

Jandt | Steidle [Hrsg.]

Datenschutz und Internet

DS-GVO | BDSG | TDDDG
KI-VO | DMA | DSA

2. Auflage



Nomos

NOMOSPRAXIS

Silke Jandt | Roland Steidle [Hrsg.]

Datenschutz und Internet

DS-GVO | BDSG | TDDDG
KI-VO | DMA | DSA

2. Auflage

Dr. Jens Ambrock, Referatsleiter beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit | **Dr. Ubbo Aßmus**, Rechtsanwalt und Fachanwalt für Informationstechnologierecht; Geschäftsführer der lawcode GmbH, Lehrbeauftragter an der Hochschule RheinMain | **Dr. Tim Bagger von Grafenstein**, Rechtsanwalt und Fachanwalt für Sportrecht, Partner, München | **Dr. Henning Dehnert**, Referent beim Landesbeauftragten für den Datenschutz Niedersachsen | **Louisa Endrös**, Rechtsanwältin und Fachanwältin für Sport- und Datenschutzrecht, München | **Dr. habil. Christian L. Geminn**, Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und Privatdozent, Universität Kassel | **Dr. Volker Hammer**, Editor der DIN 66398 „Leitlinie Löschkonzept“ und Co-Editor der ISO/IEC 27555, freiberuflicher Berater für Löschprojekte (loeschprojekte.de), Bensheim | **Prof. Dr. Felix Hermonies**, Mag. rer. publ. LL.M., Professor für Datenschutz- und Medienrecht, Hochschule Darmstadt | **Dr. habil. Silke Jandt**, Stellvertretende Referatsleiterin beim Landesbeauftragten für den Datenschutz Niedersachsen | **Dr. Moritz Karg**, Referatsleiter Grundsatzangelegenheiten der Digitalisierung und des EGovernments, Staatskanzlei Schleswig-Holstein | **Dr. Sophie Victoria Knebel**, Fachanwältin für Informationstechnologierecht sowie Senior Legal Counsel bei der Parshipmeet Group | **Henry Krasemann**, Referatsleiter Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Dozent, Jurafunk, Kiel | **Anna Pokutnev**, Referentin bei dem Landesbeauftragten für Datenschutz Niedersachsen | **Dr. Philipp Richter**, Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz | **Dr. Annika Selzer**, Abteilungsleiterin für IT-Recht am Fraunhofer SIT und Co-Forschungsbereichs Koordinatorin für IT-Recht in ATHENE | **Dr. Hendrik Skistims**, Rechtsanwalt und Syndikusanwalt bei Union Investment, Frankfurt a.M. | **Dr. Tobias Stadler**, Referatsleiter bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) | **Dr. Roland Steidle**, LL.M. Rechtsanwalt und Fachanwalt für Informationstechnologierecht, Partner, Lehrbeauftragter an der Hochschule Darmstadt, Frankfurt a.M. | **Dr. Stefanie Wegener**, Rechtsanwältin und Fachanwältin für Arbeits- und Informationstechnologierecht, Hamburg | **Prof. Dr. Thomas Wilmer**, Professor für Informationsrecht, Hochschule Darmstadt



Nomos

Zitiervorschlag: Jandt/Steidle Datenschutz-HdB

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7560-1302-9 (Print)

ISBN 978-3-7489-1810-3 (ePDF)

2. Auflage 2025

© Nomos Verlagsgesellschaft, Baden-Baden 2025. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten.

Vorwort der Herausgeber

Die erste Ausgabe des Handbuchs „Datenschutz im Internet“ war vor allem durch das Inkrafttreten der europäischen Datenschutz-Grundverordnung am 24. Mai 2016 und deren vorrangiger Geltung vor den nationalen Datenschutzgesetzen in der Union ab dem 25. Mai 2018 motiviert. Die in allen Mitgliedstaaten unmittelbar und einheitlich geltende Verordnung ist nach wie vor ein Meilenstein in der Harmonisierung des europäischen Datenschutzrechts, das bis dahin auf der europäischen Datenschutz-Richtlinie aus dem Jahr 1995 und den jeweils national umgesetzten Datenschutzgesetzen basierte.

In den Jahren nach dem Erscheinen der Erstausgabe des Handbuchs gab es so viele rechtliche Weiterentwicklungen in Bezug auf das Internet, dass eine Neuauflage unvermeidlich war. Selbst beim Schreiben der Zweitaufgabe wurden die Autorinnen und Autoren immer wieder durch Gesetzesnovellierungen überholt. Nachdem die Datenschutz-Grundverordnung nunmehr seit über sechs Jahren gilt, sind Gerichtsurteile zu einzelnen Vorschriften und zu Auslegungsfragen ergangen und es hat sich gezeigt, wie die europäischen und deutschen Aufsichtsbehörden die Datenschutz-Grundverordnung um- und durchsetzen. Die neuere Rechtsentwicklung ist vor allem durch die Digitalstrategie der Europäischen Kommission mit mehreren Verordnungen sowie den ergänzenden nationalen Vorschriften geprägt, die auch den Datenschutz im Internet tangieren. Hervorzuheben sind hier der Digital Services Act, der Digital Markets Act und das Digitale Dienste Gesetz. Da Techniken der Künstlichen Intelligenz in immer mehr Diensten des Internets und in Apps integriert sind, beeinflusst auch die europäische KI-Verordnung als erstes Gesetz zur Regulierung von Künstlicher Intelligenz den Datenschutz im Internet maßgeblich.

