Gesetzes gegen Wettbewerbsbeschränkungen bleiben, soweit nicht durch dieses Gesetz ausdrücklich abschließende Regelungen getroffen werden, anwendbar. Die Aufgaben und Zuständigkeiten der Kartellbehörden bleiben unberührt.

(5) Die hoheitlichen Rechte des Bundesministeriums der Verteidigung bleiben unberührt.

(6) Die Belange der Behörden und Organisationen mit Sicherheitsaufgaben des Bundes und der Länder sind zu berücksichtigen, ebenso nach Maßgabe dieses Gesetzes die Belange der Bundeswehr.

(7) Die Belange des Rundfunks und vergleichbarer Telemedien sind unabhängig von der Art der Übertragung zu berücksichtigen. Die medienrechtlichen Bestimmungen der Länder bleiben unberührt.

§ 3 Begriffsbestimmungen

Im Sinne dieses Gesetzes ist oder sind

1. „Anbieter von Telekommunikationsdiensten“ jeder, der Telekommunikationsdienste erbringt;

2. „Anruf“ eine über einen öffentlich zugänglichen interpersonellen Telekommunikationsdienst aufgebaute Verbindung, die eine zweiseitige oder mehrseitige Sprachkommunikation ermöglicht;

3. „Anschlusskennung“ eine Rufnummer oder andere eindeutige und einmalige Zeichenfolge, die einem bestimmten Anschlussinhaber dauerhaft zugewiesen ist und die Telekommunikation über den jeweiligen Anschluss eindeutig und gleichbleibend kennzeichnet;

4. „Anwendungs-Programmierschnittstelle“ die Software-Schnittstelle zwischen Anwendungen, die von Sendeanstalten oder Diensteanbietern zur Verfügung gestellt werden, und den Anschlüssen in den erweiterten digitalen Fernsehempfangsgeräten für digitale Fernseh- und Hörfunkdienste;

5. „Auskunftsdienste“ bundesweit jederzeit telefonisch erreichbare Dienste, insbesondere des Rufnummernbereichs 118, die ausschließlich der Weitergabe von Rufnummer, Name, Anschrift sowie zusätzlichen Angaben von Endnutzern dienen; die Weitervermittlung zu einem erfragten Endnutzer oder Dienst kann Bestandteil des Auskunftsdienstes sein;

6. „Bestandsdaten“ Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste;

§ 80 Informationen über Breitbandausbau

(1) Informationen über den Breitbandausbau beruhen auf einer von der zentralen Informationsstelle des Bundes durchzuführenden geografischen Erhebung zur örtlichen Verfügbarkeit öffentlicher Telekommunikationsnetze, die sie in regelmäßigen Abständen, jedoch mindestens einmal im Jahr durchführt.

(2) Die Informationen über den Breitbandausbau umfassen eine gebiets- und haushaltsbezogene Übersicht über die örtliche Verfügbarkeit von öffentlichen Telekommunikationsnetzen sowie Informationen über Gebiete, in denen der Ausbau öffentlicher Telekommunikationsnetze öffentlich gefördert wird, soweit diese Informationen der zentralen Informationsstelle des Bundes vorliegen. Die Übersicht muss hinreichende Details zu lokalen Gegebenheiten sowie ausreichende Informationen über die Dienstqualität und deren Parameter enthalten.

(3) Die zentrale Informationsstelle des Bundes muss sicherstellen, dass die Informationen über den Breitbandausbau unter Wahrung von Betriebs- und Geschäftsgeheimnissen vertraulich behandelt werden.

(4) Die zentrale Informationsstelle des Bundes stellt Endnutzern ein Informationswerkzeug bereit, damit diese die Verfügbarkeit von Netzanbindungen in verschiedenen Gebieten mit einem Detailgrad ermitteln können, der geeignet ist, ihnen bei der Auswahl des Betreibers oder Diensteanbieters zu helfen. Satz 1 gilt nicht, wenn ein Informationswerkzeug, das die Anforderungen des Satzes 1 erfüllt, auf dem Markt zur Verfügung steht.

§ 84 Gebiete mit Ausbaufizit

(1) Für allgemeine Planungs- und Förderzwecke kann die zentrale Informationsstelle des Bundes geographisch eindeutig abgegrenzte Gebiete ausweisen, für die aufgrund der gemäß den §§ 80 und 81 erfassten Informationen festgestellt wird, dass während des Zeitraums, den die Informationen über künftigen Netzausbau abdecken,

1. kein Unternehmen und keine öffentliche Stelle ein Netz mit sehr hoher Kapazität ausbaut oder auszubauen plant und

2. keine bedeutsame Modernisierung oder Erweiterung des Telekommunikationsnetzes mit dem Ziel höherer Download-Geschwindigkeiten geplant ist.

Die zentrale Informationsstelle des Bundes veröffentlicht, welche Gebiete sie gemäß Satz 1 ausgewiesen hat.

(2) Die zentrale Informationsstelle des Bundes kann Unternehmen und öffentliche Stellen ersuchen, ihre Absicht zu bekunden, während des betreffenden Zeitraums der Vorausschau Netze mit sehr hoher Kapazität innerhalb des gemäß Absatz 1 Satz 1 ausgewiesenen Gebietes auszubauen. Bekundet ein Unternehmen oder eine öffentliche Stelle daraufhin die Absicht im Sinne des Satzes 1, kann die zentrale Informationsstelle des Bundes andere Unternehmen und öffentliche Stellen auffordern, deren etwaige Absicht zu bekunden,

1. in diesem Gebiet Netze mit sehr hoher Kapazität aufzubauen oder

2. eine bedeutsame Modernisierung oder Erweiterung ihres Telekommunikationsnetzes mit dem Ziel höherer Download-Geschwindigkeiten vorzunehmen.

Die zentrale Informationsstelle des Bundes gibt an, welche Informationen in der Absichtsbekundung enthalten sein müssen, damit sie mindestens den Anforderungen des § 80 Absatz 2 Satz 2 entspricht. Die zentrale Informationsstelle des Bundes teilt allen Unternehmen oder öffentlichen Stellen auf Anfrage mit, ob das ausgewiesene Gebiet nach den gemäß den §§ 80 und 81 erhobenen Informationen von einem Netz der nächsten Generation unter Nennung der Größenordnung der jeweiligen Download-Geschwindigkeiten versorgt wird oder wahrscheinlich versorgt werden wird, soweit diese Informationen der zentralen Informationsstelle des Bundes vorliegen.

(3) Maßnahmen nach Absatz 2 werden nach einem effizienten, objektiven, transparenten und diskriminierungsfreien Verfahren durchgeführt, von dem kein Unternehmen von vornherein ausgeschlossen ist

§ 156 Recht auf Versorgung mit Telekommunikationsdiensten

(1) Endnutzer haben gegenüber Unternehmen, die durch die Bundesnetzagentur nach § 161 Absatz 1, 2 oder 3 verpflichtet worden sind (Diensteverpflichtete), einen Anspruch auf Versorgung mit den von der Verpflichtung umfassten Telekommunikationsdiensten nach § 157 Absatz 2, einschließlich des hierfür notwendigen Anschlusses an ein öffentliches Telekommunikationsnetz, an ihrer Hauptwohnung oder an ihrem Geschäftsort, soweit diese sich in dem von der Verpflichtung umfassten Gebiet befinden. Der Diensteverpflichtete hat die Versorgung innerhalb der von der Bundesnetzagentur festgelegten Frist des § 161 Absatz 2 Satz 4 nach Geltendmachung durch den Endnutzer sicherzustellen.

(2) Diensteverpflichtete haben die Leistungen so anzubieten und zu erbringen, dass Endnutzer nicht für Einrichtungen oder Telekommunikationsdienste zu zahlen haben, die nicht notwendig oder für die gewählten Telekommunikationsdienste nicht erforderlich sind.

(3) Diensteverpflichtete haben der Bundesnetzagentur auf Anfrage angemessene und aktuelle Informationen über ihre Leistungen bei der Versorgung mit Telekommunikationsdiensten nach § 157 Absatz 2 mitzuteilen. Dabei werden die Parameter, Definitionen und Messverfahren für die Dienstqualität zugrunde gelegt, die in Anhang X der Richtlinie (EU) 2018/1972 dargelegt sind.

(4) Auf Antrag eines Verbrauchers kann die Versorgung mit Telekommunikationsdiensten gemäß § 157 Absatz 2 auf Sprachkommunikationsdienste beschränkt werden.

§ 157 Verfügbarkeit der Telekommunikationsdienste

(1) Die Bundesnetzagentur überwacht in regelmäßigen Abständen die Verfügbarkeit eines Mindestangebots gemäß Absatz 2. Sie berücksichtigt hierbei die Ergebnisse der Erhebungen der zentralen Informationsstelle des Bundes gemäß den §§ 80, 81 und 84. Die Bundesnetzagentur berichtet in dem Jahresbericht nach § 196 über die Ergebnisse der Überwachung nach Satz 1.

(2) Mindestens verfügbar sein müssen Sprachkommunikationsdienste sowie ein schneller Internetzugangsdienst für eine angemessene soziale und wirtschaftliche Teilhabe im Sinne des Absatzes 3, einschließlich des hierfür notwendigen Anschlusses an ein öffentliches Telekommunikationsnetz an einem festen Standort.

(3) In einer Rechtsverordnung des Bundesministeriums für Verkehr und digitale Infrastruktur, die des Einvernehmens mit dem Ausschuss für Verkehr und digitale Infrastruktur des Deutschen Bundestages bedarf, wird mit Zustimmung des Bundesrates festgelegt, welche Anforderungen ein Internetzugangsdienst sowie ein Sprachkommunikationsdienst nach Absatz 2 erfüllen müssen. Bei der Festlegung der Anforderungen an den Internetzugangsdienst nach Satz 1 werden insbesondere die von mindestens 80 Prozent der Verbraucher im Bundesgebiet genutzte Mindestbandbreite, Uploadrate und Latenz sowie weitere nationale Gegebenheiten, wie die Auswirkungen der festgelegten Qualität auf Anreize zum privatwirtschaftlichen Breitbandausbau und zu Breitbandfördermaßnahmen, berücksichtigt. Der Internetzugangsdienst muss stets mindestens die in Anhang V der Richtlinie (EU) 2018/1972 in der jeweils gültigen Fassung aufgeführten Dienste, Teleheimarbeit einschließlich Verschlüsselungsverfahren im üblichen Umfang und eine für Verbraucher marktübliche Nutzung von Online-Inhaltediensten ermöglichen. Die nach Satz 1 festzulegende Uploadrate und Latenz können niedriger, als die von 80 Prozent der Verbraucher im Bundesgebiet genutzten Werte sein, wenn tatsächlich nachgewiesen ist, dass die in Satz 3 genannten Dienste auch bei geringeren Vorgaben beim Endnutzer funktionieren. In einer Rechtsverordnung nach Satz 1 können kürzere als die in § 160 und § 161 genannten Fristen festgelegt werden, wenn durch eine Digitalisierung der Verfahrensabläufe eine Beschleunigung erreicht werden konnte.

(4) Die Rechtsverordnung nach Absatz 3 ist innerhalb von sechs Monaten nach Inkrafttreten dieser Regelung zu erlassen. Das Bundesministerium für Verkehr und digitale Infrastruktur hat die festgelegten Anforderungen jährlich zu überprüfen. Über das Ergebnis unterrichtet es den Ausschuss für Verkehr und digitale Infrastruktur des Deutschen Bundestages.

(5) Das Bundesministerium für Verkehr und digitale Infrastruktur kann die Ermächtigung nach Absatz 3 sowie die Pflichten nach Absatz 4 durch Rechtsverordnung auf die Bundesnetzagentur übertragen. Eine Rechtsverordnung der Bundesnetzagentur nach Satz 1 bedarf des Einvernehmens mit dem Bundesministerium für Verkehr und digitale Infrastruktur und mit dem Ausschuss für Verkehr und digitale Infrastruktur des Deutschen Bundestages und der Zustimmung des Bundesrates. Das Ergebnis des Prüfberichts der Bundesnetzagentur nach Absatz 4 bedarf des Einvernehmens mit dem Bundesministerium für Verkehr und digitale Infrastruktur und mit dem Ausschuss für Verkehr und digitale Infrastruktur des Deutschen Bundestages.

§ 158 Erschwinglichkeit der Telekommunikationsdienste

(1) Telekommunikationsdienste nach § 157 Absatz 2, einschließlich des hierfür notwendigen Anschlusses an ein öffentliches Telekommunikationsnetz an einem festen Standort, müssen Verbrauchern zu einem erschwinglichen Preis angeboten werden. Die Bundesnetzagentur veröffentlicht nach Anhörung der betroffenen Kreise Grundsätze über die Ermittlung erschwinglicher Preise für Telekommunikationsdienste nach § 157 Absatz 2, einschließlich des hierfür notwendigen Anschlusses an ein öffentliches Telekommunikationsnetz an einem festen Standort, innerhalb von sechs Monaten nach Inkrafttreten dieser Regelung.

(2) Die Bundesnetzagentur überwacht die Entwicklung und Höhe der Preise für Telekommunikationsdienste nach § 157 Absatz 2, einschließlich des hierfür notwendigen Anschlusses an ein öffentliches Telekommunikationsnetz an einem festen Standort.

§ 159 Beitrag von Unternehmen zur Versorgung mit Telekommunikationsdiensten

Jeder Anbieter, der auf dem sachlichen Markt der Versorgung mit Telekommunikationsdiensten nach § 157 Absatz 2 im Geltungsbereich dieses Gesetzes tätig ist, ist verpflichtet, dazu beizutragen, dass die Versorgung mit Telekommunikationsdiensten nach den §§ 157 und 158 erbracht werden kann. Die Verpflichtung nach Satz 1 ist nach Maßgabe der Bestimmungen dieses Abschnitts zu erfüllen.

§ 160 Feststellung der Unterversorgung

(1) Stellt die Bundesnetzagentur im Rahmen ihrer Überwachung gemäß § 157 Absatz 1 und § 158 Absatz 2 fest, dass einer der nachfolgenden Umstände vorliegt, so veröffentlicht sie innerhalb von zwei Monaten nach erstmaliger Kenntniserlangung diese Feststellung:

1. eine Versorgung mit Telekommunikationsdiensten nach § 157 Absatz 2 wird weder aktuell noch in objektiv absehbarer Zeit angemessen, ausreichend oder nach § 158 Absatz 1 zu einem erschwinglichen Endnutzerpreis erbracht,
2. es ist zu besorgen, dass eine Versorgung mit Telekommunikationsdiensten nach § 157 Absatz 2 zukünftig nicht mehr gewährleistet sein wird.

Die Bundesnetzagentur kann die ihr gesetzte Frist für die Veröffentlichung der Unterversorgungsfeststellung nach Satz 1 bei außergewöhnlichen Umständen um bis zu einen Monat überschreiten. Die Umstände sind hinreichend zu begründen.

(2) Stellt die Bundesnetzagentur im Rahmen ihrer Feststellung nach Absatz 1 in dem von der Feststellung umfassten Gebiet einen tatsächlichen Bedarf für eine Versorgung mit den nach § 157 Absatz 2 mindestens verfügbaren Telekommunikationsdiensten fest, kündigt sie mit der Veröffentlichung der Unterversorgungsfeststellung an, nach den Vorschriften des § 161 Absatz 2 vorzugehen, sofern kein Unternehmen innerhalb eines Monats nach Veröffentlichung der Unterversorgungsfeststellung schriftlich oder elektronisch gegenüber der Bundesnetzagentur zusagt, sich zur Versorgung mit Telekommunikationsdiensten nach § 157 Absatz 2 und § 158 Absatz 1 ohne Ausgleich nach § 162 zu verpflichten.

§ 172 Daten für Auskunftersuchen der Sicherheitsbehörden

(1) Wer nummerngebundene interpersonelle Telekommunikationsdienste, Internetzugangsdienste oder Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, erbringt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 173 und 174 vor der Freischaltung folgende Daten zu erheben und unverzüglich zu speichern, auch, soweit diese Daten für betriebliche Zwecke nicht erforderlich sind:

1. die Rufnummern,
2. andere von ihm vergebene Anschlusskennungen,
3. den Namen und die Anschrift des Anschlussinhabers,
4. bei natürlichen Personen deren Geburtsdatum,
5. bei Festnetzanschlüssen die Anschrift des Anschlusses,
6. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
7. das Datum der Vergabe der Rufnummer und, soweit abweichend, das Datum des Vertragsbeginns.

Das Datum der Beendigung der Zuordnung der Rufnummer und, sofern davon abweichend, das Datum des Vertragsendes sind bei Bekanntwerden ebenfalls zu speichern. Die Sätze 1 und 2 gelten auch, sofern die Daten nicht in Endnutzerverzeichnisse eingetragen werden. Für das Auskunftsverfahren nach § 174 ist die Form der Datenspeicherung freigestellt.

(2) Anbieter von im Voraus bezahlten Mobilfunkdiensten haben die Richtigkeit der nach Absatz 1 Satz 1 Nummer 3 und 4 erhobenen Daten, sofern die Daten in den vorgelegten Dokumenten oder eingesehenen Registern oder Verzeichnissen enthalten sind, vor der Freischaltung zu überprüfen durch

1. Vorlage eines Ausweises im Sinne des § 2 Absatz 1 des Personalausweisgesetzes,
2. Vorlage eines Passes im Sinne des § 1 Absatz 2 des Passgesetzes,
3. Vorlage eines sonstigen gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, wozu insbesondere auch ein nach ausländerrechtlichen Bestimmungen anerkannter oder zugelassener Pass, Personalausweis oder Pass- oder Ausweisersatz zählt,
4. Vorlage eines Aufenthaltstitels,
5. Vorlage eines Ankunftsnachweises nach § 63a Absatz 1 des Asylgesetzes oder einer Bescheinigung über die Aufenthaltsgestattung nach § 63 Absatz 1 des Asylgesetzes,
6. Vorlage einer Bescheinigung über die Aussetzung der Abschiebung nach § 60a Absatz 4 des Aufenthaltsgesetzes oder
7. Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den darin enthaltenen Daten, sofern es sich bei dem Anschlussinhaber um eine juristische Person oder Personengesellschaft handelt.

Dazu darf ihnen abweichend von § 20 Absatz 2 Satz 2 des Personalausweisgesetzes und § 18 Absatz 3 Satz 2 des Passgesetzes ein Vertriebspartner eine elektronische Kopie des Personalausweises oder Reisepasses übersenden. Die Überprüfung kann auch durch andere geeignete Verfahren erfolgen; die Bundesnetzagentur legt nach Anhörung der betroffenen Kreise fest, welche anderen Verfahren zur Überprüfung geeignet sind, wobei jeweils zum Zweck der Identifikation vor Freischaltung der vertraglich vereinbarten Mobilfunkdienstleistung ein Dokument im Sinne des Satzes 1 genutzt werden muss. Verpflichtete haben vor Nutzung anderer geeigneter Verfahren die Feststellung der Übereinstimmung eines Verfahrens mit der Festlegung der Bundesnetzagentur durch eine Konformitätsbewertungsstelle im Sinne der Begriffsbestimmung in Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30) nachzuweisen, die gemäß jener Verordnung als zur Durchführung der Konformitätsbewertung von anderen geeigneten Verfahren nach Satz 3 akkreditiert worden ist. Die Feststellung darf bei Nutzung des Verfahrens nicht älter als 24 Monate sein. Bei der Überprüfung ist die Art des eingesetzten Verfahrens zu speichern; bei Überprüfung mittels eines Dokumentes im Sinne des Satzes 1 Nummer 1 bis 6 sind ferner Angaben zu Art, Nummer und ausstellender Stelle zu speichern. Für die Identifizierung anhand eines

elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes gilt § 8 Absatz 2 Satz 5 des Geldwäschegesetzes entsprechend.

(3) Die Verpflichtung zur unverzüglichen Speicherung nach Absatz 1 Satz 1 gilt hinsichtlich der Daten nach Absatz 1 Satz 1 Nummer 1, 3, 4 und 7 entsprechend für denjenigen, der nummernunabhängige interpersonelle Telekommunikationsdienste erbringt und dabei Daten nach Absatz 1 Satz 1 Nummer 1, 3, 4 und 7 erhebt, wobei an die Stelle der Daten nach Absatz 1 Satz 1 Nummer 1 die entsprechenden Kennungen des Dienstes und an die Stelle des Anschlussinhabers nach Absatz 1 Satz 1 Nummer 3 der Nutzer des Dienstes tritt.

(4) Wird dem Verpflichteten nach den Absätzen 1 bis 3 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen.

(5) Bedient sich ein Verpflichteter nach den Absätzen 1 bis 3 zur Erhebung der Daten nach Absatz 1 Satz 1 und 2 und Absatz 3 oder Überprüfung der Daten nach Absatz 2 eines Dritten, bleibt er für die Erfüllung der Pflichten nach den Absätzen 1 bis 3 verantwortlich. Es ist dem Dritten verboten, unrichtige Daten zu verwenden oder zu verarbeiten. Werden dem Dritten im Rahmen des üblichen Geschäftsablaufs Änderungen der Daten nach Absatz 1 Satz 1 und 2 und Absatz 3 bekannt, hat er diese dem Anbieter des Telekommunikationsdienstes unverzüglich zu übermitteln.

(6) Die Daten nach den Absätzen 1 bis 3 sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(7) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

DDG Digitale Dienste Gesetz (in der Entwurfsfassung der Bundesregierung)

Teil 1 - Allgemeine Vorschriften

§ 1 Anwendungsbereich, Begriffsbestimmungen

(1) Dieses Gesetz gilt für alle Diensteanbieter nach Absatz 4 Nummer 5, sofern in diesem Gesetz nichts anderes bestimmt ist. Abweichend von Satz 1 gelten die Vorschriften dieses Gesetzes zur Durchsetzung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (ABl. L 186 vom 11.7.2019, S. 57) für Anbieter von Online-Vermittlungsdiensten nach Artikel 2 Nummer 2 und 3 sowie für Anbieter von Online-Suchmaschinen nach Artikel 2 Nummer 5 und 6 dieser Verordnung. Dieses Gesetz gilt nicht für Rundfunk im Sinne der medienrechtlichen Bestimmungen der Länder.

(2) Die inhalts- und vielfaltsbezogenen Anforderungen an digitale Dienste und die hierfür zuständigen Aufsichtsbehörden ergeben sich aus den medienrechtlichen Bestimmungen der Länder. Die Vorschriften des Gesetzes gegen Wettbewerbsbeschränkungen einschließlich dessen §§ 19 bis 20 sowie der Regelungen zu den Aufgaben, Befugnissen und Zuständigkeiten der Kartellbehörden bleiben unberührt.

(3) Dieses Gesetz trifft weder Regelungen im Bereich des internationalen Privatrechts noch regelt es die Zuständigkeit der Gerichte.

(4) Im Sinne dieses Gesetzes ist oder sind

1. „digitaler Dienst“ ein Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1);

2. „Koordinierungsstelle für digitale Dienste“ der nationale Koordinator für digitale Dienste im Sinne des Artikels 49 Absatz 2 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27.10.2022, S. 1; L 310 vom 1.12.2022, S. 17);

3. „drahtloses lokales Netzwerk“ ein Drahtloszugangssystem mit geringer Leistung und geringer Reichweite sowie mit geringem Störungsrisiko für weitere, von anderen Nutzern in unmittelbarer Nähe installierte Systeme dieser Art, das nicht exklusive Grundfrequenzen nutzt;
4. „audiovisuelle Mediendienste“
 - a) audiovisuelle Mediendienste auf Abruf (Nummer 6) und
 - b) die audiovisuelle kommerzielle Kommunikation (Nummer 7);
5. „Diensteanbieter“ Anbieter digitaler Dienste;
6. „audiovisuelle Mediendienste auf Abruf“ nichtlineare audiovisuelle Mediendienste, bei denen der Hauptzweck des Dienstes oder eines trennbaren Teils des Dienstes darin besteht, unter der redaktionellen Verantwortung eines Anbieters von audiovisuellen Mediendiensten der Allgemeinheit Sendungen zur Information, Unterhaltung oder Bildung zum individuellen Abruf zu einem vom Nutzer gewählten Zeitpunkt bereitzustellen;
7. „audiovisuelle kommerzielle Kommunikation“ jede Form der Kommunikation mit Bildern mit oder ohne Ton, die einer Sendung oder einem nutzergenerierten Video gegen Entgelt oder gegen eine ähnliche Gegenleistung oder als Eigenwerbung beigefügt oder darin enthalten ist, wenn die Kommunikation der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren und Dienstleistungen oder der Förderung des Erscheinungsbilds natürlicher oder juristischer Personen, die einer wirtschaftlichen Tätigkeit nachgehen, dient, einschließlich Sponsoring und Produktplatzierung;
8. „Videosharingplattform-Dienste“
 - a) digitale Dienste, bei denen der Hauptzweck oder eine wesentliche Funktion darin besteht, Sendungen oder nutzergenerierte Videos, für die der Diensteanbieter keine redaktionelle Verantwortung trägt, der Allgemeinheit bereitzustellen, wobei der Diensteanbieter die Organisation der Sendungen und der nutzergenerierten Videos, auch mit automatischen Mitteln, bestimmt,
 - b) trennbare Teile digitaler Dienste, wenn für den trennbaren Teil der in Buchstabe a genannte Hauptzweck vorliegt;
9. „Videosharingplattform-Anbieter“ ein Diensteanbieter, der Videosharingplattform-Dienste betreibt;
10. „redaktionelle Verantwortung“ die Ausübung einer wirksamen Kontrolle hinsichtlich der Zusammenstellung der Sendungen und ihrer Bereitstellung mittels eines Katalogs;
11. „Sendung“ eine Abfolge von bewegten Bildern mit oder ohne Ton, die unabhängig von ihrer Länge Einzelbestandteil eines von einem Diensteanbieter erstellten Sendeplans oder Katalogs ist;
12. „nutzergeneriertes Video“ eine von einem Nutzer erstellte Abfolge von bewegten Bildern mit oder ohne Ton, die unabhängig von ihrer Länge einen Einzelbestandteil darstellt und die von diesem Nutzer oder einem anderen Nutzer auf einen Videosharingplattform-Dienst hochgeladen wird;
13. „Mitgliedstaat“ jeder Mitgliedstaat der Europäischen Union und jeder andere Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, für den die Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) (ABl. L 95 vom 15.4.2010, S. 1; L 263 vom 6.10.2010, S. 15), die durch die Richtlinie (EU) 2018/1808 (ABl. L 303 vom 28.11.2018, S. 69) geändert worden ist, gilt;
14. „Drittstaat“ jeder Staat, der nicht Mitgliedstaat ist;
15. „Mutterunternehmen“ ein Unternehmen, das ein oder mehrere Tochterunternehmen kontrolliert;
16. „Tochterunternehmen“ ein Unternehmen, das unmittelbar oder mittelbar von einem Mutterunternehmen kontrolliert wird;

17. „Gruppe“ die Gesamtheit eines Mutterunternehmens und seiner Tochterunternehmen sowie aller anderen mit dem Mutterunternehmen und seinen Tochterunternehmen wirtschaftlich und rechtlich verbundenen Unternehmen.

§ 2 Europäisches Sitzland

(1) Sitzland des Diensteanbieters innerhalb des Geltungsbereichs der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr) (ABl. L 178 vom 17.7.2000, S. 1), die zuletzt durch die Verordnung (EU) 2022/2065 (ABl. L 277 vom 27.10.2022, S. 1 L 310 vom 1.12.2022, S. 17) geändert worden ist, ist der Mitgliedstaat, in dessen Hoheitsgebiet der Diensteanbieter niedergelassen ist.

(2) Abweichend von Absatz 1 gilt bei audiovisuellen Mediendiensten im Anwendungsbereich der Richtlinie 2010/13/EU derjenige Mitgliedstaat als Sitzland des Anbieters von audiovisuellen Mediendiensten, in dem die Hauptverwaltung des Diensteanbieters liegt und in dem die redaktionellen Entscheidungen über den audiovisuellen Mediendienst getroffen werden. Werden die redaktionellen Entscheidungen über den audiovisuellen Mediendienst in einem anderen Mitgliedstaat als in dem des Sitzes der Hauptverwaltung getroffen, so gilt als Sitzland des Diensteanbieters

1. derjenige dieser beiden Mitgliedstaaten, in dem ein erheblicher Teil des Personals des Diensteanbieters, das mit der Durchführung der programmbezogenen Tätigkeiten des audiovisuellen Mediendienstes betraut ist, tätig ist,
2. derjenige dieser beiden Mitgliedstaaten, in dem die Hauptverwaltung des Diensteanbieters liegt, wenn ein erheblicher Teil des Personals des Anbieters audiovisueller Mediendienste, das mit der Ausübung der sendungsbezogenen Tätigkeiten betraut ist, in beiden Mitgliedstaaten tätig ist, oder
3. derjenige dieser beiden Mitgliedstaaten, in dem der Diensteanbieter zuerst mit seiner Tätigkeit nach Maßgabe des Rechts dieses Mitgliedstaats begonnen hat, sofern
 - a) eine dauerhafte und tatsächliche Verbindung mit der Wirtschaft dieses Mitgliedstaats fortbesteht und
 - b) ein erheblicher Teil des Personals des Anbieters von audiovisuellen Mediendiensten, das mit der Ausübung der sendungsbezogenen Tätigkeiten betraut ist, in keinem der beiden Mitgliedstaaten tätig ist.

Werden die redaktionellen Entscheidungen über den audiovisuellen Mediendienst in einem Drittstaat getroffen, so gilt derjenige Mitgliedstaat als Sitzland, in dem die Hauptverwaltung des Diensteanbieters liegt. Liegt die Hauptverwaltung des Diensteanbieters in einem Drittstaat und werden die redaktionellen Entscheidungen über den audiovisuellen Mediendienst in einem Mitgliedstaat getroffen, gilt der Mitgliedstaat als Sitzland, in dem ein erheblicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals tätig ist.

(3) Für Anbieter von audiovisuellen Mediendiensten, die nicht bereits aufgrund ihrer Niederlassung der Rechtshoheit eines Mitgliedstaats unterliegen, gilt derjenige Mitgliedstaat als Sitzland, in dem sie

1. eine dort gelegene Satelliten-Bodenstation für die Aufwärtsstrecke nutzen oder
2. zwar keine dort gelegene Satelliten-Bodenstation für die Aufwärtsstrecke, aber eine diesem Mitgliedstaat zugewiesene Übertragungskapazität eines Satelliten nutzen.

Liegt keines dieser beiden Kriterien vor, gilt derjenige Mitgliedstaat, in dem der Anbieter von audiovisuellen Mediendiensten gemäß den Artikeln 49 bis 55 des Vertrages über die Arbeitsweise der Europäischen Union niedergelassen ist, auch als Sitzland für diesen Anbieter von audiovisuellen Mediendiensten.

(4) Ist ein Videosharingplattform-Anbieter im Anwendungsbereich der Richtlinie 2010/13/EU nicht im Hoheitsgebiet eines Mitgliedstaats niedergelassen, so gilt abweichend von Absatz 1 derjenige Mitgliedstaat als Sitzland, in dessen Hoheitsgebiet

1. ein Mutterunternehmen oder ein Tochterunternehmen des Videosharingplattform-Anbieters niedergelassen ist oder

2. ein anderes Unternehmen einer Gruppe, von der der Videosharingplattform-Anbieter ein Teil ist, niedergelassen ist.

(5) Sind in den Fällen des Absatzes 4 das Mutterunternehmen, das Tochterunternehmen oder die anderen Unternehmen der Gruppe jeweils in verschiedenen Mitgliedstaaten niedergelassen, so gilt der Videosharingplattform-Anbieter als in dem Mitgliedstaat niedergelassen, in dem

1. sein Mutterunternehmen niedergelassen ist,
2. mangels einer Niederlassung nach Nummer 1 sein Tochterunternehmen niedergelassen ist oder
3. mangels einer Niederlassung nach Nummer 2 das oder die anderen Unternehmen der Gruppe niedergelassen ist oder sind.

(6) Gibt es mehrere Tochterunternehmen und ist jedes dieser Tochterunternehmen in einem anderen Mitgliedstaat niedergelassen, so gilt der Videosharingplattform-Anbieter als in dem Mitgliedstaat niedergelassen, in dem eines der Tochterunternehmen zuerst seine Tätigkeit aufgenommen hat. Voraussetzung ist, dass eine dauerhafte und tatsächliche Verbindung zwischen dem Tochterunternehmen und der Wirtschaft dieses Mitgliedstaats besteht.

(7) Gibt es mehrere andere Unternehmen, die Teil der Gruppe sind und von denen jedes in einem anderen Mitgliedstaat niedergelassen ist, so gilt der Videosharingplattform-Anbieter als in dem Mitgliedstaat niedergelassen, in dem eines dieser Unternehmen zuerst seine Tätigkeit aufgenommen hat. Voraussetzung ist, dass eine dauerhafte und tatsächliche Verbindung zwischen dem Unternehmen und der Wirtschaft dieses Mitgliedstaats besteht.

(8) Treten zwischen der zuständigen inländischen Behörde und einer Behörde eines anderen Mitgliedstaats Meinungsverschiedenheiten darüber auf, welcher Mitgliedstaat Sitzland des Diensteanbieters nach den Absätzen 2 bis 7 ist oder als solcher gilt, so bringt die zuständige inländische Behörde diese Meinungsverschiedenheiten der Europäischen Kommission unverzüglich zur Kenntnis.

§ 3 Herkunftslandprinzip

(1) Diensteanbieter und ihre digitalen Dienste, die nach § 2 in Deutschland niedergelassen sind, unterliegen den Anforderungen des deutschen Rechts auch dann, wenn die digitalen Dienste innerhalb des Geltungsbereichs der Richtlinie 2000/31/EG und der Richtlinie 2010/13/EU in einem anderen Mitgliedstaat geschäftsmäßig angeboten oder verbreitet werden, soweit nicht die Verordnung (EU) 2022/2065 unmittelbar gilt.

(2) Der freie Verkehr von digitalen Diensten, die innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 2010/13/EU in Deutschland von Diensteanbietern, die in einem anderen Mitgliedstaat niedergelassen sind, geschäftsmäßig angeboten oder verbreitet werden, wird vorbehaltlich der Absätze 5 und 6 nicht eingeschränkt.

3) Von den Absätzen 1 und 2 bleiben unberührt:

1. die Freiheit der Rechtswahl,
2. die Vorschriften für vertragliche Schuldverhältnisse in Bezug auf Verbraucherverträge,
3. gesetzliche Vorschriften über die Form des Erwerbs von Grundstücken und grundstücksgleichen Rechten sowie über die Form der Begründung, Übertragung, Änderung oder Aufhebung von dinglichen Rechten an Grundstücken und grundstücksgleichen Rechten und
4. das für den Schutz personenbezogener Daten geltende Recht.

(4) Die Absätze 1 und 2 gelten nicht für

1. die Tätigkeit von Notaren sowie von Angehörigen anderer Berufe, soweit diese ebenfalls hoheitlich tätig sind,
2. die Vertretung von Mandanten und die Wahrnehmung ihrer Interessen vor Gericht,

3. die Zulässigkeit nicht angeforderter kommerzieller Kommunikationen durch elektronische Post,
 4. Gewinnspiele mit einem einen Geldwert darstellenden Einsatz bei Glücksspielen, einschließlich Lotterien und Wetten,
 5. die Anforderungen an Verteildienste,
 6. das Urheberrecht, verwandte Schutzrechte, Rechte im Sinne der Richtlinie 87/54/EWG des Rates vom 16. Dezember 1986 über den Rechtsschutz der Topographien von Halbleitererzeugnissen (ABl. Nr. L 24 vom 27.1.1987, S. 36) und der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken (ABl. L 77 vom 27.3.1996, S. 20) sowie für gewerbliche Schutzrechte,
 7. die Ausgabe elektronischen Geldes durch Institute, die gemäß Artikel 8 Absatz 1 der Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (ABl. L 275 vom 27.10.2000, S. 39) von der Anwendung einiger oder aller Vorschriften dieser Richtlinie und von der Anwendung der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates vom 20. März 2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (ABl. L 126 vom 25.5.2000, S. 1) freigestellt sind,
 8. Vereinbarungen oder Verhaltensweisen, die dem Kartellrecht unterliegen,
 9. Bereiche, die erfasst sind von den §§ 39, 57 bis 59, 61 bis 65, 146, 241 bis 243b, 305 und 306 des Versicherungsaufsichtsgesetzes vom 1. April 2015 (BGBl. I S. 434), das zuletzt durch Artikel 9 des Gesetzes vom 31. Mai 2023 (BGBl. 2023 I Nr. 140) geändert worden ist, für Bereiche, die erfasst sind von den Vorschriften der Versicherungsberichterstattungs-Verordnung vom 19. Juli 2017 (BGBl. I S. 2858), die durch Artikel 7 des Gesetzes vom 17. August 2017 (BGBl. I S. 3214) geändert worden ist, für die Regelungen über das auf Versicherungsverträge anwendbare Recht sowie für Bedingungen, die für das Angebot und den Abschluss von Versicherungen zur Erfüllung einer in einem Mitgliedstaat vorgeschriebenen Versicherungspflicht gelten.
- (5) Das Angebot von digitalen Diensten, bei denen es sich nicht um audiovisuelle Mediendienste handelt, durch einen Diensteanbieter, der in einem anderen Mitgliedstaat niedergelassen ist, darf durch Maßnahmen auf Grundlage des deutschen Rechts eingeschränkt werden, sofern
1. dies dazu dient, folgende Schutzziele vor Beeinträchtigungen oder ernsthaften und schwerwiegenden Gefahren zu schützen:
 - a) die öffentliche Sicherheit und Ordnung, einschließlich des Jugendschutzes, insbesondere im Hinblick auf
 - aa) die Verhütung, Ermittlung, Aufklärung, Verfolgung und Vollstreckung von Straftaten und Ordnungswidrigkeiten,
 - bb) die Bekämpfung der Verunglimpfung aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität,
 - cc) Verletzungen der Menschenwürde einzelner Personen oder
 - dd) die Wahrung nationaler Sicherheits- und Verteidigungsinteressen,
 - b) die öffentliche Gesundheit oder
 - c) die Interessen der Verbraucher und die Interessen von Anlegern und
 2. die Maßnahmen, die auf der Grundlage des deutschen Rechts in Betracht kommen, in einem angemessenen Verhältnis zu den Schutzzielen nach Nummer 1 stehen.

Maßnahmen nach Satz 1 Nummer 2 sind nur zulässig, wenn die gemäß Artikel 3 Absatz 4 Buchstabe b und Absatz 5 der Richtlinie 2000/31/EG erforderlichen Verfahren eingehalten werden; davon unberührt bleiben gerichtliche Verfahren einschließlich etwaiger Vorverfahren und die Verfolgung von Straftaten einschließlich der Strafvollstreckung und von Ordnungswidrigkeiten.

(6) Der freie Empfang und die Weiterverbreitung von audiovisuellen Mediendiensten aus anderen Mitgliedstaaten darf abweichend von Absatz 2 vorübergehend beeinträchtigt werden, wenn diese audiovisuellen Mediendienste

1. in offensichtlicher, ernsthafter und schwerwiegender Weise Folgendes enthalten:

a) eine Aufstachelung zu Gewalt oder Hass gegen eine Gruppe von Personen oder gegen ein Mitglied einer Gruppe von Personen aus einem der in Artikel 21 der Charta der Grundrechte der Europäischen Union (ABl. C 364 vom 18.12.2000, S. 1) genannten Gründe,

b) eine öffentliche Aufforderung zur Begehung einer terroristischen Straftat gemäß Artikel 5 der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. L 88 vom 31.3.2017, S. 6),

c) einen Verstoß gegen die Vorgaben zum Schutz von Minderjährigen nach Artikel 6a Absatz 1 der Richtlinie 2010/13/EU oder

2. eine Beeinträchtigung oder eine ernsthafte und schwerwiegende Gefahr der Beeinträchtigung darstellen für

a) die öffentliche Gesundheit,

b) die öffentliche Sicherheit oder

c) die Wahrung nationaler Sicherheits- und Verteidigungsinteressen.

Maßnahmen nach Satz 1 sind nur zulässig, wenn die Voraussetzungen des Artikels 3 Absatz 2 bis 5 der Richtlinie 2010/13/EU erfüllt sind.

§ 4 Zulassungsfreiheit

Das Anbieten von digitalen Diensten ist im Rahmen der Gesetze zulassungs- und anmeldefrei.

Teil 2 Informationspflichten

§ 5 Allgemeine Informationspflichten

(1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene digitale Dienste folgende Informationen, die leicht erkennbar und unmittelbar erreichbar sein müssen, ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen,

2. Angaben, die eine schnelle elektronische Kontaktaufnahme und eine unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse für die elektronische Post,

3. soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,

4. die Angabe des Handelsregisters oder ähnlicher Register, in das sie eingetragen sind, und die entsprechende Registernummer,

5. soweit der Dienst angeboten oder erbracht wird in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens dreijährige Berufsausbildung abschließen (ABl. L 19 vom 24.1.1989, S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung beruflicher Befähigungsnachweise in Ergänzung zur Richtlinie 89/48/EWG (ABl. L 209 vom 24.7.1992, S. 25; L 17 vom 25.1.1995, S. 20), die zuletzt durch die Richtlinie 2006/100/EG (ABl. L 363 vom 20.12.2006, S. 141) geändert worden ist, Angaben über

- a) die Kammer, der die Diensteanbieter angehören,
 - b) die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,
 - c) die Bezeichnung der berufsrechtlichen Regelungen und die Angabe, wie diese Regelungen zugänglich sind,
6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a Absatz 1 Satz 1, 2 oder 3 des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c Absatz 1 der Abgabenordnung besitzen, die Angabe dieser Nummer,
7. bei Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung, die sich in Abwicklung oder Liquidation befinden, die Angabe hierüber,
8. bei Anbietern von audiovisuellen Mediendiensten die Angabe
- a) des Mitgliedstaats, der für sie Sitzland ist oder als Sitzland gilt sowie
 - b) der zuständigen Regulierungs- und Aufsichtsbehörden.
- (2) Weitergehende Informationspflichten nach anderen Rechtsvorschriften bleiben unberührt.

§ 6 Besondere Pflichten bei kommerziellen Kommunikationen

- (1) Diensteanbieter haben bei kommerziellen Kommunikationen, die digitale Dienste oder Bestandteile von digitalen Diensten sind, mindestens zu beachten, dass
- 1. kommerzielle Kommunikationen klar als solche zu erkennen sein müssen,
 - 2. die natürliche oder juristische Person, in deren Auftrag kommerzielle Kommunikationen erfolgen, klar identifizierbar sein muss,
 - 3. Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke klar als solche erkennbar sein müssen und die Bedingungen für ihre Inanspruchnahme leicht zugänglich sein sowie klar und unzweideutig angegeben werden müssen und
 - 4. Preisausschreiben oder Gewinnspiele mit Werbecharakter klar als solche erkennbar sein müssen und die Teilnahmebedingungen leicht zugänglich sein sowie klar und unzweideutig angegeben werden müssen.
- (2) Werden kommerzielle Kommunikationen per elektronischer Post versandt, darf in der Kopf- und in der Betreffzeile weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- oder die Betreffzeile absichtlich so gestaltet ist, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.
- (3) Videosharingplattform-Anbieter müssen eine Funktion bereitstellen, mit der Nutzer, die nutzergenerierte Videos hochladen, erklären können, ob diese Videos audiovisuelle kommerzielle Kommunikation enthalten.
- (4) Videosharingplattform-Anbieter sind verpflichtet, audiovisuelle kommerzielle Kommunikation, die Nutzer auf den Videosharingplattform-Dienst hochgeladen haben, als solche zu kennzeichnen, sofern sie nach Absatz 3 oder anderweitig Kenntnis von dieser erlangt haben.
- (5) Die Vorschriften des Gesetzes gegen den unlauteren Wettbewerb und der Preisangabenverordnung bleiben unberührt.

Teil 3 Rechtsverletzungen von Nutzern

§ 7 Beschränkte Verantwortlichkeit bei Durchleitung von Informationen

- (1) Diensteanbieter, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen, dürfen von einer Behörde nicht verpflichtet werden,

1. vor Gewährung des Zugangs
 - a) die persönlichen Daten von Nutzern zu erheben und zu speichern (Registrierung) oder
 - b) die Eingabe eines Passworts zu verlangen oder
2. das Anbieten des Dienstes dauerhaft einzustellen.

Diensteanbieter können jedoch auf freiwilliger Basis die Nutzer identifizieren, eine Passworтеingabe verlangen oder andere freiwillige Maßnahmen ergreifen.

(2) Haften Diensteanbieter nach Artikel 4 der Verordnung (EU) 2022/2065 nicht, so können sie auch nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Satz 1 ist nicht anzuwenden, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(3) Die Absätze 1 und 2 sowie Artikel 4 der Verordnung (EU) 2022/2065 sind auf Diensteanbieter, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen, auch dann anzuwenden, wenn der Dienst unentgeltlich erbracht wird.

§ 8 Anspruch auf Sperrung bei Rechtsverletzung

(1) Wurde ein digitaler Dienst, der darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln oder den Zugang zu einem Kommunikationsnetz zu vermitteln, von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen, und besteht für den Inhaber des Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuwehren, so kann der Inhaber des Rechts von dem betroffenen Diensteanbieter die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern.

(2) Die Sperrung muss zumutbar und verhältnismäßig sein.

(3) Ein Anspruch gegen den Diensteanbieter auf Erstattung der vor- und außergerichtlichen Kosten für die Geltendmachung und Durchsetzung des Anspruchs nach Absatz 1 besteht nicht, es sei denn, der Diensteanbieter arbeitet absichtlich mit einem Nutzer seines Dienstes zusammen, um das geistige Eigentum eines anderen zu verletzen.

(4) Die Absätze 1 bis 3 gelten auch dann, wenn der Dienst unentgeltlich erbracht wird.

Teil 4 Vorschriften für Anbieter von audiovisuellen Mediendiensten und für Videosharingplattform-Anbieter

§ 9 Listen der Anbieter von audiovisuellen Mediendiensten und der Videosharingplattform-Anbieter

(1) Die nach Landesrecht zuständige Behörde erstellt jeweils eine Liste der Anbieter von audiovisuellen Mediendiensten und der Videosharingplattform-Anbieter, deren Sitzland Deutschland ist oder für die Deutschland als Sitzland gilt. In der Liste sind zu jedem audiovisuellen Mediendiensteanbieter und Videosharingplattform-Anbieter die maßgeblichen Kriterien nach § 2 Absatz 2 bis 7 anzugeben.

(2) Die nach Landesrecht zuständige Behörde übermittelt die Listen der Anbieter von audiovisuellen Mediendiensten und der Videosharingplattform-Anbieter sowie alle Aktualisierungen dieser Listen der für Kultur und Medien zuständigen obersten Bundesbehörde.

(3) Die für Kultur und Medien zuständige oberste Bundesbehörde leitet die ihr übermittelten Listen der Anbieter von audiovisuellen Mediendiensten und Videosharingplattform-Anbietern sowie alle Aktualisierungen dieser Listen an die Europäische Kommission weiter.

§ 10 Auskunftsverlangen der nach Landesrecht zuständigen Behörde

(1) Anbieter von audiovisuellen Mediendiensten und Videosharingplattform-Anbieter sind verpflichtet, der nach Landesrecht zuständigen Behörde auf Verlangen Auskünfte über die in § 2 Absatz 2 bis 7 genannten Kriterien zu erteilen, soweit dies für die Erfüllung der Aufgaben nach § 9 Absatz 1 Satz 2 und Absatz 2 erforderlich ist.

(2) Anbieter von audiovisuellen Mediendiensten und Videosharingplattform-Anbieter können die Auskunft auf solche Fragen verweigern, deren Beantwortung sie selbst oder einen der in § 383 Absatz 1 Nummer 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder einer Ordnungswidrigkeit aussetzen würde. Sie sind über ihr Recht zur Auskunftsverweigerung zu belehren. Die Tatsache, auf die der Anbieter von audiovisuellen Mediendiensten oder der Videosharingplattform-Anbieter die Verweigerung der Auskunft nach Satz 1 stützt, ist auf Verlangen glaubhaft zu machen. Es genügt die eidliche Versicherung des Anbieters von audiovisuellen Mediendiensten oder des Videosharingplattform-Anbieters.

§ 11 Vertragliche Nutzungsverbote

(1) Videosharingplattform-Anbieter sind verpflichtet, mit ihren Nutzern wirksam zu vereinbaren, dass diese auf der Videosharingplattform keine unzulässige audiovisuelle kommerzielle Kommunikation verbreiten dürfen.

(2) Unzulässige audiovisuelle kommerzielle Kommunikation im Sinne dieser Vorschrift ist audiovisuelle kommerzielle Kommunikation, die gegen folgende Vorschriften verstößt:

1. § 20 des Tabakerzeugnisgesetzes vom 4. April 2016 (BGBl. I S. 569), das zuletzt durch Artikel 2 Absatz 5 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2752) geändert worden ist, oder

2. § 10 des Heilmittelwerbegesetzes in der Fassung der Bekanntmachung vom 19. Oktober 1994 (BGBl. I S. 3068), das zuletzt durch Artikel 6 des Gesetzes vom 11. Juli 2022 (BGBl. I S. 1082) geändert worden ist.

Teil 5 Durchführung der Verordnung (EU) 2022/2065

Abschnitt 1 Zuständige Behörden und Koordinierungsstelle für digitale Dienste

Unterabschnitt 1 Zuständige Behörden

§ 12 Zuständige Behörden nach Artikel 49 Absatz 1 der Verordnung (EU) 2022/2065

(1) Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) ist vorbehaltlich der Absätze 2 und 3 zuständige Behörde nach Artikel 49 Absatz 1 der Verordnung (EU) 2022/2065.

(2) Die Bundeszentrale für Kinder- und Jugendmedienschutz ist zuständige Behörde für die Durchsetzung von Artikel 14 Absatz 3 und für die Durchsetzung von strukturellen Vorsorgemaßnahmen nach Artikel 28 Absatz 1 der Verordnung (EU) 2022/2065, soweit diese nicht Maßnahmen nach dem Jugendmedienschutz-Staatsvertrag in der Fassung vom 14. Dezember 2021 betreffen. Für diese Maßnahmen sind die nach den medienrechtlichen Bestimmungen der Länder benannten Stellen zuständige Behörden. Zur Durchsetzung und Überwachung der Verordnung (EU) 2022/2065 wird in der Bundeszentrale für Kinder- und Jugendmedienschutz eine Stelle zur Durchsetzung von Kinderrechten in digitalen Diensten mit Sitz in Bonn eingerichtet. Auf die Stelle zur Durchsetzung von Kinderrechten in digitalen Diensten sind folgende Regelungen entsprechend anzuwenden:

1. hinsichtlich der Ausstattung § 14 Absatz 2,
2. hinsichtlich der Unabhängigkeit § 15 und
3. hinsichtlich der Leitung § 16 Absatz 1.

Die Direktorin oder der Direktor der Bundeszentrale für Kinder- und Jugendmedienschutz tritt an die Stelle der Präsidentin oder des Präsidenten der Bundesnetzagentur. Die Leiterin oder der Leiter der Stelle zur Durchsetzung von Kinderrechten in digitalen Diensten wird von der Direktorin oder dem Direktor der Bundeszentrale für Kinder- und Jugendmedienschutz ernannt.

(3) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zuständige Behörde für die Durchsetzung von Artikel 26 Absatz 3 und Artikel 28 Absatz 2 und 3 der Verordnung (EU) 2022/2065.

(4) Im Übrigen bleiben die für die Beaufsichtigung von Diensteanbietern bestehenden gesetzlichen Zuständigkeiten unberührt.

- (5) Das Deutsche-Welle-Gesetz und die medienrechtlichen Bestimmungen der Länder bleiben unberührt.

§ 13 Meldung des Verdachts auf Straftaten gemäß Artikel 18 der Verordnung (EU) 2022/2065 an das Bundeskriminalamt

Das Bundeskriminalamt nimmt als Zentralstelle Informationen nach Artikel 18 Absatz 1 und 2 der Verordnung (EU) 2022/2065 entgegen, verarbeitet diese Informationen im Rahmen seiner gesetzlichen Aufgaben nach dem Bundeskriminalamtgesetz und leitet die Informationen an die jeweils zuständige Strafverfolgungsbehörde weiter.

Unterabschnitt 2 Koordinierungsstelle für digitale Dienste

§ 14 Errichtung und Ausstattung

- (1) Zur Durchsetzung und Überwachung der Verordnung (EU) 2022/2065 wird eine Koordinierungsstelle für digitale Dienste in der Bundesnetzagentur mit Sitz in Bonn eingerichtet.
- (2) Der Koordinierungsstelle für digitale Dienste ist für die Erfüllung ihrer Aufgaben die notwendige Personal- und Sachausstattung zur Verfügung zu stellen.
- (3) Eine angemessene finanzielle Ausstattung nach Absatz 2 umfasst auch einen Forschungsetat.

§ 15 Unabhängigkeit

Die Koordinierungsstelle für digitale Dienste handelt bei der Wahrnehmung der ihr durch die Verordnung (EU) 2022/2065 zugewiesenen Aufgaben und Befugnisse völlig unabhängig. Sie unterliegt weder direkter noch indirekter Beeinflussung von außen und ersucht weder um Weisungen noch nimmt sie Weisungen entgegen, sofern diese Weisungen den fachlichen Bereich der unabhängigen Aufgabenerfüllung betreffen.

§ 16 Leitung der Koordinierungsstelle für digitale Dienste

- (1) Die Leiterin oder der Leiter der Koordinierungsstelle für digitale Dienste trifft die von der Verordnung (EU) 2022/2065 vorgesehenen Entscheidungen.
- (2) Die Leiterin oder der Leiter der Koordinierungsstelle für digitale Dienste vertritt die Bundesrepublik Deutschland im Europäischen Gremium für digitale Dienste nach Artikel 61 der Verordnung (EU) 2022/2065. Die Leiterin oder der Leiter der Koordinierungsstelle für digitale Dienste kann sich hierbei gemäß Artikel 62 Absatz 1 Satz 1 der Verordnung (EU) 2022/2065 vertreten lassen. Die zuständigen Behörden nach § 12 Absatz 2 und 3 können sich nach Maßgabe ihrer spezifischen Zuständigkeiten an der Arbeit des Gremiums nach Artikel 62 Absatz 1 Satz 3 der Verordnung (EU) 2022/2065 beteiligen.
- (3) Die Leiterin oder der Leiter der Koordinierungsstelle für digitale Dienste steht in einem Beamtenverhältnis auf Zeit. Die Amtszeit beträgt fünf Jahre. Eine einmalige Verlängerung um fünf Jahre ist zulässig.
- (4) Die Leiterin oder der Leiter der Koordinierungsstelle für digitale Dienste wird von der Präsidentin oder dem Präsidenten der Bundesnetzagentur gegenüber dem Bundesministerium für Wirtschaft und Klimaschutz vorgeschlagen. Für den Vorschlag stellt das Bundesministerium für Wirtschaft und Klimaschutz das Einvernehmen mit dem Bundesministerium für Digitales und Verkehr her. Die Ernennung der Leiterin oder des Leiters erfolgt durch die Bundespräsidentin oder den Bundespräsidenten. Bis zur Ernennung der Leiterin oder des Leiters der Koordinierungsstelle für digitale Dienste nimmt der Präsident oder die Präsidentin der Bundesnetzagentur geschäftsführend die Aufgaben der Leitung wahr. Wird eine Bundesbeamtin oder ein Bundesbeamter zur Leiterin oder zum Leiter ernannt, ruhen für die Dauer des Beamtenverhältnisses auf Zeit die in dem Beamtenverhältnis auf Lebenszeit begründeten Rechte und Pflichten. Davon ausgenommen sind die Pflicht zur Verschwiegenheit und das Verbot, Belohnungen oder Geschenke oder sonstige Vorteile anzunehmen.

§ 17 Tätigkeitsbericht

- (1) Die Koordinierungsstelle für digitale Dienste legt den nach Artikel 55 der Verordnung (EU) 2022/2065 jährlich zu erstellenden Tätigkeitsbericht den gesetzgebenden Körperschaften des Bundes vor.
- (2) Der Tätigkeitsbericht enthält insbesondere folgende Angaben der Koordinierungsstelle für digitale Dienste und der weiteren nach § 12 Absatz 2 und 3 für die Durchsetzung der Verordnung (EU) 2022/2065 zuständigen Behörden:

1. die Anzahl der eingegangenen Beschwerden gemäß Artikel 53 der Verordnung (EU) 2022/2065 und eine Übersicht über die aufgrund der Beschwerden eingeleiteten Maßnahmen,
 2. die Anzahl und den Gegenstand der Anordnungen zum Vorgehen gegen rechtswidrige Inhalte und der Auskunftsanordnungen, die gemäß den Artikeln 9 und 10 der Verordnung (EU) 2022/2065 von den nationalen Justiz- oder Verwaltungsbehörden erlassen wurden,
 3. die Anzahl und den Gegenstand der Ausführungen der in Nummer 2 genannten Anordnungen, wie sie der Koordinierungsstelle für digitale Dienste gemäß den Artikeln 9 und 10 der Verordnung (EU) 2022/2065 mitgeteilt wurden,
 4. Angaben zu den eingesetzten personellen und finanziellen Ressourcen,
 5. Anzahl der Gespräche, aufgeschlüsselt nach Datum und Namen der Organisation, die die Koordinierungsstelle für digitale Dienste mit Vertreterinnen und Vertretern von Unternehmen, Verbänden oder sonstigen Interessenvertretern im Zusammenhang mit den ihr gesetzlich zugewiesenen Aufgaben zur Durchsetzung der Verordnung (EU) 2022/2065 geführt hat,
 6. Anzahl und Gegenstand der festgestellten Verstöße gegen die Verordnung (EU) 2022/2065 sowie
 7. Anzahl eingeleiteter Ordnungswidrigkeitenverfahren nach § 33 und weiterer eingeleiteter Maßnahmen nach § 27 sowie die Höhe der festgesetzten Buß- und Zwangsgelder.
- (3) Die Koordinierungsstelle für digitale Dienste veröffentlicht den Tätigkeitsbericht zeitgleich mit der Vorlage nach Absatz 1 in elektronischer Form und in einem für Menschen mit Behinderungen barrierefreien Format auf ihrer Internetseite.
- (4) Die nach § 12 Absatz 2 und 3 zuständigen Behörden teilen der Koordinierungsstelle für digitale Dienste alle Informationen gemäß Absatz 2 mit, die für die Erstellung erforderlich sind.

§ 18 Zusammenarbeit der Koordinierungsstelle für digitale Dienste mit den zuständigen Behörden, Verwaltungsvereinbarung

- (1) Die nach § 12 Absatz 2 und 3 für die Durchsetzung der Verordnung (EU) 2022/2065 zuständigen Behörden und die Koordinierungsstelle für digitale Dienste arbeiten zur Erfüllung ihrer Aufgaben im Rahmen ihrer jeweiligen Zuständigkeiten kooperativ und vertrauensvoll zusammen. Sie teilen einander Beobachtungen und Feststellungen mit, die für die Erfüllung der beiderseitigen Aufgaben von Bedeutung sein können.
- (2) Die Einzelheiten der Zusammenarbeit nach Absatz 1 können in einer Verwaltungsvereinbarung näher geregelt werden. In der Verwaltungsvereinbarung kann insbesondere Folgendes geregelt werden:
 1. eine Koordinierung des Daten- und Informationsaustausches nach Absatz 3,
 2. eine Verfahrensweise zur Entgegennahme und Weiterleitung von Beschwerden nach § 20.
- (3) Soweit es zur Aufsicht und Sanktionierung im Rahmen der Durchsetzung der Verordnung (EU) 2022/2065 sowie zur Durchführung der Aufgabe der Koordinierungsstelle für digitale Dienste als zentrale Informationsstelle nach § 20 erforderlich ist, dürfen die zuständigen Behörden nach § 12 Absatz 2 und 3 und die Koordinierungsstelle für digitale Dienste einander folgende Inhalte und Daten einschließlich personenbezogener Daten übermitteln:
 1. Internetinhalte sowie die zugehörigen Bestands- und Nutzungsdaten des Nutzerkontos eines digitalen Dienstes sowie
 2. Nutzerbeschwerden und die jeweils zugehörige Kommunikation mit Beschwerdeführern.

Die Koordinierungsstelle für digitale Dienste und die zuständigen Behörden nach § 12 Absatz 2 und 3 dürfen die ihnen übermittelten Inhalte und Daten in ihren Aufsichts- und Sanktionsverfahren verwerten. Beweisverwertungsverbote bleiben unberührt.

§ 19 Zusammenarbeit mit anderen Behörden, Einrichtung von Verbindungsschnittstellen, Verwaltungsvereinbarung

(1) Sofern Aufgaben der Koordinierungsstelle für digitale Dienste die Prüfung der Einhaltung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 7. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1, und sonstiger Vorschriften über den Datenschutz berühren, entscheidet die Koordinierungsstelle für digitale Dienste im Benehmen mit der zuständigen Datenschutzaufsichtsbehörde.

(2) Im Rahmen ihrer jeweiligen Zuständigkeiten arbeiten die Koordinierungsstelle für digitale Dienste und die nach § 12 Absatz 2 Satz 1 und Absatz 3 zuständigen Behörden mit dem Bundeskartellamt und mit der Bundesnetzagentur, soweit ihre sonstigen Aufgabenbereiche unabhängig von der Koordinierungsstelle für digitale Dienste betroffen sind, kooperativ und vertrauensvoll zusammen. Die in Satz 1 genannten Behörden können unabhängig von der jeweils gewählten Verfahrensart untereinander Informationen einschließlich Betriebs- und Geschäftsgeheimnissen austauschen, soweit dies zur Erfüllung ihrer jeweiligen Aufgaben erforderlich ist, sowie diese Informationen in ihren Verfahren verwerten. Soweit es zur Erfüllung der Aufgaben nach diesem Gesetz, nach dem Terroristische-Online-Inhalte-Bekämpfungsgesetz oder nach dem Gesetz gegen Wettbewerbsbeschränkungen erforderlich ist, können die in Satz 1 genannten Behörden im Rahmen des Austausches nach Satz 2 auch personenbezogene Daten austauschen und in den betreffenden Verfahren verwerten. Beweisverwertungsverbote bleiben unberührt.

(3) Im Rahmen ihrer jeweiligen Zuständigkeiten nach diesem Gesetz arbeitet die Koordinierungsstelle für digitale Dienste zur Wahrnehmung der Aufgaben nach der Verordnung (EU) 2022/2065 mit dem Bundeskriminalamt zusammen. Die Koordinierungsstelle für digitale Dienste und das Bundeskriminalamt dürfen einander Internetinhalte sowie die zugehörigen Bestands- und Nutzungsdaten des Nutzerkontos eines digitalen Dienstes sowie auf eine Meldung bezogene Verwaltungsdaten, jeweils einschließlich personenbezogener Daten übermitteln, soweit dies zur Aufsicht und Sanktionierung durch die Koordinierungsstelle für digitale Dienste im Rahmen der Durchsetzung der Verordnung (EU) 2022/2065 erforderlich ist. Die Koordinierungsstelle für digitale Dienste darf die ihr übermittelten Daten in ihren Aufsichts- und Sanktionsverfahren verwenden. Beweisverwertungsverbote bleiben unberührt.

(4) Die Koordinierungsstelle für digitale Dienste und die nach § 12 Absatz 2 und 3 zuständigen Behörden arbeiten mit den weiteren für die Beaufsichtigung von Diensteanbietern zuständigen nationalen Behörden nach § 12 Absatz 4 und mit nach Absatz 5 eingerichteten Verbindungsschnittstellen zur Erfüllung ihrer Aufgaben im Rahmen ihrer jeweiligen Zuständigkeiten kooperativ und vertrauensvoll zusammen. Die in Satz 1 genannten Behörden teilen einander Beobachtungen und Feststellungen mit, die für die Erfüllung der beiderseitigen Aufgaben von Bedeutung sein können.

(5) Bundesministerien können innerhalb ihrer Zuständigkeitsbereiche Verbindungsschnittstellen einrichten, die bei ihnen eingehende Beschwerden an die jeweils zuständigen Behörden weiterleiten. Zur Wahrnehmung der Aufgabe als Verbindungsschnittstelle dürfen diese Nutzerbeschwerden, die einen Bereich betreffen, nach dem nach § 12 Absatz 4 die gesetzliche Zuständigkeit von Landesbehörden unberührt bleibt, einschließlich enthaltener personenbezogener Daten, entgegennehmen und an die jeweils zuständige Behörde weiterleiten.

(6) Die Einzelheiten der Zusammenarbeit der Koordinierungsstelle für digitale Dienste und der nach § 12 Absatz 2 und 3 zuständigen Behörden mit den Behörden nach § 12 Absatz 4 und mit den Verbindungsschnittstellen nach Absatz 5 können in Verwaltungsvereinbarungen näher geregelt werden. In den Verwaltungsvereinbarungen kann insbesondere Folgendes geregelt werden:

1. die Art und Weise der Zusammenarbeit,
2. die Art und Weise des Informationsaustausches nach Absatz 4 Satz 2 und
3. die Übermittlung von Anordnungen durch eine für die Beaufsichtigung von Diensteanbietern zuständige nationale Justiz- oder Verwaltungsbehörde an den Koordinator für digitale Dienste nach Artikel 9 Absatz 3 und Artikel 10 Absatz 3 der Verordnung (EU) 2022/2065.

§ 20 Zentrale Beschwerdestelle

(1) Unbeschadet der Vorgaben des Artikels 53 der Verordnung (EU) 2022/2065 ist die Koordinierungsstelle für digitale Dienste über den gesamten Zeitraum des Beschwerdeverfahrens wegen einer Zuwiderhandlung gegen die Verordnung (EU) 2022/2065 Ansprechpartnerin des Beschwerdeführers (zentrale Beschwerdestelle). Die Koordinierungsstelle für digitale Dienste ist über den gesamten Zeitraum des Beschwerdeverfahrens auch zentrale Beschwerdestelle im Fall einer Weiterleitung an eine gemäß § 12 Absatz 2 und 3 zuständige Behörde, sofern der Beschwerdeführer nicht diese Behörde als Ansprechpartnerin benennt. Unbeschadet der Informationspflichten zu personenbezogenen Daten nach der Verordnung (EU) 2016/679 ist der Beschwerdeführer unverzüglich nach Feststellung der Zuständigkeit einer nach § 12 Absatz 2 und 3 zuständigen Behörde für eine Beschwerde über Folgendes zu informieren:

1. über die Funktion der zentralen Beschwerdestelle als Ansprechpartnerin des Beschwerdeführers auch für den Fall, dass eine andere Behörde nach § 12 Absatz 2 und 3 für die konkrete Beschwerde zuständig ist,
2. über die Weiterleitung und den Austausch seiner Beschwerde und der folgenden Kommunikation,
3. über das Verfahren der Weiterleitung und des Austausches zwischen der zentralen Beschwerdestelle und den zuständigen Behörden nach § 12 Absatz 2 und 3,
4. über die Möglichkeit, die gemäß § 12 Absatz 2 und 3 zuständige Behörde als Ansprechpartnerin zu benennen.

(2) Zur Erfüllung ihrer Aufgaben als zentrale Beschwerdestelle hat die Koordinierungsstelle für digitale Dienste das Recht, sich von der gemäß § 12 Absatz 2 und 3 zuständigen Behörde auf Nachfrage des Beschwerdeführers jederzeit angemessen über den Stand der Beschwerde unterrichten zu lassen.

§ 21 Beirat

(1) Bei der Koordinierungsstelle für digitale Dienste wird ein Beirat eingerichtet.

(2) Der Beirat besteht aus den folgenden 16 Mitgliedern:

1. vier Vertreterinnen und Vertreter der Wissenschaft,
2. acht Vertreterinnen und Vertreter der Zivilgesellschaft, einschließlich Verbraucherverbänden, und
3. vier Vertreterinnen und Vertreter von Wirtschaftsverbänden.

Unternehmen können nicht Mitglieder des Beirats sein. Die Vertreterinnen und Vertreter sollen hinsichtlich der Art und Weise der Tätigkeit digitaler Dienste über besondere rechtliche, wirtschaftswissenschaftliche, sozialpolitische oder technologische Erfahrungen oder über ausgewiesene einschlägige wissenschaftliche Kenntnisse verfügen.

(3) Der Beirat hat die Aufgabe,

1. die Koordinierungsstelle für digitale Dienste in grundsätzlichen Fragen der Anwendung und Durchsetzung der Verordnung (EU) 2022/2065 zu beraten,
2. allgemeine Empfehlungen zur wirkungsvollen und einheitlichen Durchführung der Verordnung (EU) 2022/2065 vorzuschlagen und
3. wissenschaftliche Fragestellungen, insbesondere auch zum Umgang mit Daten, an die Koordinierungsstelle für digitale Dienste heranzutragen.

(4) Die Mitglieder des Beirats werden vom Deutschen Bundestag vorgeschlagen und für die Dauer der Wahlperiode des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Klimaschutz im Einvernehmen mit dem Bundesministerium für Digitales und Verkehr berufen. Sie bleiben nach Beendigung der Wahlperiode des Deutschen Bundestages noch so lange im Amt, bis die neuen Mitglieder berufen worden sind. Die Mitglieder des Beirats können auf ihre Mitgliedschaft verzichten. Der Verzicht ist gegenüber dem Bundesministerium für Wirtschaft und Klimaschutz schriftlich oder elektronisch zu erklären. Hierüber ist das Bundesministerium für Digitales und Verkehr vom Bundesministerium für Wirtschaft und Klimaschutz zu

unterrichten. Scheidet ein Mitglied vorzeitig aus, so ist unverzüglich an seiner Stelle ein neues Mitglied zu berufen.

- (5) Die Mitglieder des Beirats sind in der Ausübung ihrer Tätigkeit im Beirat unabhängig, unterliegen keinen Weisungen und sind ausschließlich dem öffentlichen Interesse verpflichtet.
- (6) Der Beirat gibt sich eine Geschäftsordnung, die der Genehmigung des Bundesministeriums für Wirtschaft und Klimaschutz im Benehmen mit dem Bundesministerium für Digitales und Verkehr und der Zustimmung des Deutschen Bundestages bedarf.
- (7) Der Beirat wählt nach Maßgabe seiner Geschäftsordnung aus seiner Mitte ein vorsitzendes und ein stellvertretendes vorsitzendes Mitglied.
- (8) Für den Beirat unterhält die Bundesnetzagentur eine Geschäftsstelle. Diese Geschäftsstelle muss angemessen ausgestattet werden.
- (9) Die Mitglieder des Beirats erhalten Ersatz von Reisekosten und ein angemessenes Sitzungsgeld, das das Bundesministerium für Wirtschaft und Klimaschutz im Benehmen mit dem Bundesministerium für Digitales und Verkehr festsetzt.
- (10) Der Beirat soll mindestens einmal im Vierteljahr zu einer Sitzung zusammentreten. Sitzungen sind anzuberaumen, wenn die Koordinierungsstelle für digitale Dienste oder mindestens drei Mitglieder die Einberufung schriftlich beantragen. Die oder der Vorsitzende des Beirats kann jederzeit eine Sitzung anberaumen. Der Beirat kann andere Einrichtungen und Gruppen im Rahmen seiner Tätigkeit in geeigneter Form einbeziehen.
- (11) Die Sitzungen sind öffentlich, soweit der Beirat nach Maßgabe seiner Geschäftsordnung nichts anderes beschließt.
- (12) Die Leiterin oder der Leiter der Koordinierungsstelle für digitale Dienste oder die Stellvertretung nimmt an den Sitzungen teil. Sie oder er muss während der Sitzung jederzeit gehört werden. Der Beirat kann die Anwesenheit der Leiterin oder des Leiters der Koordinierungsstelle für digitale Dienste verlangen, wenn die Stellvertretung der Leiterin oder des Leiters verhindert ist.
- (13) Der Beirat berichtet dem Deutschen Bundestag jährlich über seine Tätigkeit nach Absatz 3 sowie im Hinblick auf die Zusammenarbeit mit der Koordinierungsstelle für digitale Dienste.

Teil 7 Befugnisse und Verfahren

§ 24 Ermittlungen

- (1) Im Rahmen der Ausübung der Befugnisse gemäß Artikel 51 Absatz 1 der Verordnung (EU) 2022/2065 dürfen die Koordinierungsstelle für digitale Dienste und die nach § 12 Absatz 2 Satz 1 und Absatz 3 zuständigen Behörden alle Ermittlungen führen und alle Beweise erheben, die erforderlich sind.
- (2) Für den Beweis durch Augenschein, Zeugen und Sachverständige sind § 372 Absatz 1, die §§ 376 bis 378, 380 bis 387, 390, 395 bis 397, 398 Absatz 1 und die §§ 401, 402, 404, 404a, 406 bis 409, 411 bis 414 der Zivilprozessordnung entsprechend anzuwenden; Haft darf nicht verhängt werden. Für die Entscheidung über die Beschwerde ist das Oberlandesgericht zuständig.
- (3) Über die Aussagen der Zeuginnen und Zeugen sowie über die Aussagen der Sachverständigen soll ein Protokoll erstellt werden. Das Protokoll ist von der ermittelnden Person der zuständigen Behörde und, wenn ein Urkundsbeamter zugezogen ist, auch von diesem zu unterschreiben. Das Protokoll soll Ort und Tag der Verhandlung sowie die Namen der Mitwirkenden und Beteiligten enthalten. Das Protokoll ist den Zeuginnen und Zeugen sowie den Sachverständigen zur Genehmigung vorzulesen oder zur eigenen Durchsicht vorzulegen. Die erteilte Genehmigung ist zu vermerken und von den Betreffenden zu unterschreiben. Unterbleibt die Unterschrift, so ist der Grund hierfür anzugeben.
- (4) Die Koordinierungsstelle für digitale Dienste und die nach § 12 Absatz 2 Satz 1 und Absatz 3 zuständigen Behörden können das Amtsgericht um die Beeidigung von Zeuginnen und Zeugen ersuchen, wenn sie die

Beeidigung zur Herbeiführung einer wahrheitsgemäßen Aussage für notwendig erachten. Über die Beeidigung entscheidet das Gericht.

(5) Sofern die Ermittlungen ergeben haben, dass ein Anbieter von Vermittlungsdiensten gegen Auflagen oder Anordnungen der Koordinierungsstelle für digitale Dienste oder der nach § 12 Absatz 2 Satz 1 und Absatz 3 zuständigen Behörden verstoßen hat, hat der Anbieter der Koordinierungsstelle für digitale Dienste oder den nach § 12 Absatz 2 Satz 1 und Absatz 3 zuständigen Behörden die Aufwendungen für diese Ermittlungen einschließlich ihrer Auslagen für Sachverständige zu erstatten.

§ 25 Auskunftserteilung und Durchsuchungen

(1) Die in Artikel 51 Absatz 1 Buchstabe a und c der Verordnung (EU) 2022/2065 genannten Personen sind verpflichtet, auf Verlangen der Koordinierungsstelle für digitale Dienste oder der nach § 12 Absatz 2 Satz 1 und Absatz 3 zuständigen Behörden die betreffenden Informationen zur Verfügung zu stellen. Die in Artikel 51 Absatz 1 Buchstabe b der Verordnung (EU) 2022/2065 genannten Personen sind verpflichtet, die Prüfung der geschäftlichen Unterlagen sowie das Betreten der in Artikel 51 Absatz 1 Buchstabe b der Verordnung (EU) 2022/2065 genannten Räumlichkeiten während der üblichen Geschäftszeiten zu dulden. Bei juristischen Personen, Gesellschaften oder nicht rechtsfähigen Vereinen gelten die Verpflichtungen nach den Sätzen 1 und 2 für die nach Gesetz oder Satzung zur Vertretung berufenen Personen.

(2) Die nach Absatz 1 zur Information Verpflichteten können die Auskunft auf solche Fragen verweigern, deren Beantwortung sie selbst oder Personen nach § 383 Absatz 1 Nummer 1 bis 3 der Zivilprozessordnung der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

(3) Personen, die mit der Durchführung von Nachprüfungen beauftragt werden, dürfen die Büro- und Geschäftsräume von Unternehmen sowie von Vereinigungen von Unternehmen während der üblichen Geschäftszeiten betreten. Durchsuchungen dürfen nur auf Anordnung des Amtsgerichts, in dessen Bezirk die Durchsuchungen erfolgen sollen, vorgenommen werden. Auf die Anfechtung einer solchen Anordnung sind die §§ 306 bis 310 und § 311a der Strafprozessordnung entsprechend anzuwenden. Bei Gefahr im Verzug dürfen die Personen, die die Nachprüfung durchführen, während der Geschäftszeit die erforderlichen Durchsuchungen ohne richterliche Anordnung vornehmen. An Ort und Stelle ist von ihnen ein Protokoll über die Durchsuchung und ihr wesentliches Ergebnis zu erstellen, aus dem sich, falls keine richterliche Anordnung ergangen ist, auch die Tatsachen ergeben, die zur Annahme einer Gefahr im Verzug geführt haben.

Teil 8 - Bußgeldvorschriften

§ 33 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer absichtlich entgegen § 6 Absatz 2 Satz 1 den Absender oder den kommerziellen Charakter der Nachricht verschleiert oder verheimlicht.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 5 Absatz 1 eine Information nicht, nicht richtig oder nicht vollständig verfügbar hält,

2. entgegen § 10 Absatz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,

3. entgegen

a) § 25 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, oder

b) § 30 in Verbindung mit § 203 Absatz 1 Satz 1 des Telekommunikationsgesetzes

eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zur Verfügung stellt oder

4. entgegen

a) § 25 Absatz 1 Satz 2, auch in Verbindung mit Satz 3, oder

b) § 30 in Verbindung mit § 204 Absatz 1 Satz 1 Nummer 3 des Telekommunikationsgesetzes eine dort genannte Prüfung oder ein dort genanntes Betreten nicht duldet.

(3) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (ABl. L 186 vom 11.7.2019, S. 57) verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 3 Absatz 5 nicht sicherstellt, dass die dort genannte Identität erkennbar ist,
2. entgegen Artikel 4 Absatz 1 oder Absatz 2, jeweils in Verbindung mit Artikel 4 Absatz 5, eine Begründung nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig übermittelt,
3. entgegen Artikel 4 Absatz 3 Satz 1 oder Artikel 5 Absatz 4 eine dort genannte Möglichkeit nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig bietet,
4. entgegen Artikel 4 Absatz 3 Satz 2 einen gewerblichen Nutzer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig einsetzt,
5. entgegen Artikel 4 Absatz 4 Unterabsatz 2 eine Begründung nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig zur Verfügung stellt,
6. entgegen Artikel 5 Absatz 2 Satz 1 in Verbindung mit Artikel 5 Absatz 3 oder Absatz 5 einen Hauptparameter oder die Gewichtung der Hauptparameter nicht richtig darstellt,
7. entgegen Artikel 5 Absatz 2 Satz 2 in Verbindung mit Artikel 5 Absatz 3 oder Absatz 5 nicht dafür sorgt, dass eine Beschreibung aktuell ist,
8. entgegen Artikel 7 Absatz 2 in Verbindung mit Artikel 7 Absatz 3 eine dort genannte Erläuterung nicht, nicht richtig oder nicht vollständig vornimmt,
9. entgegen Artikel 11 Absatz 1 Unterabsatz 1 in Verbindung mit Unterabsatz 2 ein internes System nicht, nicht richtig, nicht vollständig oder nicht spätestens mit dem Anbieten des Online-Vermittlungsdienstes einrichtet,
10. entgegen Artikel 11 Absatz 2 Buchstabe a eine Prüfung nicht oder nicht unverzüglich nach Kenntnisnahme durchführt,
11. entgegen Artikel 11 Absatz 2 Buchstabe b eine Bearbeitung nicht oder nicht unverzüglich nach der Feststellung, dass eine Bearbeitung erforderlich ist, durchführt,
12. entgegen Artikel 11 Absatz 2 Buchstabe c eine Unterrichtung nicht oder nicht unverzüglich nach Beendigung der Bearbeitung durchführt,
13. entgegen Artikel 11 Absatz 4 Unterabsatz 1 Satz 1 eine Information nicht oder nicht spätestens mit der Einrichtung des Beschwerdesystems verfügbar macht,
14. entgegen Artikel 11 Absatz 4 Unterabsatz 1 Satz 2 eine Information nicht oder nicht rechtzeitig überprüft oder nicht oder nicht rechtzeitig aktualisiert oder
15. entgegen Artikel 12 Absatz 6 eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig bereitstellt.

(4) Ordnungswidrig handelt, wer entgegen Artikel 16 Absatz 6 Satz 1 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27.10.2022, S. 1; L 310 vom 1.12.2022, S. 17) eine Entscheidung nicht frei von Willkür oder nicht objektiv trifft und eine solche Handlung beharrlich wiederholt.

(5) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2022/2065 verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 9 Absatz 1 oder Absatz 5 Satz 1, Artikel 10 Absatz 1 oder Absatz 5 Satz 1, Artikel 14 Absatz 2 oder Artikel 32 Absatz 1 eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gibt,

2. entgegen Artikel 11 Absatz 1, Artikel 12 Absatz 1 oder Artikel 13 Absatz 1 in Verbindung mit Artikel 13 Absatz 2 eine Kontaktstelle oder eine Person nicht, nicht richtig oder nicht spätestens mit Anbieten des Vermittlungsdienstes benennt,
3. entgegen Artikel 11 Absatz 2 Satz 1 in Verbindung mit Artikel 11 Absatz 3 oder Artikel 12 Absatz 2 Satz 1 eine Information nicht oder nicht spätestens mit Anbieten des Vermittlungsdienstes veröffentlicht,
4. entgegen Artikel 13 Absatz 4 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht spätestens mit Anbieten des Vermittlungsdienstes macht,
5. entgegen Artikel 13 Absatz 4 Satz 2 nicht dafür sorgt, dass eine dort genannte Angabe aktuell ist,
6. entgegen Artikel 14 Absatz 3 eine Erläuterung nicht, nicht richtig oder nicht vollständig vornimmt,
7. entgegen Artikel 15 Absatz 1 Satz 1 in Verbindung mit Satz 2, jeweils auch in Verbindung mit Artikel 24 Absatz 1, einen Bericht nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig zur Verfügung stellt,
8. entgegen Artikel 16 Absatz 1 Satz 1 in Verbindung mit Satz 2 oder Artikel 16 Absatz 2 ein Meldeverfahren nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht spätestens mit Anbieten des Hostingdienstes einrichtet,
9. entgegen Artikel 16 Absatz 5 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht oder einen Hinweis nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gibt,
10. entgegen Artikel 17 Absatz 1 in Verbindung mit Artikel 17 Absatz 2 Unterabsatz 1 Satz 2, Absatz 3 oder Absatz 4 eine Begründung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,
11. entgegen Artikel 20 Absatz 1 in Verbindung mit Artikel 20 Absatz 2 oder Absatz 3 einen Zugang zu einem Beschwerdemanagementsystem nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht für die vorgeschriebene Dauer gewährt,
12. entgegen Artikel 20 Absatz 4 Satz 2 eine Entscheidung nicht oder nicht rechtzeitig rückgängig macht,
13. entgegen Artikel 20 Absatz 5 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
14. entgegen Artikel 20 Absatz 6 nicht sicherstellt, dass eine Entscheidung in dort genannter Weise getroffen wird,
15. entgegen Artikel 21 Absatz 1 Unterabsatz 2 nicht sicherstellt, dass eine dort genannte Information zugänglich ist,
16. entgegen Artikel 22 Absatz 1 eine Maßnahme nicht oder nicht spätestens mit Anbieten der Online-Plattform ergreift,
17. entgegen Artikel 24 Absatz 3 Satz 1 oder Absatz 5 Satz 1 eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,
18. entgegen Artikel 24 Absatz 5 Satz 2 nicht sicherstellt, dass eine dort genannte Information personenbezogene Daten nicht enthält,
19. entgegen Artikel 25 Absatz 1 eine Online-Schnittstelle konzipiert, organisiert oder betreibt,
20. entgegen Artikel 26 Absatz 1 nicht sicherstellt, dass ein Nutzer in der Lage ist, eine dort genannte Angabe zu erkennen,
21. entgegen Artikel 26 Absatz 2 Unterabsatz 1 eine Funktion nicht oder nicht richtig bietet,
22. entgegen Artikel 26 Absatz 2 Unterabsatz 2 nicht sicherstellt, dass ein Nutzer einen dort genannten Sachverhalt feststellen kann,
23. entgegen Artikel 26 Absatz 3 Werbung anzeigt,

24. entgegen Artikel 27 Absatz 1 in Verbindung mit Artikel 27 Absatz 2 einen Parameter nicht, nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise darlegt,
 25. entgegen Artikel 27 Absatz 3 Satz 1 in Verbindung mit Satz 2 eine Funktion nicht, nicht richtig oder nicht in der vorgeschriebenen Weise zugänglich macht,
 26. entgegen Artikel 28 Absatz 2 Werbung darstellt,
 27. entgegen Artikel 30 Absatz 1 nicht sicherstellt, dass ein Unternehmer eine Online-Plattform nur unter einer dort genannten Voraussetzung nutzen kann,
 28. entgegen Artikel 30 Absatz 3 Unterabsatz 1 eine Aufforderung nicht, nicht richtig oder nicht rechtzeitig vornimmt,
 29. entgegen Artikel 30 Absatz 5 Satz 1 eine Information nicht oder nicht mindestens sechs Monate speichert,
 30. entgegen Artikel 30 Absatz 6 eine Information weitergibt,
 31. entgegen Artikel 30 Absatz 7 eine Information nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht spätestens mit Anbieten der Online-Plattform zur Verfügung stellt,
 32. entgegen Artikel 31 Absatz 1 Unterabsatz 1 oder Absatz 2 nicht sicherstellt, dass eine Online-Schnittstelle in dort genannter Weise konzipiert oder organisiert ist, oder
 33. entgegen Artikel 32 Absatz 2 eine Information nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht unverzüglich nach Kenntnisnahme zugänglich macht.
- (6) Die Ordnungswidrigkeit kann geahndet werden
1. in den Fällen der
 - a) Absätze 1 und 3 Nummer 1, 3, 4, 9, 10 und 11 und
 - b) Absätze 4 und 5 Nummer 8, 10 bis 12, 14, 16, 18, 20 bis 30 und 32 mit einer Geldbuße bis zu dreihunderttausend Euro,
 2. in den Fällen des
 - a) Absatzes 3 Nummer 2, 5 bis 8, 12 bis 14 und 15 und
 - b) Absatzes 5 Nummer 1 bis 7, 9, 13, 15, 17, 19, 31 und 33mit einer Geldbuße bis zu hunderttausend Euro und
 3. in den Fällen des Absatzes 2 mit einer Geldbuße bis zu fünfzigtausend Euro.
- (7) Bei einer juristischen Person oder Personenvereinigung mit einem Jahresumsatz von mehr als
1. 5 Millionen Euro kann abweichend von Absatz 6 Nummer 1 Buchstabe b eine dort genannte Ordnungswidrigkeit mit einer Geldbuße bis zu 6 Prozent,
 2. 10 Millionen Euro kann abweichend von Absatz 6 Nummer 2 Buchstabe b eine dort genannte Ordnungswidrigkeit mit einer Geldbuße bis zu 1 Prozent des Jahresumsatzes geahndet werden, der von der juristischen Person oder Personenvereinigung weltweit in dem Geschäftsjahr erzielt wurde, das der Behördenentscheidung vorausgeht.
- (8) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen
1. des Absatzes 2 Nummer 3 Buchstabe a und Nummer 4 Buchstabe a und des Absatzes 5 Nummer 1 bis 5, 7 bis 22, 24, 25 und 27 bis 33 die Koordinierungsstelle für digitale Dienste,

2. des Absatzes 2 Nummer 3 Buchstabe b und Nummer 4 Buchstabe b und des Absatzes 3 die Bundesnetzagentur,
3. des Absatzes 5 Nummer 6 die Bundeszentrale für Kinder- und Jugendmedienschutz, soweit sie nach § 12 Absatz 2 Satz 1 für die Durchsetzung des Artikels 14 Absatz 3 der Verordnung (EU) 2022/2065 zuständig ist,
4. des Absatzes 5 Nummer 23 und 26 der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Medienstaatsvertrag (MStV)

§ 18 Informationspflichten und Auskunftsrechte

(1) Anbieter von Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen, haben folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. Name und Anschrift sowie
2. bei juristischen Personen auch Name und Anschrift des Vertretungsberechtigten.

(2) Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten, in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden, haben zusätzlich zu den Angaben nach den §§ 5 und 6 des Telemediengesetzes einen Verantwortlichen mit Angabe des Namens und der Anschrift zu benennen. Werden mehrere Verantwortliche benannt, ist kenntlich zu machen, für welchen Teil des Dienstes der jeweils Benannte verantwortlich ist. Als Verantwortlicher darf nur benannt werden, wer

1. seinen ständigen Aufenthalt im Inland hat,
2. die Fähigkeit, öffentliche Ämter zu bekleiden, nicht durch Richterspruch verloren hat,
3. unbeschränkt geschäftsfähig ist und
4. unbeschränkt strafrechtlich verfolgt werden kann.

Satz 3 Nr. 3 und 4 gilt nicht für Jugendliche, die Telemedien verantworten, die für Jugendliche bestimmt sind.

(3) Anbieter von Telemedien in sozialen Netzwerken sind verpflichtet, bei mittels eines Computerprogramms automatisiert erstellten Inhalten oder Mitteilungen den Umstand der Automatisierung kenntlich zu machen, sofern das hierfür verwandte Nutzerkonto seinem äußeren Erscheinungsbild nach für die Nutzung durch natürliche Personen bereitgestellt wurde. Dem Inhalt oder der Mitteilung ist der Hinweis gut lesbar bei- oder voranzustellen, dass dieser oder diese unter Einsatz eines das Nutzerkonto steuernden Computerprogrammes automatisiert erstellt und versandt wurde. Ein Erstellen im Sinne dieser Vorschrift liegt nicht nur vor, wenn Inhalte und Mitteilungen unmittelbar vor dem Versenden automatisiert generiert werden, sondern auch, wenn bei dem Versand automatisiert auf einen vorgefertigten Inhalt oder eine vorprogrammierte Mitteilung zurückgegriffen wird.

(4) Für Anbieter von Telemedien nach Absatz 2 Satz 1 gilt § 5 entsprechend.

UrhG - Gesetz über Urheberrecht und verwandte Schutzrechte

§ 1 Allgemeines

Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes.

§ 2 Geschützte Werke

(1) Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören insbesondere:

1. Sprachwerke, wie Schriftwerke, Reden und Computerprogramme;
2. Werke der Musik;

3. pantomimische Werke einschließlich der Werke der Tanzkunst;
4. Werke der bildenden Künste einschließlich der Werke der Baukunst und der angewandten Kunst und Entwürfe solcher Werke;
5. Lichtbildwerke einschließlich der Werke, die ähnlich wie Lichtbildwerke geschaffen werden;
6. Filmwerke einschließlich der Werke, die ähnlich wie Filmwerke geschaffen werden;
7. Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen.

(2) Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen.

§ 7 Urheber

Urheber ist der Schöpfer des Werkes.

§ 11 Allgemeines

Das Urheberrecht schützt den Urheber in seinen geistigen und persönlichen Beziehungen zum Werk und in der Nutzung des Werkes. Es dient zugleich der Sicherung einer angemessenen Vergütung für die Nutzung des Werkes.

§ 12 Veröffentlichungsrecht

(1) Der Urheber hat das Recht zu bestimmen, ob und wie sein Werk zu veröffentlichen ist.

(2) Dem Urheber ist es vorbehalten, den Inhalt seines Werkes öffentlich mitzuteilen oder zu beschreiben, solange weder das Werk noch der wesentliche Inhalt oder eine Beschreibung des Werkes mit seiner Zustimmung veröffentlicht ist.

§ 15 Allgemeines

(1) Der Urheber hat das ausschließliche Recht, sein Werk in körperlicher Form zu verwerten; das Recht umfaßt insbesondere

1. das Vervielfältigungsrecht (§ 16),
2. das Verbreitungsrecht (§ 17),
3. das Ausstellungsrecht (§ 18).

(2) Der Urheber hat ferner das ausschließliche Recht, sein Werk in unkörperlicher Form öffentlich wiederzugeben (Recht der öffentlichen Wiedergabe). Das Recht der öffentlichen Wiedergabe umfaßt insbesondere

1. das Vortrags-, Aufführungs- und Vorführungsrecht (§ 19),
2. das Recht der öffentlichen Zugänglichmachung (§ 19a),
3. das Senderecht (§ 20),
4. das Recht der Wiedergabe durch Bild- oder Tonträger (§ 21),
5. das Recht der Wiedergabe von Funksendungen und von öffentlicher Zugänglichmachung (§ 22).

(3) Die Wiedergabe ist öffentlich, wenn sie für eine Mehrzahl von Mitgliedern der Öffentlichkeit bestimmt ist. Zur Öffentlichkeit gehört jeder, der nicht mit demjenigen, der das Werk verwertet, oder mit den anderen Personen, denen das Werk in unkörperlicher Form wahrnehmbar oder zugänglich gemacht wird, durch persönliche Beziehungen verbunden ist.

§ 16 Vervielfältigungsrecht

(1) Das Vervielfältigungsrecht ist das Recht, Vervielfältigungsstücke des Werkes herzustellen, gleichviel ob vorübergehend oder dauerhaft, in welchem Verfahren und in welcher Zahl.

(2) Eine Vervielfältigung ist auch die Übertragung des Werkes auf Vorrichtungen zur wiederholbaren Wiedergabe von Bild- oder Tonfolgen (Bild- oder Tonträger), gleichviel, ob es sich um die Aufnahme einer Wiedergabe des Werkes auf einen Bild- oder Tonträger oder um die Übertragung des Werkes von einem Bild- oder Tonträger auf einen anderen handelt.

§ 17 Verbreitungsrecht

(1) Das Verbreitungsrecht ist das Recht, das Original oder Vervielfältigungsstücke des Werkes der Öffentlichkeit anzubieten oder in Verkehr zu bringen.

(2) Sind das Original oder Vervielfältigungsstücke des Werkes mit Zustimmung des zur Verbreitung Berechtigten im Gebiet der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum im Wege der Veräußerung in Verkehr gebracht worden, so ist ihre Weiterverbreitung mit Ausnahme der Vermietung zulässig.

(3) Vermietung im Sinne der Vorschriften dieses Gesetzes ist die zeitlich begrenzte, unmittelbar oder mittelbar Erwerbszwecken dienende Gebrauchsüberlassung. Als Vermietung gilt jedoch nicht die Überlassung von Originalen oder Vervielfältigungsstücken

1. von Bauwerken und Werken der angewandten Kunst oder
2. im Rahmen eines Arbeits- oder Dienstverhältnisses zu dem ausschließlichen Zweck, bei der Erfüllung von Verpflichtungen aus dem Arbeits- oder Dienstverhältnis benutzt zu werden.

§ 19a Recht der öffentlichen Zugänglichmachung

Das Recht der öffentlichen Zugänglichmachung ist das Recht, das Werk drahtgebunden oder drahtlos der Öffentlichkeit in einer Weise zugänglich zu machen, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist.

§ 21 Recht der Wiedergabe durch Bild- oder Tonträger

Das Recht der Wiedergabe durch Bild- oder Tonträger ist das Recht, Vorträge oder Aufführungen des Werkes mittels Bild- oder Tonträger öffentlich wahrnehmbar zu machen. § 19 Abs. 3 gilt entsprechend.

§ 23 Bearbeitungen und Umgestaltungen

(1) Bearbeitungen oder andere Umgestaltungen eines Werkes, insbesondere auch einer Melodie, dürfen nur mit Zustimmung des Urhebers veröffentlicht oder verwertet werden. Wahrt das neu geschaffene Werk einen hinreichenden Abstand zum benutzten Werk, so liegt keine Bearbeitung oder Umgestaltung im Sinne des Satzes 1 vor.

(2) Handelt es sich um

1. die Verfilmung eines Werkes,
2. die Ausführung von Plänen und Entwürfen eines Werkes der bildenden Künste,
3. den Nachbau eines Werkes der Baukunst oder
4. die Bearbeitung oder Umgestaltung eines Datenbankwerkes,

so bedarf bereits das Herstellen der Bearbeitung oder Umgestaltung der Zustimmung des Urhebers.

(3) Auf ausschließlich technisch bedingte Änderungen eines Werkes bei Nutzungen nach § 44b Absatz 2, § 60d Absatz 1, § 60e Absatz 1 sowie § 60f Absatz 2 sind die Absätze 1 und 2 nicht anzuwenden.

§ 25 Zugang zu Werkstücken

(1) Der Urheber kann vom Besitzer des Originals oder eines Vervielfältigungsstückes seines Werkes verlangen, daß er ihm das Original oder das Vervielfältigungsstück zugänglich macht, soweit dies zur Herstellung von Vervielfältigungsstücken oder Bearbeitungen des Werkes erforderlich ist und nicht berechnete Interessen des Besitzers entgegenstehen.

(2) Der Besitzer ist nicht verpflichtet, das Original oder das Vervielfältigungsstück dem Urheber herauszugeben.

§ 28 Vererbung des Urheberrechts

(1) Das Urheberrecht ist vererblich.

(2) Der Urheber kann durch letztwillige Verfügung die Ausübung des Urheberrechts einem Testamentsvollstrecker übertragen. § 2210 des Bürgerlichen Gesetzbuchs ist nicht anzuwenden.

§ 29 Rechtsgeschäfte über das Urheberrecht

(1) Das Urheberrecht ist nicht übertragbar, es sei denn, es wird in Erfüllung einer Verfügung von Todes wegen oder an Miterben im Wege der Erbauseinandersetzung übertragen.

(2) Zulässig sind die Einräumung von Nutzungsrechten (§ 31), schuldrechtliche Einwilligungen und Vereinbarungen zu Verwertungsrechten sowie die in § 39 geregelten Rechtsgeschäfte über Urheberpersönlichkeitsrechte.

§ 30 Rechtsnachfolger des Urhebers

Der Rechtsnachfolger des Urhebers hat die dem Urheber nach diesem Gesetz zustehenden Rechte, soweit nichts anderes bestimmt ist.

§ 31 Einräumung von Nutzungsrechten

(1) Der Urheber kann einem anderen das Recht einräumen, das Werk auf einzelne oder alle Nutzungsarten zu nutzen (Nutzungsrecht). Das Nutzungsrecht kann als einfaches oder ausschließliches Recht sowie räumlich, zeitlich oder inhaltlich beschränkt eingeräumt werden.

(2) Das einfache Nutzungsrecht berechtigt den Inhaber, das Werk auf die erlaubte Art zu nutzen, ohne dass eine Nutzung durch andere ausgeschlossen ist.

(3) Das ausschließliche Nutzungsrecht berechtigt den Inhaber, das Werk unter Ausschluss aller anderen Personen auf die ihm erlaubte Art zu nutzen und Nutzungsrechte einzuräumen. Es kann bestimmt werden, dass die Nutzung durch den Urheber vorbehalten bleibt. § 35 bleibt unberührt.

(4) (weggefallen)

(5) Sind bei der Einräumung eines Nutzungsrechts die Nutzungsarten nicht ausdrücklich einzeln bezeichnet, so bestimmt sich nach dem von beiden Partnern zugrunde gelegten Vertragszweck, auf welche Nutzungsarten es sich erstreckt. Entsprechendes gilt für die Frage, ob ein Nutzungsrecht eingeräumt wird, ob es sich um ein einfaches oder ausschließliches Nutzungsrecht handelt, wie weit Nutzungsrecht und Verbotswort reichen und welchen Einschränkungen das Nutzungsrecht unterliegt.

§ 32 Angemessene Vergütung

(1) Der Urheber hat für die Einräumung von Nutzungsrechten und die Erlaubnis zur Werknutzung Anspruch auf die vertraglich vereinbarte Vergütung. Ist die Höhe der Vergütung nicht bestimmt, gilt die angemessene Vergütung als vereinbart. Soweit die vereinbarte Vergütung nicht angemessen ist, kann der Urheber von seinem Vertragspartner die Einwilligung in die Änderung des Vertrages verlangen, durch die dem Urheber die angemessene Vergütung gewährt wird.

(2) Eine nach einer gemeinsamen Vergütungsregel (§ 36) ermittelte Vergütung ist angemessen. Im Übrigen ist die Vergütung angemessen, wenn sie im Zeitpunkt des Vertragsschlusses dem entspricht, was im Geschäftsverkehr nach Art und Umfang der eingeräumten Nutzungsmöglichkeit, insbesondere nach Dauer, Häufigkeit, Ausmaß und Zeitpunkt der Nutzung, unter Berücksichtigung aller Umstände üblicher- und redlicherweise zu leisten ist. Eine pauschale Vergütung muss eine angemessene Beteiligung des Urhebers am voraussichtlichen Gesamtertrag der Nutzung gewährleisten und durch die Besonderheiten der Branche gerechtfertigt sein.

(2a) Eine gemeinsame Vergütungsregel kann zur Ermittlung der angemessenen Vergütung auch bei Verträgen herangezogen werden, die vor ihrem zeitlichen Anwendungsbereich abgeschlossen wurden.

(3) Auf eine Vereinbarung, die zum Nachteil des Urhebers von den Absätzen 1 bis 2a abweicht, kann der Vertragspartner sich nicht berufen. Die in Satz 1 bezeichneten Vorschriften finden auch Anwendung, wenn sie

durch anderweitige Gestaltungen umgangen werden. Der Urheber kann aber unentgeltlich ein einfaches Nutzungsrecht für jedermann einräumen.

(4) Der Urheber hat keinen Anspruch nach Absatz 1 Satz 3, soweit die Vergütung für die Nutzung seiner Werke tarifvertraglich bestimmt ist.

§ 45 Rechtspflege und öffentliche Sicherheit

(1) Zulässig ist, einzelne Vervielfältigungsstücke von Werken zur Verwendung in Verfahren vor einem Gericht, einem Schiedsgericht oder einer Behörde herzustellen oder herstellen zu lassen.

(2) Gerichte und Behörden dürfen für Zwecke der Rechtspflege und der öffentlichen Sicherheit Bildnisse vervielfältigen oder vervielfältigen lassen.

(3) Unter den gleichen Voraussetzungen wie die Vervielfältigung ist auch die Verbreitung, öffentliche Ausstellung und öffentliche Wiedergabe der Werke zulässig.

§ 49 Zeitungsartikel und Rundfunkkommentare

(1) Zulässig ist die Vervielfältigung und Verbreitung einzelner Rundfunkkommentare und einzelner Artikel sowie mit ihnen im Zusammenhang veröffentlichter Abbildungen aus Zeitungen und anderen lediglich Tagesinteressen dienenden Informationsblättern in anderen Zeitungen und Informationsblättern dieser Art sowie die öffentliche Wiedergabe solcher Kommentare, Artikel und Abbildungen, wenn sie politische, wirtschaftliche oder religiöse Tagesfragen betreffen und nicht mit einem Vorbehalt der Rechte versehen sind. Für die Vervielfältigung, Verbreitung und öffentliche Wiedergabe ist dem Urheber eine angemessene Vergütung zu zahlen, es sei denn, daß es sich um eine Vervielfältigung, Verbreitung oder öffentliche Wiedergabe kurzer Auszüge aus mehreren Kommentaren oder Artikeln in Form einer Übersicht handelt. Der Anspruch kann nur durch eine Verwertungsgesellschaft geltend gemacht werden.

(2) Unbeschränkt zulässig ist die Vervielfältigung, Verbreitung und öffentliche Wiedergabe von vermischten Nachrichten tatsächlichen Inhalts und von Tagesneuigkeiten, die durch Presse oder Funk veröffentlicht worden sind; ein durch andere gesetzliche Vorschriften gewährter Schutz bleibt unberührt.

§ 50 Berichterstattung über Tagesereignisse

Zur Berichterstattung über Tagesereignisse durch Funk oder durch ähnliche technische Mittel, in Zeitungen, Zeitschriften und in anderen Druckschriften oder sonstigen Datenträgern, die im Wesentlichen Tagesinteressen Rechnung tragen, sowie im Film, ist die Vervielfältigung, Verbreitung und öffentliche Wiedergabe von Werken, die im Verlauf dieser Ereignisse wahrnehmbar werden, in einem durch den Zweck gebotenen Umfang zulässig.

§ 51 Zitate

Zulässig ist die Vervielfältigung, Verbreitung und öffentliche Wiedergabe eines veröffentlichten Werkes zum Zweck des Zitats, sofern die Nutzung in ihrem Umfang durch den besonderen Zweck gerechtfertigt ist. Zulässig ist dies insbesondere, wenn

1. einzelne Werke nach der Veröffentlichung in ein selbständiges wissenschaftliches Werk zur Erläuterung des Inhalts aufgenommen werden,
2. Stellen eines Werkes nach der Veröffentlichung in einem selbständigen Sprachwerk angeführt werden,
3. einzelne Stellen eines erschienenen Werkes der Musik in einem selbständigen Werk der Musik angeführt werden.

Von der Zitierbefugnis gemäß den Sätzen 1 und 2 umfasst ist die Nutzung einer Abbildung oder sonstigen Vervielfältigung des zitierten Werkes, auch wenn diese selbst durch ein Urheberrecht oder ein verwandtes Schutzrecht geschützt ist.

§ 53 Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch

(1) Zulässig sind einzelne Vervielfältigungen eines Werkes durch eine natürliche Person zum privaten Gebrauch auf beliebigen Trägern, sofern sie weder unmittelbar noch mittelbar Erwerbszwecken dienen, soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage

verwendet wird. Der zur Vervielfältigung Befugte darf die Vervielfältigungsstücke auch durch einen anderen herstellen lassen, sofern dies unentgeltlich geschieht oder es sich um Vervielfältigungen auf Papier oder einem ähnlichen Träger mittels beliebiger photomechanischer Verfahren oder anderer Verfahren mit ähnlicher Wirkung handelt.

(2) Zulässig ist, einzelne Vervielfältigungsstücke eines Werkes herzustellen oder herstellen zu lassen

1. (weggefallen)

2. zur Aufnahme in ein eigenes Archiv, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und als Vorlage für die Vervielfältigung ein eigenes Werkstück benutzt wird,

3. zur eigenen Unterrichtung über Tagesfragen, wenn es sich um ein durch Funk gesendetes Werk handelt,

4. zum sonstigen eigenen Gebrauch,

a) wenn es sich um kleine Teile eines erschienenen Werkes oder um einzelne Beiträge handelt, die in Zeitungen oder Zeitschriften erschienen sind,

b) wenn es sich um ein seit mindestens zwei Jahren vergriffenes Werk handelt.

Dies gilt nur, wenn zusätzlich

1. die Vervielfältigung auf Papier oder einem ähnlichen Träger mittels beliebiger photomechanischer Verfahren oder anderer Verfahren mit ähnlicher Wirkung vorgenommen wird oder

2. eine ausschließlich analoge Nutzung stattfindet.

(3) (weggefallen)

(4) Die Vervielfältigung

a) graphischer Aufzeichnungen von Werken der Musik,

b) eines Buches oder einer Zeitschrift, wenn es sich um eine im wesentlichen vollständige Vervielfältigung handelt,

ist, soweit sie nicht durch Abschreiben vorgenommen wird, stets nur mit Einwilligung des Berechtigten zulässig oder unter den Voraussetzungen des Absatzes 2 Satz 1 Nr. 2 oder zum eigenen Gebrauch, wenn es sich um ein seit mindestens zwei Jahren vergriffenes Werk handelt.

(5) Die Absätze 1 und 2 Satz 1 Nr. 2 bis 4 finden keine Anwendung auf Datenbankwerke, deren Elemente einzeln mit Hilfe elektronischer Mittel zugänglich sind.

(6) Die Vervielfältigungsstücke dürfen weder verbreitet noch zu öffentlichen Wiedergaben benutzt werden. Zulässig ist jedoch, rechtmäßig hergestellte Vervielfältigungsstücke von Zeitungen und vergriffenen Werken sowie solche Werkstücke zu verleihen, bei denen kleine beschädigte oder abhanden gekommene Teile durch Vervielfältigungsstücke ersetzt worden sind.

(7) Die Aufnahme öffentlicher Vorträge, Aufführungen oder Vorführungen eines Werkes auf Bild- oder Tonträger, die Ausführung von Plänen und Entwürfen zu Werken der bildenden Künste und der Nachbau eines Werkes der Baukunst sind stets nur mit Einwilligung des Berechtigten zulässig.

§ 54 Vergütungspflicht

(1) Lässt die Art des Werkes eine nach § 53 Absatz 1 oder 2 oder den §§ 60a bis 60f erlaubte Vervielfältigung erwarten, so hat der Urheber des Werkes gegen den Hersteller von Geräten und von Speichermedien, deren Typ allein oder in Verbindung mit anderen Geräten, Speichermedien oder Zubehör zur Vornahme solcher Vervielfältigungen benutzt wird, Anspruch auf Zahlung einer angemessenen Vergütung.

(2) Der Anspruch nach Absatz 1 entfällt, soweit nach den Umständen erwartet werden kann, dass die Geräte oder Speichermedien im Geltungsbereich dieses Gesetzes nicht zu Vervielfältigungen benutzt werden.

§ 57 Unwesentliches Beiwerk

Zulässig ist die Vervielfältigung, Verbreitung und öffentliche Wiedergabe von Werken, wenn sie als unwesentliches Beiwerk neben dem eigentlichen Gegenstand der Vervielfältigung, Verbreitung oder öffentlichen Wiedergabe anzusehen sind.

§ 54a Vergütungshöhe

(1) Maßgebend für die Vergütungshöhe ist, in welchem Maß die Geräte und Speichermedien als Typen tatsächlich für Vervielfältigungen nach § 53 Absatz 1 oder 2 oder den §§ 60a bis 60f genutzt werden. Dabei ist zu berücksichtigen, inwieweit technische Schutzmaßnahmen nach § 95a auf die betreffenden Werke angewendet werden.

(2) Die Vergütung für Geräte ist so zu gestalten, dass sie auch mit Blick auf die Vergütungspflicht für in diesen Geräten enthaltene Speichermedien oder andere, mit diesen funktionell zusammenwirkende Geräte oder Speichermedien insgesamt angemessen ist.

(3) Bei der Bestimmung der Vergütungshöhe sind die nutzungsrelevanten Eigenschaften der Geräte und Speichermedien, insbesondere die Leistungsfähigkeit von Geräten sowie die Speicherkapazität und Mehrfachbeschreibbarkeit von Speichermedien, zu berücksichtigen.

(4) Die Vergütung darf Hersteller von Geräten und Speichermedien nicht unzumutbar beeinträchtigen; sie muss in einem wirtschaftlich angemessenen Verhältnis zum Preisniveau des Geräts oder des Speichermediums stehen.

§ 60a Unterricht und Lehre

(1) Zur Veranschaulichung des Unterrichts und der Lehre an Bildungseinrichtungen dürfen zu nicht kommerziellen Zwecken bis zu 15 Prozent eines veröffentlichten Werkes vervielfältigt, verbreitet, öffentlich zugänglich gemacht und in sonstiger Weise öffentlich wiedergegeben werden

1. für Lehrende und Teilnehmer der jeweiligen Veranstaltung,
2. für Lehrende und Prüfer an derselben Bildungseinrichtung sowie
3. für Dritte, soweit dies der Präsentation des Unterrichts, von Unterrichts- oder Lernergebnissen an der Bildungseinrichtung dient.

(2) Abbildungen, einzelne Beiträge aus derselben Fachzeitschrift oder wissenschaftlichen Zeitschrift, sonstige Werke geringen Umfangs und vergriffene Werke dürfen abweichend von Absatz 1 vollständig genutzt werden.

(3) Nicht nach den Absätzen 1 und 2 erlaubt sind folgende Nutzungen:

1. Vervielfältigung durch Aufnahme auf Bild- oder Tonträger und öffentliche Wiedergabe eines Werkes, während es öffentlich vorgetragen, aufgeführt oder vorgeführt wird,
2. Vervielfältigung, Verbreitung und öffentliche Wiedergabe eines Werkes, das ausschließlich für den Unterricht an Schulen geeignet, bestimmt und entsprechend gekennzeichnet ist, an Schulen sowie
3. Vervielfältigung von grafischen Aufzeichnungen von Werken der Musik, soweit sie nicht für die öffentliche Zugänglichmachung nach den Absätzen 1 oder 2 erforderlich ist.

Satz 1 ist nur anzuwenden, wenn Lizenzen für diese Nutzungen leicht verfügbar und auffindbar sind, den Bedürfnissen und Besonderheiten von Bildungseinrichtungen entsprechen und Nutzungen nach Satz 1 Nummer 1 bis 3 erlauben.

(3a) Werden Werke in gesicherten elektronischen Umgebungen für die in Absatz 1 Nummer 1 und 2 sowie Absatz 2 genannten Zwecke in Mitgliedstaaten der Europäischen Union und Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genutzt, so gilt diese Nutzung nur als in dem Mitgliedstaat oder Vertragsstaat erfolgt, in dem die Bildungseinrichtung ihren Sitz hat.

(4) Bildungseinrichtungen sind frühkindliche Bildungseinrichtungen, Schulen, Hochschulen sowie Einrichtungen der Berufsbildung oder der sonstigen Aus- und Weiterbildung.

§ 60b Unterrichts- und Lehrmedien

(1) Hersteller von Unterrichts- und Lehrmedien dürfen für solche Sammlungen bis zu 10 Prozent eines veröffentlichten Werkes vervielfältigen, verbreiten und öffentlich zugänglich machen.

(2) § 60a Absatz 2 und 3 Satz 1 ist entsprechend anzuwenden.

(3) Unterrichts- und Lehrmedien im Sinne dieses Gesetzes sind Sammlungen, die Werke einer größeren Anzahl von Urhebern vereinigen und ausschließlich zur Veranschaulichung des Unterrichts und der Lehre an Bildungseinrichtungen (§ 60a) zu nicht kommerziellen Zwecken geeignet, bestimmt und entsprechend gekennzeichnet sind.

§ 60c Wissenschaftliche Forschung

(1) Zum Zweck der nicht kommerziellen wissenschaftlichen Forschung dürfen bis zu 15 Prozent eines Werkes vervielfältigt, verbreitet und öffentlich zugänglich gemacht werden

1. für einen bestimmt abgegrenzten Kreis von Personen für deren eigene wissenschaftliche Forschung sowie
2. für einzelne Dritte, soweit dies der Überprüfung der Qualität wissenschaftlicher Forschung dient.

(2) Für die eigene wissenschaftliche Forschung dürfen bis zu 75 Prozent eines Werkes vervielfältigt werden.

(3) Abbildungen, einzelne Beiträge aus derselben Fachzeitschrift oder wissenschaftlichen Zeitschrift, sonstige Werke geringen Umfangs und vergriffene Werke dürfen abweichend von den Absätzen 1 und 2 vollständig genutzt werden.

(4) Nicht nach den Absätzen 1 bis 3 erlaubt ist es, während öffentlicher Vorträge, Aufführungen oder Vorführungen eines Werkes diese auf Bild- oder Tonträger aufzunehmen und später öffentlich zugänglich zu machen.

§ 63 Quellenangabe

(1) Wenn ein Werk oder ein Teil eines Werkes in den Fällen des § 45 Abs. 1, der §§ 45a bis 48, 50, 51, 58, 59 sowie der §§ 60a bis 60c, 61, 61c, 61d und 61f vervielfältigt oder verbreitet wird, ist stets die Quelle deutlich anzugeben. Bei der Vervielfältigung oder Verbreitung ganzer Sprachwerke oder ganzer Werke der Musik ist neben dem Urheber auch der Verlag anzugeben, in dem das Werk erschienen ist, und außerdem kenntlich zu machen, ob an dem Werk Kürzungen oder andere Änderungen vorgenommen worden sind. Die Verpflichtung zur Quellenangabe entfällt, wenn die Quelle weder auf dem benutzten Werkstück oder bei der benutzten Werkwiedergabe genannt noch dem zur Vervielfältigung oder Verbreitung Befugten anderweit bekannt ist oder im Fall des § 60a oder des § 60b Prüfungszwecke einen Verzicht auf die Quellenangabe erfordern.

(2) Soweit nach den Bestimmungen dieses Abschnitts die öffentliche Wiedergabe eines Werkes zulässig ist, ist die Quelle deutlich anzugeben, wenn und soweit die Verkehrssitte es erfordert. In den Fällen der öffentlichen Wiedergabe nach den §§ 46, 48, 51, 60a bis 60d, 61, 61c, 61d und 61f sowie bei digitalen sonstigen Nutzungen gemäß § 60a ist die Quelle einschließlich des Namens des Urhebers stets anzugeben, es sei denn, dass dies nicht möglich ist.

(3) Wird ein Artikel aus einer Zeitung oder einem anderen Informationsblatt nach § 49 Abs. 1 in einer anderen Zeitung oder in einem anderen Informationsblatt abgedruckt oder durch Funk gesendet, so ist stets außer dem Urheber, der in der benutzten Quelle bezeichnet ist, auch die Zeitung oder das Informationsblatt anzugeben, woraus der Artikel entnommen ist; ist dort eine andere Zeitung oder ein anderes Informationsblatt als Quelle angeführt, so ist diese Zeitung oder dieses Informationsblatt anzugeben. Wird ein Rundfunkkommentar nach § 49 Abs. 1 in einer Zeitung oder einem anderen Informationsblatt abgedruckt oder durch Funk gesendet, so ist stets außer dem Urheber auch das Sendeunternehmen anzugeben, das den Kommentar gesendet hat.

§ 64 Allgemeines

Das Urheberrecht erlischt siebenzig Jahre nach dem Tode des Urhebers.

Abschnitt 8

Besondere Bestimmungen für Computerprogramme

§ 69a Gegenstand des Schutzes

- (1) Computerprogramme im Sinne dieses Gesetzes sind Programme in jeder Gestalt, einschließlich des Entwurfsmaterials.
- (2) Der gewährte Schutz gilt für alle Ausdrucksformen eines Computerprogramms. Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrundeliegenden Ideen und Grundsätze, sind nicht geschützt.
- (3) Computerprogramme werden geschützt, wenn sie individuelle Werke in dem Sinne darstellen, daß sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind. Zur Bestimmung ihrer Schutzfähigkeit sind keine anderen Kriterien, insbesondere nicht qualitative oder ästhetische, anzuwenden.
- (4) Auf Computerprogramme finden die für Sprachwerke geltenden Bestimmungen Anwendung, soweit in diesem Abschnitt nichts anderes bestimmt ist.
- (5) Die §§ 32 bis 32g, 36 bis 36d, 40a und 41 sind auf Computerprogramme nicht anzuwenden.

§ 69b Urheber in Arbeits- und Dienstverhältnissen

- (1) Wird ein Computerprogramm von einem Arbeitnehmer in Wahrnehmung seiner Aufgaben oder nach den Anweisungen seines Arbeitgebers geschaffen, so ist ausschließlich der Arbeitgeber zur Ausübung aller vermögensrechtlichen Befugnisse an dem Computerprogramm berechtigt, sofern nichts anderes vereinbart ist.
- (2) Absatz 1 ist auf Dienstverhältnisse entsprechend anzuwenden.

§ 72 Lichtbilder

- (1) Lichtbilder und Erzeugnisse, die ähnlich wie Lichtbilder hergestellt werden, werden in entsprechender Anwendung der für Lichtbildwerke geltenden Vorschriften des Teils 1 geschützt.
- (2) Das Recht nach Absatz 1 steht dem Lichtbildner zu.
- (3) Das Recht nach Absatz 1 erlischt fünfzig Jahre nach dem Erscheinen des Lichtbildes oder, wenn seine erste erlaubte öffentliche Wiedergabe früher erfolgt ist, nach dieser, jedoch bereits fünfzig Jahre nach der Herstellung, wenn das Lichtbild innerhalb dieser Frist nicht erschienen oder erlaubterweise öffentlich wiedergegeben worden ist. Die Frist ist nach § 69 zu berechnen.

§ 97 Anspruch auf Unterlassung und Schadensersatz

- (1) Wer das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht widerrechtlich verletzt, kann von dem Verletzten auf Beseitigung der Beeinträchtigung, bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der Anspruch auf Unterlassung besteht auch dann, wenn eine Zuwiderhandlung erstmalig droht.
- (2) Wer die Handlung vorsätzlich oder fahrlässig vornimmt, ist dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet. Bei der Bemessung des Schadensersatzes kann auch der Gewinn, den der Verletzer durch die Verletzung des Rechts erzielt hat, berücksichtigt werden. Der Schadensersatzanspruch kann auch auf der Grundlage des Betrages berechnet werden, den der Verletzer als angemessene Vergütung hätte entrichten müssen, wenn er die Erlaubnis zur Nutzung des verletzten Rechts eingeholt hätte. Urheber, Verfasser wissenschaftlicher Ausgaben (§ 70), Lichtbildner (§ 72) und ausübende Künstler (§ 73) können auch wegen des Schadens, der nicht Vermögensschaden ist, eine Entschädigung in Geld verlangen, wenn und soweit dies der Billigkeit entspricht.

§ 97a Abmahnung

- (1) Der Verletzte soll den Verletzer vor Einleitung eines gerichtlichen Verfahrens auf Unterlassung abmahnen und ihm Gelegenheit geben, den Streit durch Abgabe einer mit einer angemessenen Vertragsstrafe bewehrten Unterlassungsverpflichtung beizulegen.
- (2) Die Abmahnung hat in klarer und verständlicher Weise
 1. Name oder Firma des Verletzten anzugeben, wenn der Verletzte nicht selbst, sondern ein Vertreter abmahnt,

2. die Rechtsverletzung genau zu bezeichnen,
3. geltend gemachte Zahlungsansprüche als Schadensersatz- und Aufwendungsersatzansprüche aufzuschlüsseln und
4. wenn darin eine Aufforderung zur Abgabe einer Unterlassungsverpflichtung enthalten ist, anzugeben, ob die vorgeschlagene Unterlassungsverpflichtung erheblich über die abgemahnte Rechtsverletzung hinausgeht.

Eine Abmahnung, die nicht Satz 1 entspricht, ist unwirksam.

(3) Soweit die Abmahnung berechtigt ist und Absatz 2 Satz 1 Nummer 1 bis 4 entspricht, kann der Ersatz der erforderlichen Aufwendungen verlangt werden. Für die Inanspruchnahme anwaltlicher Dienstleistungen beschränkt sich der Ersatz der erforderlichen Aufwendungen hinsichtlich der gesetzlichen Gebühren auf Gebühren nach einem Gegenstandswert für den Unterlassungs- und Beseitigungsanspruch von 1 000 Euro, wenn der Abgemahnte

1. eine natürliche Person ist, die nach diesem Gesetz geschützte Werke oder andere nach diesem Gesetz geschützte Schutzgegenstände nicht für ihre gewerbliche oder selbständige berufliche Tätigkeit verwendet, und
2. nicht bereits wegen eines Anspruchs des Abmahnenden durch Vertrag, auf Grund einer rechtskräftigen gerichtlichen Entscheidung oder einer einstweiligen Verfügung zur Unterlassung verpflichtet ist.

Der in Satz 2 genannte Wert ist auch maßgeblich, wenn ein Unterlassungs- und ein Beseitigungsanspruch nebeneinander geltend gemacht werden. Satz 2 gilt nicht, wenn der genannte Wert nach den besonderen Umständen des Einzelfalles unbillig ist.

(4) Soweit die Abmahnung unberechtigt oder unwirksam ist, kann der Abgemahnte Ersatz der für seine Rechtsverteidigung erforderlichen Aufwendungen verlangen, es sei denn, es war für den Abmahnenden zum Zeitpunkt der Abmahnung nicht erkennbar, dass die Abmahnung unberechtigt war. Weitergehende Ersatzansprüche bleiben unberührt.

Unterabschnitt 2

Straf- und Bußgeldvorschriften

§ 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 108 Unerlaubte Eingriffe in verwandte Schutzrechte

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten

1. eine wissenschaftliche Ausgabe (§ 70) oder eine Bearbeitung oder Umgestaltung einer solchen Ausgabe vervielfältigt, verbreitet oder öffentlich wiedergibt,
2. ein nachgelassenes Werk oder eine Bearbeitung oder Umgestaltung eines solchen Werkes entgegen § 71 verwertet,
3. ein Lichtbild (§ 72) oder eine Bearbeitung oder Umgestaltung eines Lichtbildes vervielfältigt, verbreitet oder öffentlich wiedergibt,
4. die Darbietung eines ausübenden Künstlers entgegen den § 77 Abs. 1 oder Abs. 2 Satz 1, § 78 Abs. 1 verwertet,
5. einen Tonträger entgegen § 85 verwertet,
6. eine Funksendung entgegen § 87 verwertet,
7. einen Bildträger oder Bild- und Tonträger entgegen §§ 94 oder 95 in Verbindung mit § 94 verwertet,

8. eine Datenbank entgegen § 87b Abs. 1 verwertet,
wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 108a Gewerbsmäßige unerlaubte Verwertung

(1) Handelt der Täter in den Fällen der §§ 106 bis 108 gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(2) Der Versuch ist strafbar.

§ 109 Strafantrag

In den Fällen der §§ 106 bis 108 und des § 108b wird die Tat nur auf Antrag verfolgt, es sei denn, daß die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

§ 110 Einziehung

Gegenstände, auf die sich eine Straftat nach den §§ 106, 107 Abs. 1 Nr. 2, §§ 108 bis 108b bezieht, können eingezogen werden. § 74a des Strafgesetzbuches ist anzuwenden. Soweit den in § 98 bezeichneten Ansprüchen im Verfahren nach den Vorschriften der Strafprozeßordnung über die Entschädigung des Verletzten (§§ 403 bis 406c) stattgegeben wird, sind die Vorschriften über die Einziehung nicht anzuwenden.

StGB – Strafgesetzbuch

§ 1 Keine Strafe ohne Gesetz

Eine Tat kann nur bestraft werden, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde.

Fünftehnter Abschnitt

Verletzung des persönlichen Lebens- und Geheimbereichs

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überläßt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 263a Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 6 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er

1. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt oder

2. Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

§ 267 Urkundenfälschung

(1) Wer zur Täuschung im Rechtsverkehr eine unechte Urkunde herstellt, eine echte Urkunde verfälscht oder eine unechte oder verfälschte Urkunde gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Betrug oder Urkundenfälschung verbunden hat,

2. einen Vermögensverlust großen Ausmaßes herbeiführt,

3. durch eine große Zahl von unechten oder verfälschten Urkunden die Sicherheit des Rechtsverkehrs erheblich gefährdet oder

4. seine Befugnisse oder seine Stellung als Amtsträger oder Europäischer Amtsträger mißbraucht.

(4) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer die Urkundenfälschung als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat, gewerbsmäßig begeht.

§ 269 Fälschung beweisheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweishebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.

Siebenundzwanzigster Abschnitt

§ 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303c Strafantrag

In den Fällen der §§ 303, 303a Abs. 1 und 2 sowie § 303b Abs. 1 bis 3 wird die Tat nur auf Antrag verfolgt, es sei denn, daß die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

§ 353b Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht

(1) Wer ein Geheimnis, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt oder
4. Europäischer Amtsträger,

anvertraut worden oder sonst bekanntgeworden ist, unbefugt offenbart und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. 2 Hat der Täter durch die Tat fahrlässig wichtige öffentliche Interessen gefährdet, so wird er mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Wer, abgesehen von den Fällen des Absatzes 1, unbefugt einen Gegenstand oder eine Nachricht, zu deren Geheimhaltung er

1. auf Grund des Beschlusses eines Gesetzgebungsorgans des Bundes oder eines Landes oder eines seiner Ausschüsse verpflichtet ist oder

2. von einer anderen amtlichen Stelle unter Hinweis auf die Strafbarkeit der Verletzung der Geheimhaltungspflicht förmlich verpflichtet worden ist, an einen anderen gelangen läßt oder öffentlich bekanntmacht und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(3) Der Versuch ist strafbar.

(3a) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geheimnisses oder des Gegenstandes oder der Nachricht, zu deren Geheimhaltung eine besondere Verpflichtung besteht, beschränken.

(4) 1Die Tat wird nur mit Ermächtigung verfolgt. 2Die Ermächtigung wird erteilt

1. von dem Präsidenten des Gesetzgebungsorgans

a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit bei einem oder für ein Gesetzgebungsorgan des Bundes oder eines Landes bekanntgeworden ist,

b) in den Fällen des Absatzes 2 Nr. 1;

2. von der obersten Bundesbehörde

a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit sonst bei einer oder für eine Behörde oder bei einer anderen amtlichen Stelle des Bundes oder für eine solche Stelle bekanntgeworden ist,

b) in den Fällen des Absatzes 2 Nr. 2, wenn der Täter von einer amtlichen Stelle des Bundes verpflichtet worden ist;

3. von der Bundesregierung in den Fällen des Absatzes 1 Satz 1 Nummer 4, wenn dem Täter das Geheimnis während seiner Tätigkeit bei einer Dienststelle der Europäischen Union bekannt geworden ist;

4. von der obersten Landesbehörde in allen übrigen Fällen der Absätze 1 und 2 Nr. 2.

3In den Fällen des Satzes 2 Nummer 3 wird die Tat nur verfolgt, wenn zudem ein Strafverlangen der Dienststelle vorliegt.

StPO - Strafprozeßordnung

§ 100a Telekommunikationsüberwachung

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat auch im Einzelfall schwer wiegt und

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

1. aus dem Strafgesetzbuch:

- a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80a bis 82, 84 bis 86, 87 bis 89a, 89c Absatz 1 bis 4, 94 bis 100a,
- b) Bestechlichkeit und Bestechung von Mandatsträgern nach § 108e,
- c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,
- d) Straftaten gegen die öffentliche Ordnung nach § 127 Absatz 3 und 4 sowie den §§ 129 bis 130,
- e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,
- f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176, 176c, 176d und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,
- g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Inhalte nach § 184b, § 184c Absatz 2,
- h) Mord und Totschlag nach den §§ 211 und 212,
- i) Straftaten gegen die persönliche Freiheit nach den §§ 232, 232a Absatz 1 bis 5, den §§ 232b, 233 Absatz 2, den §§ 233a, 234, 234a, 239a und 239b,
- j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2, Wohnungseinbruchdiebstahl nach § 244 Absatz 4 und schwerer Bandendiebstahl nach § 244a,
- k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,
- l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,
- m) Geldwäsche nach § 261, wenn die Vortat eine der in den Nummern 1 bis 11 genannten schweren Straftaten ist,
- n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,
- o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,
- p) Sportwettbetrug und Manipulation von berufssportlichen Wettbewerben unter den in § 265e Satz 2 genannten Voraussetzungen,
- q) Vorenthalten und Veruntreuen von Arbeitsentgelt unter den in § 266a Absatz 4 Satz 2 Nummer 4 genannten Voraussetzungen,
- r) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,
- s) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,
- t) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,
- u) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c,
- v) Bestechlichkeit und Bestechung nach den §§ 332 und 334,

2. aus der Abgabenordnung:

a) Steuerhinterziehung unter den in § 370 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzungen, sofern der Täter als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Taten nach § 370 Absatz 1 verbunden hat, handelt, oder unter den in § 370 Absatz 3 Satz 2 Nummer 5 genannten Voraussetzungen,

b) gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,

c) Steuerhehlerei im Falle des § 374 Abs. 2,

3. aus dem Anti-Doping-Gesetz:

Straftaten nach § 4 Absatz 4 Nummer 2 Buchstabe b,

4. aus dem Asylgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,

5. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Abs. 2,

b) Einschleusen mit Todesfolge und gewerbs- und bandenmäßiges Einschleusen nach § 97,

5a. aus dem Ausgangsstoffgesetz:

Straftaten nach § 13 Absatz 3,

6. aus dem Außenwirtschaftsgesetz:

vorsätzliche Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes,

7. aus dem Betäubungsmittelgesetz:

a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,

b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,

7a. aus dem Konsumcannabisgesetz:

a) Straftaten nach einer in § 34 Absatz 3 Satz 2 Nummer 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,

b) Straftaten nach § 34 Absatz 4,

7b. aus dem Medizinal-Cannabisgesetz:

a) Straftaten nach einer in § 25 Absatz 4 Satz 2 Nummer 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,

b) Straftaten nach § 25 Absatz 5,

8. aus dem Grundstoffüberwachungsgesetz:

Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,

9. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,

b) Straftaten nach § 22a Abs. 1 bis 3,

9a. aus dem Neue-psychoaktive-Stoffe-Gesetz:

Straftaten nach § 4 Absatz 3 Nummer 1 Buchstabe a,

10. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

d) Verbrechen der Aggression nach § 13,

11. aus dem Waffengesetz:

a) Straftaten nach § 51 Abs. 1 bis 3,

b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.

(4) Auf Grund der Anordnung einer Überwachung und Aufzeichnung der Telekommunikation hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) diese Maßnahmen zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Absatz 2 gilt entsprechend.

(5) Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:

a) die laufende Telekommunikation (Absatz 1 Satz 2), oder

b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),

2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(6) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

§ 100b Online-Durchsuchung

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,
2. die Tat auch im Einzelfall besonders schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Besonders schwere Straftaten im Sinne des Absatzes 1 Nummer 1 sind:

1. aus dem Strafgesetzbuch:

a) Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 81, 82, 89a, 89c Absatz 1 bis 4, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,

b) Betreiben krimineller Handelsplattformen im Internet in den Fällen des § 127 Absatz 3 und 4, sofern der Zweck der Handelsplattform im Internet darauf ausgerichtet ist, in den Buchstaben a und c bis o sowie in den Nummern 2 bis 10 genannte besonders schwere Straftaten zu ermöglichen oder zu fördern,

c) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,

d) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,

e) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176 Absatz 1 und der §§ 176c, 176d und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

f) Verbreitung, Erwerb und Besitz kinderpornografischer Inhalte in den Fällen des § 184b Absatz 1 Satz 1 und Absatz 2,

g) Mord und Totschlag nach den §§ 211, 212,

h) Straftaten gegen die persönliche Freiheit in den Fällen des § 232 Absatz 2 und 3, des § 232a Absatz 1, 3, 4 und 5 zweiter Halbsatz, des § 232b Absatz 1 und 3 sowie Absatz 4, dieser in Verbindung mit § 232a Absatz 4 und 5 zweiter Halbsatz, des § 233 Absatz 2, des § 233a Absatz 1, 3 und 4 zweiter Halbsatz, der §§ 234 und 234a Absatz 1 und 2 sowie der §§ 239a und 239b,

i) Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a,

j) schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251,

k) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen,

l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,

m) besonders schwerer Fall der Geldwäsche nach § 261 unter den in § 261 Absatz 5 Satz 2 genannten Voraussetzungen, wenn die Vortat eine der in den Nummern 1 bis 7 genannten besonders schweren Straftaten ist,

n) Computerbetrug in den Fällen des § 263a Absatz 2 in Verbindung mit § 263 Absatz 5,

o) besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Absatz 1 unter den in § 335 Absatz 2 Nummer 1 bis 3 genannten Voraussetzungen,

2. aus dem Asylgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Absatz 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a Absatz 1,

3. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Absatz 2,

b) Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,

4. aus dem Außenwirtschaftsgesetz:

a) Straftaten nach § 17 Absatz 1, 2 und 3, jeweils auch in Verbindung mit Absatz 6 oder 7,

b) Straftaten nach § 18 Absatz 7 und 8, jeweils auch in Verbindung mit Absatz 10,

5. aus dem Betäubungsmittelgesetz:

a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,

b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,

5a. aus dem Konsumcannabisgesetz:

Straftaten nach § 34 Absatz 4 Nummer 1, 3 oder Nummer 4,

5b. aus dem Medizinal-Cannabisgesetz:

Straftaten nach § 25 Absatz 5 Nummer 1, 3 oder Nummer 4,

6. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,

b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,

7. aus dem Grundstoffüberwachungsgesetz:

Straftaten nach § 19 Absatz 3,

8. aus dem Neue-psychoaktive-Stoffe-Gesetz:

Straftaten nach § 4 Absatz 3 Nummer 1,

9. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

d) Verbrechen der Aggression nach § 13,

10. aus dem Waffengesetz:

a) besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,

b) besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5.

(3) Die Maßnahme darf sich nur gegen den Beschuldigten richten. Ein Eingriff in informationstechnische Systeme anderer Personen ist nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte informationstechnische Systeme der anderen Person benutzt, und

2. die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(4) § 100a Absatz 5 und 6 gilt mit Ausnahme von Absatz 5 Satz 1 Nummer 1 entsprechend.

Nichtamtliches Inhaltsverzeichnis

§ 100c Akustische Wohnraumüberwachung

(1) Auch ohne Wissen der Betroffenen darf das in einer Wohnung nichtöffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,

2. die Tat auch im Einzelfall besonders schwer wiegt,

3. auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind, und

4. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre.

(2) Die Maßnahme darf sich nur gegen den Beschuldigten richten und nur in Wohnungen des Beschuldigten durchgeführt werden. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte sich dort aufhält und

2. die Maßnahme in Wohnungen des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

§ 100d Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte

(1) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den §§ 100a bis 100c allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig.

(2) Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den §§ 100a bis 100c erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.

(3) Bei Maßnahmen nach § 100b ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach § 100b erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(4) Maßnahmen nach § 100c dürfen nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung

zuzurechnen sind, nicht erfasst werden. Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Ist eine Maßnahme unterbrochen worden, so darf sie unter den in Satz 1 genannten Voraussetzungen fortgeführt werden. Im Zweifel hat die Staatsanwaltschaft über die Unterbrechung oder Fortführung der Maßnahme unverzüglich eine Entscheidung des Gerichts herbeizuführen; § 100e Absatz 5 gilt entsprechend. Auch soweit für bereits erlangte Erkenntnisse ein Verwertungsverbot nach Absatz 2 in Betracht kommt, hat die Staatsanwaltschaft unverzüglich eine Entscheidung des Gerichts herbeizuführen. Absatz 3 Satz 3 gilt entsprechend.

(5) In den Fällen des § 53 sind Maßnahmen nach den §§ 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass ein Fall des § 53 vorliegt, gilt Absatz 2 entsprechend. In den Fällen der §§ 52 und 53a dürfen aus Maßnahmen nach den §§ 100b und 100c gewonnene Erkenntnisse nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes eines Beschuldigten steht. § 160a Absatz 4 gilt entsprechend.

§ 100e Verfahren bei Maßnahmen nach den §§ 100a bis 100c

(1) Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) Maßnahmen nach den §§ 100b und 100c dürfen nur auf Antrag der Staatsanwaltschaft durch die in § 74a Absatz 4 des Gerichtsverfassungsgesetzes genannte Kammer des Landgerichts angeordnet werden, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat. Bei Gefahr im Verzug kann diese Anordnung auch durch den Vorsitzenden getroffen werden. Dessen Anordnung tritt außer Kraft, wenn sie nicht binnen drei Werktagen von der Strafkammer bestätigt wird. Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Ist die Dauer der Anordnung auf insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen das Oberlandesgericht.

(3) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
2. der Tatvorwurf, auf Grund dessen die Maßnahme angeordnet wird,
3. Art, Umfang, Dauer und Endzeitpunkt der Maßnahme,
4. die Art der durch die Maßnahme zu erhebenden Informationen und ihre Bedeutung für das Verfahren,
5. bei Maßnahmen nach § 100a die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist; im Fall des § 100a Absatz 1 Satz 2 und 3 eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das eingegriffen werden soll,
6. bei Maßnahmen nach § 100b eine möglichst genaue Bezeichnung des informationstechnischen Systems, aus dem Daten erhoben werden sollen,
7. bei Maßnahmen nach § 100c die zu überwachende Wohnung oder die zu überwachenden Wohnräume.

(4) In der Begründung der Anordnung oder Verlängerung von Maßnahmen nach den §§ 100a bis 100c sind deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen anzugeben:

1. die bestimmten Tatsachen, die den Verdacht begründen,
2. die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme,

3. bei Maßnahmen nach § 100c die tatsächlichen Anhaltspunkte im Sinne des § 100d Absatz 4 Satz 1.

(5) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Das anordnende Gericht ist nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten. Bei Maßnahmen nach den §§ 100b und 100c ist das anordnende Gericht auch über den Verlauf zu unterrichten. Liegen die Voraussetzungen der Anordnung nicht mehr vor, so hat das Gericht den Abbruch der Maßnahme anzuordnen, sofern der Abbruch nicht bereits durch die Staatsanwaltschaft veranlasst wurde. Die Anordnung des Abbruchs einer Maßnahme nach den §§ 100b und 100c kann auch durch den Vorsitzenden erfolgen.

(6) Die durch Maßnahmen nach den §§ 100b und 100c erlangten und verwertbaren personenbezogenen Daten dürfen für andere Zwecke nach folgenden Maßgaben verwendet werden:

1. Die Daten dürfen in anderen Strafverfahren ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer Maßnahmen nach § 100b oder § 100c angeordnet werden könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.

2. Die Verwendung der Daten, auch solcher nach § 100d Absatz 5 Satz 1 zweiter Halbsatz, zu Zwecken der Gefahrenabwehr ist nur zur Abwehr einer im Einzelfall bestehenden Lebensgefahr oder einer dringenden Gefahr für Leib oder Freiheit einer Person, für die Sicherheit oder den Bestand des Staates oder für Gegenstände von bedeutendem Wert, die der Versorgung der Bevölkerung dienen, von kulturell herausragendem Wert oder in § 305 des Strafgesetzbuches genannt sind, zulässig. Die Daten dürfen auch zur Abwehr einer im Einzelfall bestehenden dringenden Gefahr für sonstige bedeutende Vermögenswerte verwendet werden. Sind die Daten zur Abwehr der Gefahr oder für eine vorgerichtliche oder gerichtliche Überprüfung der zur Gefahrenabwehr getroffenen Maßnahmen nicht mehr erforderlich, so sind Aufzeichnungen über diese Daten von der für die Gefahrenabwehr zuständigen Stelle unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige vorgerichtliche oder gerichtliche Überprüfung zurückgestellt ist, dürfen die Daten nur für diesen Zweck verwendet werden; für eine Verwendung zu anderen Zwecken sind sie zu sperren.

3. Sind verwertbare personenbezogene Daten durch eine entsprechende polizeirechtliche Maßnahme erlangt worden, dürfen sie in einem Strafverfahren ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer die Maßnahmen nach § 100b oder § 100c angeordnet werden könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.

§ 100f Akustische Überwachung außerhalb von Wohnraum

(1) Auch ohne Wissen der betroffenen Personen darf außerhalb von Wohnungen das nichtöffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100a Abs. 2 bezeichnete, auch im Einzelfall schwerwiegende Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat, und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(2) Die Maßnahme darf sich nur gegen einen Beschuldigten richten. Gegen andere Personen darf die Maßnahme nur angeordnet werden, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie mit einem Beschuldigten in Verbindung stehen oder eine solche Verbindung hergestellt wird, die Maßnahme zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten führen wird und dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(4) § 100d Absatz 1 und 2 sowie § 100e Absatz 1, 3, 5 Satz 1 gelten entsprechend.

§ 100g Erhebung von Verkehrsdaten

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

2. eine Straftat mittels Telekommunikation begangen hat,

so dürfen Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und § 2a Absatz 1 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Im Fall des Satzes 1 Nummer 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Die Erhebung gespeicherter (retrograder) Standortdaten ist nach diesem Absatz nur unter den Voraussetzungen des Absatzes 2 zulässig. Im Übrigen ist die Erhebung von Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nummer 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, und wiegt die Tat auch im Einzelfall besonders schwer, dürfen die nach § 176 des Telekommunikationsgesetzes gespeicherten Verkehrsdaten erhoben werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Besonders schwere Straftaten im Sinne des Satzes 1 sind:

1. aus dem Strafgesetzbuch:

a) Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 81, 82, 89a, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,

b) besonders schwerer Fall des Landfriedensbruchs nach § 125a sowie Betreiben krimineller Handelsplattformen im Internet in den Fällen des § 127 Absatz 3 und 4,

c) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 sowie Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,

d) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176, 176c, 176d und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

e) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Inhalte in den Fällen des § 184b Absatz 1 Satz 1, Absatz 2 und 3 sowie des § 184c Absatz 2,

f) Mord und Totschlag nach den §§ 211 und 212,

g) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, §§ 239a, 239b und Zwangsprostitution und Zwangsarbeit nach § 232a Absatz 3, 4 oder 5 zweiter Halbsatz, § 232b Absatz 3 oder 4 in Verbindung mit § 232a Absatz 4 oder 5 zweiter Halbsatz und Ausbeutung unter Ausnutzung einer Freiheitsberaubung nach § 233a Absatz 3 oder 4 zweiter Halbsatz,

h)

Einbruchdiebstahl in eine dauerhaft genutzte Privatwohnung nach § 244 Absatz 4, schwerer Bandendiebstahl nach § 244a Absatz 1, schwerer Raub nach § 250 Absatz 1 oder Absatz 2, Raub mit Todesfolge nach § 251, räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen, gewerbsmäßige Bandenhehlerei nach § 260a Absatz 1, besonders schwerer Fall der Geldwäsche nach § 261 unter den in § 261 Absatz 5 Satz 2 genannten Voraussetzungen, wenn die Vortat eine der in den Nummern 1 bis 8 genannten besonders schweren Straftaten ist,

i) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Absatz 1 bis 3, des § 308 Absatz 1 bis 3, des § 309 Absatz 1 bis 4, des § 310 Absatz 1, der §§ 313, 314, 315 Absatz 3, des § 315b Absatz 3 sowie der §§ 316a und 316c,

2. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Absatz 2,

b) Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,

3. aus dem Außenwirtschaftsgesetz:

Straftaten nach § 17 Absatz 1 bis 3 und § 18 Absatz 7 und 8,

4. aus dem Betäubungsmittelgesetz:

a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,

b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,

5. aus dem Grundstoffüberwachungsgesetz:

eine Straftat nach § 19 Absatz 1 unter den in § 19 Absatz 3 Satz 2 genannten Voraussetzungen,

6. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,

b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,

7. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

d) Verbrechen der Aggression nach § 13,

8. aus dem Waffengesetz:

a) besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,

b) besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5.

(3) Die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten (Funkzellenabfrage) ist nur zulässig,

1. wenn die Voraussetzungen des Absatzes 1 Satz 1 Nummer 1 erfüllt sind,

2. soweit die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht und

3. soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Auf nach § 176 des Telekommunikationsgesetzes gespeicherte Verkehrsdaten darf für eine Funkzellenabfrage nur unter den Voraussetzungen des Absatzes 2 zurückgegriffen werden.

(4) Die Erhebung von Verkehrsdaten nach Absatz 2, auch in Verbindung mit Absatz 3 Satz 2, die sich gegen eine der in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannten Personen richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, ist unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist aktenkundig zu machen. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine in § 53 Absatz 1 Satz 1

Nummer 1 bis 5 genannte Person richtet, von dieser Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. § 160a Absatz 3 und 4 gilt entsprechend.

(5) Erfolgt die Erhebung von Verkehrsdaten nicht beim Erbringer von Telekommunikationsdiensten, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

§ 100h Weitere Maßnahmen außerhalb von Wohnraum

(1) Auch ohne Wissen der betroffenen Personen dürfen außerhalb von Wohnungen

1. Bildaufnahmen hergestellt werden,
2. sonstige besondere für Observationszwecke bestimmte technische Mittel verwendet werden,

wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger erfolgversprechend oder erschwert wäre. Eine Maßnahme nach Satz 1 Nr. 2 ist nur zulässig, wenn Gegenstand der Untersuchung eine Straftat von erheblicher Bedeutung ist.

(2) Die Maßnahmen dürfen sich nur gegen einen Beschuldigten richten. Gegen andere Personen sind

1. Maßnahmen nach Absatz 1 Nr. 1 nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre,
2. Maßnahmen nach Absatz 1 Nr. 2 nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie mit einem Beschuldigten in Verbindung stehen oder eine solche Verbindung hergestellt wird, die Maßnahme zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten führen wird und dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar mitbetroffen werden.

(4) § 100d Absatz 1 und 2 gilt entsprechend.

§ 100i Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, so dürfen durch technische Mittel

1. die Gerätenummer eines Mobilfunkendgerätes und die Kartenummer der darin verwendeten Karte sowie
2. der Standort eines Mobilfunkendgerätes

ermittelt werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartenummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(3) § 100a Abs. 3 und § 100e Absatz 1 Satz 1 bis 3, Absatz 3 Satz 1 und Absatz 5 Satz 1 gelten entsprechend. Die Anordnung ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen fortbestehen.

§ 100j Bestandsdatenauskunft

(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf Auskunft verlangt werden

1. über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, und

2. über Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Telemedien-Datenschutz-Gesetzes (§ 22 Absatz 1 Satz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes) von demjenigen, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt.

Bezieht sich das Auskunftsverlangen nach Satz 1 Nummer 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 174 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. 3 Bezieht sich das Auskunftsverlangen nach Satz 1 Nummer 2 auf als Bestandsdaten erhobene Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 23 des Telekommunikation-Telemedien-Datenschutz-Gesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für ihre Nutzung zur Verfolgung einer besonders schweren Straftat nach § 100b Absatz 2 Nummer 1 Buchstabe a, c, e, f, g, h oder m, Nummer 3 Buchstabe b erste Alternative oder Nummer 5, 5a, 5b, 6, 9 oder 10 vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Absatz 1 Satz 3, § 177 Absatz 1 Nummer 3 des Telekommunikationsgesetzes und § 22 Absatz 1 Satz 3 und 4 des Telekommunikation-Telemedien-Datenschutz-Gesetzes). Das Vorliegen der Voraussetzungen für ein Auskunftsverlangen nach Satz 1 ist aktenkundig zu machen.

(3) Auskunftsverlangen nach Absatz 1 Satz 2 und 3 dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Im Fall von Auskunftsverlangen nach Absatz 1 Satz 2 kann die Anordnung bei Gefahr im Verzug auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Die Sätze 1 bis 3 finden bei Auskunftsverlangen nach Absatz 1 Satz 2 keine Anwendung, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.

(4) Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und 3 und des Absatzes 2 über die Beauskunftung zu benachrichtigen. Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(5) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. § 95 Absatz 2 gilt entsprechend.

§ 100k Erhebung von Nutzungsdaten bei Telemediendiensten

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, dürfen von demjenigen, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt, Nutzungsdaten (§ 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung gespeicherter (retrograder) Standortdaten ist nur unter den Voraussetzungen von § 100g Absatz 2 zulässig. Im Übrigen ist die Erhebung von Standortdaten nur für künftig anfallende Nutzungsdaten oder in Echtzeit zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Soweit die Straftat nicht von Absatz 1 erfasst wird, dürfen Nutzungsdaten auch dann erhoben werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer mittels Telemedien eine der folgenden Straftaten begangen hat und die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre:

1. aus dem Strafgesetzbuch

- a) Verwenden von Kennzeichen verfassungswidriger Organisationen nach § 86a,
- b) Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat nach § 91,
- c) Öffentliche Aufforderung zu Straftaten nach § 111,
- d) Straftaten gegen die öffentliche Ordnung nach den §§ 126, 131 und 140,
- e) Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen nach § 166,
- f) Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte nach § 184b,
- g) Beleidigung, üble Nachrede und Verleumdung nach den §§ 185 bis 187 und Verunglimpfung des Andenkens Verstorbener nach § 189,
- h) Verletzungen des persönlichen Lebens- und Geheimbereichs nach den §§ 201a, 202a und 202c,
- i) Nachstellung nach § 238,
- j) Bedrohung nach § 241,
- k) Vorbereitung eines Computerbetruges nach § 263a Absatz 3,
- l) Datenveränderung und Computersabotage nach den §§ 303a und 303b Absatz 1,

2. aus dem Gesetz über Urheberrecht und verwandte Schutzrechte Straftaten nach den §§ 106 bis 108b,

3. aus dem Bundesdatenschutzgesetz nach § 42.

Satz 1 gilt nicht für die Erhebung von Standortdaten.

(3) Abweichend von Absatz 1 und 2 darf die Staatsanwaltschaft ausschließlich zur Identifikation des Nutzers Auskunft über die nach § 2 Absatz 2 Nummer 3 Buchstabe a des Telekommunikation-Telemediendatenschutzgesetzes erhobenen Daten verlangen, wenn ihr der Inhalt der Nutzung des Telemediendienstes bereits bekannt ist.

(4) Die Erhebung von Nutzungsdaten nach Absatz 1 und 2 ist nur zulässig, wenn aufgrund von Tatsachen die Annahme gerechtfertigt ist, dass die betroffene Person den Telemediendienst nutzt, den derjenige, gegen den sich die Anordnung richtet, geschäftsmäßig zur Nutzung bereithält oder zu dem er den Zugang zur Nutzung vermittelt.

(5) Erfolgt die Erhebung von Nutzungsdaten oder Inhalten der Nutzung eines Telemediendienstes nicht bei einem Diensteanbieter, der geschäftsmäßig Telemedien zur Nutzung bereithält, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

Nichtamtliches Inhaltsverzeichnis

§ 101 Verfahrensregelungen bei verdeckten Maßnahmen

(1) Für Maßnahmen nach den §§ 98a, 99, 100a bis 100f, 100h, 100i, 110a, 163d bis 163g gelten, soweit nichts anderes bestimmt ist, die nachstehenden Regelungen.

(2) Entscheidungen und sonstige Unterlagen über Maßnahmen nach den §§ 100b, 100c, 100f, 100h Abs. 1 Nr. 2 und § 110a werden bei der Staatsanwaltschaft verwahrt. Zu den Akten sind sie erst zu nehmen, wenn die Voraussetzungen für eine Benachrichtigung nach Absatz 5 erfüllt sind.

(3) Personenbezogene Daten, die durch Maßnahmen nach Absatz 1 erhoben wurden, sind entsprechend zu kennzeichnen. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle

1. des § 98a die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden,
2. des § 99 der Absender und der Adressat der Postsendung,
3. des § 100a die Beteiligten der überwachten Telekommunikation,
4. des § 100b die Zielperson sowie die erheblich mitbetroffenen Personen,
5. des § 100c
 - a) der Beschuldigte, gegen den sich die Maßnahme richtete,
 - b) sonstige überwachte Personen,
 - c) Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,
6. des § 100f die Zielperson sowie die erheblich mitbetroffenen Personen,
7. des § 100h Abs. 1 die Zielperson sowie die erheblich mitbetroffenen Personen,
8. des § 100i die Zielperson,
9. des § 110a
 - a) die Zielperson,
 - b) die erheblich mitbetroffenen Personen,
 - c) die Personen, deren nicht allgemein zugängliche Wohnung der Verdeckte Ermittler betreten hat,
10. des § 163d die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden,
11. des § 163e die Zielperson und die Person, deren personenbezogene Daten gemeldet worden sind,
12. des § 163f die Zielperson sowie die erheblich mitbetroffenen Personen,
13. des § 163g die Zielperson

zu benachrichtigen. Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 7 und die dafür vorgesehene Frist hinzuweisen. Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nummer 2 und 3 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(5) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, im Fall des § 110a auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers möglich ist. Wird die Benachrichtigung nach Satz 1 zurückgestellt, sind die Gründe aktenkundig zu machen.

(6) Erfolgt die nach Absatz 5 zurückgestellte Benachrichtigung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedürfen weitere Zurückstellungen der gerichtlichen Zustimmung. Das Gericht bestimmt die Dauer weiterer Zurückstellungen. Es kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme. Bei Maßnahmen nach den §§ 100b und 100c beträgt die in Satz 1 genannte Frist sechs Monate.

(7) Gerichtliche Entscheidungen nach Absatz 6 trifft das für die Anordnung der Maßnahme zuständige Gericht, im Übrigen das Gericht am Sitz der zuständigen Staatsanwaltschaft. Die in Absatz 4 Satz 1 genannten Personen können bei dem nach Satz 1 zuständigen Gericht auch nach Beendigung der Maßnahme bis zu zwei Wochen nach ihrer Benachrichtigung die Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihres Vollzugs beantragen. Gegen die Entscheidung ist die sofortige Beschwerde statthaft. Ist die öffentliche Klage erhoben und der Angeklagte benachrichtigt worden, entscheidet über den Antrag das mit der Sache befasste Gericht in der das Verfahren abschließenden Entscheidung.

(8) Sind die durch die Maßnahme erlangten personenbezogenen Daten zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich, so sind sie unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige gerichtliche Überprüfung der Maßnahme zurückgestellt ist, dürfen die Daten ohne Einwilligung der betroffenen Personen nur zu diesem Zweck verwendet werden; ihre Verarbeitung ist entsprechend einzuschränken.

§ 101a Gerichtliche Entscheidung; Datenkennzeichnung und -auswertung; Benachrichtigungspflichten bei Verkehrs- und Nutzungsdaten

(1) Bei Erhebungen von Verkehrsdaten nach § 100g gelten § 100a Absatz 3 und 4 und § 100e entsprechend mit der Maßgabe, dass

1. in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 auch die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen, eindeutig anzugeben sind,
2. der nach § 100a Absatz 4 Satz 1 zur Auskunft Verpflichtete auch mitzuteilen hat, welche der von ihm übermittelten Daten nach § 176 des Telekommunikationsgesetzes gespeichert wurden.

In den Fällen des § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 3 Satz 2, findet abweichend von Satz 1 § 100e Absatz 1 Satz 2 keine Anwendung. Bei Funkzellenabfragen nach § 100g Absatz 3 genügt abweichend von § 100e Absatz 3 Satz 2 Nummer 5 eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation.

(1a) Bei der Erhebung und Beauskunftung von Nutzungsdaten eines Telemediendienstes nach § 100k gilt § 100a Absatz 3 und 4, bei der Erhebung von Nutzungsdaten nach § 100k Absatz 1 und 2 zudem § 100e Absatz 1 und 3 bis 5 entsprechend mit der Maßgabe, dass in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 an die Stelle der Rufnummer (§ 100e Absatz 3 Satz 2 Nummer 5), soweit möglich eine eindeutige Kennung des Nutzerkontos des Betroffenen, ansonsten eine möglichst genaue Bezeichnung des Telemediendienstes tritt, auf den sich das Auskunftsverlangen bezieht.

(2) Wird eine Maßnahme nach § 100g oder § 100k Absatz 1 oder Absatz 2 angeordnet oder verlängert, sind in der Begründung einzelfallbezogen insbesondere die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme, auch hinsichtlich des Umfangs der zu erhebenden Daten und des Zeitraums, für den sie erhoben werden sollen, darzulegen.

(3) Personenbezogene Daten, die durch Maßnahmen nach § 100g oder § 100k Absatz 1 oder Absatz 2 erhoben wurden, sind entsprechend zu kennzeichnen und unverzüglich auszuwerten. Bei der Kennzeichnung ist erkennbar zu machen, ob es sich um Daten handelt, die nach § 176 des Telekommunikationsgesetzes gespeichert waren. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten. Für die Löschung personenbezogener Daten gilt § 101 Absatz 8 entsprechend.

(4) Verwertbare personenbezogene Daten, die durch Maßnahmen nach § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 1 Satz 3 oder Absatz 3 Satz 2, erhoben wurden, dürfen ohne Einwilligung der Beteiligten der betroffenen Telekommunikation nur für folgende andere Zwecke und nur nach folgenden Maßgaben verwendet werden:

1. in anderen Strafverfahren zur Aufklärung einer Straftat, auf Grund derer eine Maßnahme nach § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 1 Satz 3 oder Absatz 3 Satz 2, angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person,

2. Übermittlung zu Zwecken der Abwehr von konkreten Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes (§ 177 Absatz 1 Nummer 2 des Telekommunikationsgesetzes).

Die Stelle, die die Daten weiterleitet, macht die Weiterleitung und deren Zweck aktenkundig. Sind die Daten nach Satz 1 Nummer 2 nicht mehr zur Abwehr der Gefahr oder nicht mehr für eine vorgerichtliche oder gerichtliche Überprüfung der zur Gefahrenabwehr getroffenen Maßnahmen erforderlich, so sind Aufzeichnungen über diese Daten von der für die Gefahrenabwehr zuständigen Stelle unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige vorgerichtliche oder gerichtliche Überprüfung zurückgestellt ist, dürfen die Daten nur für diesen Zweck verwendet werden; für eine Verwendung zu anderen Zwecken sind sie zu sperren.

(5) Sind verwertbare personenbezogene Daten, die nach § 176 des Telekommunikationsgesetzes gespeichert waren, durch eine entsprechende polizeirechtliche Maßnahme erlangt worden, dürfen sie in einem Strafverfahren ohne Einwilligung der Beteiligten der betroffenen Telekommunikation nur zur Aufklärung einer Straftat, auf Grund derer eine Maßnahme nach § 100g Absatz 2, auch in Verbindung mit Absatz 3 Satz 2, angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.

(6) Die Beteiligten der betroffenen Telekommunikation und die betroffenen Nutzer des Telemediendienstes sind von der Erhebung der Verkehrsdaten nach § 100g oder der Nutzungsdaten nach § 100k Absatz 1 und 2 zu benachrichtigen. § 101 Absatz 4 Satz 2 bis 5 und Absatz 5 bis 7 gilt entsprechend mit der Maßgabe, dass

1. das Unterbleiben der Benachrichtigung nach § 101 Absatz 4 Satz 3 der Anordnung des zuständigen Gerichts bedarf;

2. abweichend von § 101 Absatz 6 Satz 1 die Zurückstellung der Benachrichtigung nach § 101 Absatz 5 Satz 1 stets der Anordnung des zuständigen Gerichts bedarf und eine erstmalige Zurückstellung auf höchstens zwölf Monate zu befristen ist.

(7) Die betroffene Person ist in den Fällen des § 100k Absatz 3 über die Beauskunftung zu benachrichtigen. Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Beauskunftung nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

Gesetzessammlung – Teil II: Datenschutzrecht

DSGVO - VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION (...) in Erwägung nachstehender Gründe:

Erwägungsgrund (1)

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Erwägungsgrund (2)

Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts

gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

Erwägungsgrund (4)

Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen.

Erwägungsgrund (19)

Der 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie der freie Verkehr dieser Daten sind in einem eigenen Unionsrechtsakt geregelt. (...)

Erwägungsgrund (22)

Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union sollte gemäß dieser Verordnung erfolgen, gleich, ob die Verarbeitung in oder außerhalb der Union stattfindet. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei nicht ausschlaggebend.

Erwägungsgrund (26)

Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, 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. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

Erwägungsgrund (32)

Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten

Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.

Erwägungsgrund (39)

Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

Erwägungsgrund (47)

Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen. Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

Erwägungsgrund (50)

Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, sollte nur zulässig sein, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. (...)

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1 Gegenstand und Ziele

- (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- (3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Artikel 2 Sachlicher Anwendungsbereich

- (1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
- (2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt, b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen, c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten, d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.
- (3) Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 98 an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.
- (4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.

Artikel 3 Räumlicher Anwendungsbereich

- (1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.
- (2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist; b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Artikel 4 Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck: 1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die 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;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe 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;

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ 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;

6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9. „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. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10. „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 verarbeiten;

11. „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

12. „Verletzung des Schutzes personenbezogener Daten“ 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 übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

13. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

14. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

15. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

16. „Hauptniederlassung“

a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

17. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

18. „Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

19. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

20. „verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern;

21. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle;

22. „betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

- a) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,
- b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder
- c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

23. „grenzüberschreitende Verarbeitung“ entweder

- a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder
- b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

24. „maßgeblicher und begründeter Einspruch“ einen Einspruch gegen einen Beschlussentwurf im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder ob beabsichtigte Maßnahmen gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;

25. „Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates (1);

26. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

KAPITEL II Grundsätze

Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

- a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
- c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- e) 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; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende

Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) 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“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Artikel 6 Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht

oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem

- a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
- d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Artikel 7 Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig 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.

Artikel 8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

(1) Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

(2) Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

(3) Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h) die Verarbeitung ist 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 und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist 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 Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen

Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

KAPITEL III Rechte der betroffenen Person

Abschnitt 1 Transparenz und Modalitäten

Artikel 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

(2) Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(6) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

(7) Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.

Abschnitt 2 Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Artikel 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

- a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
- f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der

betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Artikel 15 Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

- a) die Verarbeitungszwecke;
- b) die Kategorien personenbezogener Daten, die verarbeitet werden;
- c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Abschnitt 3 Berichtigung und Löschung Artikel 16 Recht auf Berichtigung Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

Artikel 17 Recht auf Löschung („Recht auf Vergessenwerden“)

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

- b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
 - c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
 - d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
 - e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
 - f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.
- (2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.
- (3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist
- a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
 - b) 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;
 - c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
 - d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
 - e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

KAPITEL IV Verantwortlicher und Auftragsverarbeiter

Abschnitt 1 Allgemeine Pflichten

Artikel 24 Verantwortung des für die Verarbeitung Verantwortlichen

- (1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
- (2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.
- (3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Artikel 26 Gemeinsam für die Verarbeitung Verantwortliche

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Artikel 28 Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation —

verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen —, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Artikel 30 Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- b) die Zwecke der Verarbeitung;
- c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

- a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder 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.

Artikel 31 Zusammenarbeit mit der Aufsichtsbehörde

Der Verantwortliche und der Auftragsverarbeiter und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Abschnitt 2 Sicherheit personenbezogener Daten

Artikel 32 Sicherheit der Verarbeitung

(1) 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 Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
 - b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
 - c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
 - d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- (2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.
- (3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
- (4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Artikel 44 Allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Artikel 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:

- a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl

allgemeiner als auch sektoraler Art — auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten — sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und bei internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 des vorliegenden Artikels erlassenen Beschlüsse und der nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen beeinträchtigen könnten.

(5) Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen — insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung — dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen. In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 93 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

(6) Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat.

(7) Übermittlungen personenbezogener Daten an das betreffende Drittland, das Gebiet oder einen oder mehrere spezifische Sektoren in diesem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 46 bis 49 werden durch einen Beschluss nach Absatz 5 des vorliegenden Artikels nicht berührt.

(8) Die Kommission veröffentlicht im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, für die sie durch Beschluss festgestellt hat, dass sie ein angemessenes Schutzniveau gewährleisten bzw. nicht mehr gewährleisten. 4.5.2016 L 119/61 Amtsblatt der Europäischen Union DE

(9) Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie durch einen nach dem Prüfverfahren gemäß den Absätzen 3 oder 5 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 46 Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,

b) verbindlichen internen Datenschutzvorschriften gemäß Artikel 47,

c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,

d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 genehmigt wurden,

e) genehmigten Verhaltensregeln gemäß Artikel 40 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder

f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

(3) Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien gemäß Absatz 1 auch insbesondere bestehen in

a) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder

b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

(4) Die Aufsichtsbehörde wendet das Kohärenzverfahren nach Artikel 63 an, wenn ein Fall gemäß Absatz 3 des vorliegenden Artikels vorliegt.

(5) Von einem Mitgliedstaat oder einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilte Genehmigungen bleiben so lange gültig, bis sie erforderlichenfalls von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden. Von der Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie erforderlichenfalls mit einem nach Absatz 2 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 47 Verbindliche interne Datenschutzvorschriften

(1) Die zuständige Aufsichtsbehörde genehmigt gemäß dem Kohärenzverfahren nach Artikel 63 verbindliche interne Datenschutzvorschriften, sofern diese

a) rechtlich bindend sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern durchgesetzt werden, und dies auch für ihre Beschäftigten gilt,

b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen und c) die in Absatz 2 festgelegten Anforderungen erfüllen.

(2) Die verbindlichen internen Datenschutzvorschriften nach Absatz 1 enthalten mindestens folgende Angaben:

a) Struktur und Kontaktdaten der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und jedes ihrer Mitglieder;

b) die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;

c) interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften;

d) die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundene Stellen;

e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung nach Artikel 22 unterworfen zu werden sowie des in Artikel 79 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;

f) die von dem in einem Mitgliedstaat niedergelassenen Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen internen Datenschutzvorschriften; der Verantwortliche oder der Auftragsverarbeiter ist nur dann teilweise oder vollständig von dieser Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;

g) die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Artikel 13 und 14 hinaus über die verbindlichen internen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;

h) die Aufgaben jedes gemäß Artikel 37 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen internen Datenschutzvorschriften in der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;

i) die Beschwerdeverfahren;

j) die innerhalb der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens einer Unternehmensgruppe oder der Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden;

k) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;

l) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame

Wirtschaftstätigkeit ausüben, gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe j genannten Maßnahmen gegenüber der Aufsichtsbehörde;

m) die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen internen Datenschutzvorschriften bieten, und

n) geeignete Datenschutzbildungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.

(3) Die Kommission kann das Format und die Verfahren für den Informationsaustausch über verbindliche interne Datenschutzvorschriften im Sinne des vorliegenden Artikels zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen. Artikel 48 Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Artikel 49 Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,

b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,

c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,

d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,

e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,

f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,

g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 — einschließlich der verbindlichen internen Datenschutzvorschriften — gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten

vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.

(2) Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

(3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und sowie Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.

(5) Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.

(6) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 Unterabsatz 2 des vorliegenden Artikels in der Dokumentation gemäß Artikel 30.

Artikel 82 Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadenersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

Artikel 83 Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

- a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
- b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
- d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
- e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
- f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelpfen und seine möglichen nachteiligen Auswirkungen zu mindern;
- g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
- h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
- i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
- j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
- k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

- a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
- b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43; c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

- a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
- b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
- c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

Artikel 99 Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018. Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Bundesdatenschutzgesetz (BDSG)

§ 1 Anwendungsbereich des Gesetzes

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
 - a) Bundesrecht ausführen oder
 - b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

Für nichtöffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

(2) Andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(3) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) Dieses Gesetz findet Anwendung auf öffentliche Stellen. Auf nichtöffentliche Stellen findet es Anwendung, sofern

1. der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten im Inland verarbeitet,
2. die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer inländischen Niederlassung des Verantwortlichen oder Auftragsverarbeiters erfolgt oder
3. der Verantwortliche oder Auftragsverarbeiter zwar keine Niederlassung in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat, er aber in den Anwendungsbereich der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung fällt.

Sofern dieses Gesetz nicht gemäß Satz 2 Anwendung findet, gelten für den Verantwortlichen oder Auftragsverarbeiter nur die §§ 8 bis 21, 39 bis 44.

(5) Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 in der jeweils geltenden Fassung, unmittelbar gilt.

(6) Bei Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittstaaten.

(7) Bei Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der 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, S. 89) stehen die bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands assoziierten Staaten den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittstaaten.

(8) Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten finden die Verordnung (EU) 2016/679 und die Teile 1 und 2 dieses Gesetzes entsprechend Anwendung, soweit nicht in diesem Gesetz oder einem anderen Gesetz Abweichendes geregelt ist.

§ 2 Begriffsbestimmungen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nichtöffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nichtöffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(5) Öffentliche Stellen des Bundes gelten als nichtöffentliche Stellen im Sinne dieses Gesetzes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Als nichtöffentliche Stellen im Sinne dieses Gesetzes gelten auch öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 3 Verarbeitung personenbezogener Daten durch öffentliche Stellen

Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)

Teil 1 Allgemeine Bestimmungen

§ 1 Zweck

(1) Dieses Gesetz trifft die zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 11 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72) notwendigen ergänzenden Regelungen. Innerhalb der Grenzen der Verordnung (EU) 2016/679 werden spezifische Anforderungen an die Verarbeitung personenbezogener Daten geregelt.

(2) Dieses Gesetz dient ebenfalls der Umsetzung der 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 Zweck 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).

§ 2 Sicherstellung des Datenschutzes

Die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform haben jeweils für ihren Bereich die Ausführung der Verordnung (EU) 2016/679, dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

§ 3 Zulässigkeit der Verarbeitung personenbezogener Daten

(1) Soweit spezialgesetzliche Regelungen nicht vorgehen, ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe der verarbeitenden Stellen erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(2) Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Sind personenbezogene Daten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, sind auch die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgaben

erforderlich sind, zulässig, soweit nicht schutzwürdige Belange der betroffenen Person oder Dritter überwiegen. Die nicht erforderlichen Daten unterliegen insoweit einem Verwertungsverbot.

(3) Behördliche Unterlagen über die technischen und organisatorischen Maßnahmen gemäß Artikel 32 der Verordnung (EU) 2016/679 unterliegen nicht dem allgemeinen Informationszugang nach dem Informationsfreiheitsgesetz Nordrhein-Westfalen.

§ 4 Begriffsbestimmung

Ergänzend zu Artikel 4 der Verordnung (EU) 2016/679 bezeichnet der Ausdruck „Anonymisieren“ das Verändern personenbezogener Daten dergestalt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

§ 5 Anwendungsbereich

(1) Teil 2 dieses Gesetzes gilt für die Verarbeitung personenbezogener Daten durch die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie für die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform (öffentliche Stellen). Unbeschadet der Regelung des Satzes 1 gelten Schulen der Gemeinden und Gemeindeverbände, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, als öffentliche Stellen im Sinne dieses Gesetzes. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben einer öffentlichen Stelle des Landes wahr, gilt sie als öffentliche Stelle im Sinne des Gesetzes.

(2) Öffentliche Stellen im Sinne dieses Gesetzes sind auch natürliche und juristische Personen des privaten Rechts, soweit sie Befugnisse der Verwaltung übertragen bekommen haben und hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen.

(3) Für den Landtag gilt Teil 2 dieses Gesetzes, soweit er Verwaltungsaufgaben wahrnimmt.

(4) Für den Landesrechnungshof und die Staatlichen Rechnungsprüfungsämter, die Gerichte und die Behörden der Staatsanwaltschaft gilt Teil 2 dieses Gesetzes, soweit sie Verwaltungsaufgaben wahrnehmen.

(5) Teil 2 dieses Gesetzes findet mit Ausnahme des Kapitels 3 Abschnitt 1, des Kapitels 5 und des § 32 keine Anwendung, soweit

1. wirtschaftliche Unternehmen der Gemeinden oder Gemeindeverbände ohne eigene Rechtspersönlichkeit (Eigenbetriebe),
2. öffentliche Einrichtungen, die entsprechend den Vorschriften über Eigenbetriebe geführt werden,
3. Landesbetriebe oder
4. der Aufsicht des Landes oder der Gemeinden oder Gemeindeverbänden unterstehende juristische Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen, und die NRW.BANK, personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Soweit Hochschulen im Sinne des § 1 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG) Aufgaben nach § 3 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG) wahrnehmen findet Satz 1 keine Anwendung.

Soweit dieses Gesetz nach Maßgabe von Satz 1 keine Anwendung findet, gelten die Vorschriften für nicht-öffentliche Stellen mit Ausnahme der §§ 4, 22, 26 bis 28 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung entsprechend.

(6) Soweit besondere Rechtsvorschriften auf die Verarbeitung personenbezogener Daten anzuwenden sind, gehen sie den Vorschriften des Teils 2 dieses Gesetzes vor. Regeln Rechtsvorschriften einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes insoweit Anwendung.

(7) Die Vorschriften der §§ 22-24 und 33 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Fotografie (KunstUrhG) vom 9.1.1907, zuletzt geändert durch Artikel 3 § 31 des Gesetzes vom 16.2.2001 in seiner jeweils geltenden Fassung, bleiben für die nach § 5 unter dieses Gesetz fallenden Stellen unberührt.

(8) Auf Verarbeitungen, die nicht in den Anwendungsbereich des Unionsrechts fallen, sind die Vorschriften der Verordnung (EU) 2016/679 und die Vorschriften des Teils 2 dieses Gesetzes entsprechend anzuwenden, soweit nicht dieser Teil oder andere spezielle Rechtsvorschriften abweichende Regelungen enthalten. Dies gilt nicht für die in den Absätzen 3 und 4 genannten Stellen. Im Fall der entsprechenden Anwendung sind die Vorschriften über den gerichtlichen Rechtsschutz nach § 20 des Bundesdatenschutzgesetzes anzuwenden.

(9) Für Verarbeitungen, die nicht dem Anwendungsbereich von Artikel 2 Absatz 1 der Verordnung (EU) 2016/679 unterfallen, gelten die Artikel 13 und 14 der Verordnung (EU) 2016/679 nicht.