Obschon im Vorwort der Erstauflage festgestellt wurde, dass die heutige Realität der Informationstechnologie und Datenverarbeitung im Internet nur noch wenig mit derjenigen aus dem Jahr 1995 gemein hatte, so hat sich das Rad seit 2018 noch einmal erheblich weiter gedreht. Die bereits 2018 erörterte „Vercloudung“ von Internet-Diensten hat sich fortgesetzt. Im Bereich Social Media haben sich neue Angebote wie zum Beispiel Snapchat und TikTok mit sehr großen Nutzerzahlen auf dem Markt etabliert und auf Large Language Modellen basierende KI-Chatbots gehören zum Alltag. Weiterhin hat die Miniaturisierung von Prozessoren und Netzwerkkomponenten dazu geführt, dass auch kleinste Alltagsgegenstände im „Internet der Dinge“ netzwerkfähig werden und über das Internet miteinander kommunizieren. Sensoren werden zur Ermöglichung autonomen Fahrens in Kraftfahrzeugen verbaut und erheben auch umfangreich personenbezogene Daten von Fahrern, Insassen und Verkehrsteilnehmern. Im sogenannten Metaverse erfolgt eine weitgehende Umgebungserfassung mit dem Ziel, die physisch reale Umgebung mit digitalen Räumen zu verschmelzen. All diese Entwicklungen stellen weitere Meilensteine der Digitalisierung des Alltags dar und erweitern die Anwendung der Datenschutz-Grundverordnung erheblich.

Mit der technischen Weiterentwicklung gehen neue Geschäftsmodelle und Marketingstrategien einher, die noch mehr als bisher auf der Nutzung und Monetarisierung personenbezogener Nutzerdaten basieren. Die Komplexität der Datenverarbeitungspro-

zesse und der eingebundenen Dienstleister hat sich fortwährend erhöht, so dass die Verarbeitungsvorgänge teils kaum noch nachvollziehbar, geschweige denn effektiv kontrollierbar sind. Die nochmals erheblich gestiegenen Datenmengen haben neue Branchen und Anbieter entstehen lassen, unter anderem im Bereich von Big Data und den damit einhergehenden Datenanalysen.

Die aus den neuen Analysemöglichkeiten folgenden Risiken einer ungerechtfertigten Diskriminierung einzelner Personen über Algorithmen, automatisierte Entscheidungen, Prognosen und statistische Ergebnisse, die – zumindest teilweise – ohne eine Verarbeitung personenbezogener Daten herbeigeführt werden, zeigen die Schwächen des Konzepts des Personenbezugs auf. Der Personenbezug bleibt nach der Datenschutz-Grundverordnung weiterhin alleiniger Anknüpfungspunkt für die Geltung datenschutzrechtlicher Bestimmungen. Die Ergänzungen durch den nicht an den Personenbezug anknüpfenden Art. 5 Abs. 3 E-Privacy-Richtlinie sowie § 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz zum Schutz von Endgeräten sind zwar ein Schritt in die richtige Richtung. Allerdings stammt die europäische Vorgabe, nach der anbieterseitig Daten auf Endgeräten gespeichert oder ausgelesen werden können, im Kern aus 2002 und ist daher mit Blick auf heutige Trackingtechnologien völlig veraltet.

Bedauerlicherweise hat die Datenschutz-Grundverordnung auch im Übrigen nicht zu einer inhaltlichen Modernisierung mit Blick auf die zunehmende Digitalisierung geführt. Soll das Datenschutzrecht auch all die in einer digitalen Welte anfallenden flüchtigen und meist nicht längerfristig gespeicherten Kommunikationsdaten erfassen? Der Alltag würde dann nicht nur durch Datenverarbeitungen durchdrungen, sondern noch mehr durch Datenschutzregelungen, deren Ursprung aus der Zeit der Großrechner und zentralen Datenverarbeitungen mit klar identifizierbaren Verantwortlichen stammt. Ob diese Datenschutzregelungen in dem beschriebenen künftigen Umfeld praktisch überhaupt noch anwendbar oder gar kontraproduktiv sind, ist diskussionswürdig. Dies betrifft Fragen der Verortung datenschutzrechtlicher Verantwortung in komplexen Geschäftsmodellen mit mehreren Beteiligten oder die Forderung nach umfangreichen Informationspflichten und Dokumentationen mit den damit einhergehenden zusätzlichen Datenspeicherungen. Fragen der Verwendung sensibler Daten, wie der von Biometriedaten zur Authentifizierung an Endgeräten oder bei Webdiensten, fordern ebenfalls Antworten. Ebenso ist das Verhältnis des Datenschutzrechts zur Meinungsfreiheit – nicht zuletzt wegen des Einflusses von Meinungen, Fakten oder „Fake News“ auf gesellschaftliche Entwicklungen und Wahlen – in den letzten Jahren zunehmend diskutiert worden. Die massiven Herausforderungen des Datenschutzrechts in einer digitalen Gesellschaft zeigen sich anhand vergangener und aktueller Datenschutzpannen und -skandale. Schließlich haben die Entwicklung und das Training von Large Language Modellen der Künstlichen Intelligenz einen noch größeren „Datenhunger“ ausgelöst, der kaum noch zu befriedigen ist. Die dazu technisch notwendigen Datenverarbeitungen laufen nahezu allen Grundsätzen des Datenschutzrechts zuwider – insbesondere der Datenminimierung, der Transparenz und der Zweckbindung. Die KI-Verordnung ist zwar ein Regulativ, enthält aber sehr wenige Datenschutzvorschriften. Die Datenschutz-Grundverordnung bleibt vollumfänglich anwendbar, so dass die aufgeworfenen Fragen anhand der allgemeinen Vorgaben der Datenschutz-Grundverordnung zu beantworten sind.

Obgleich die Europäische Kommission in zwei Evaluierungsberichten die europäische Datenschutz-Grundverordnung mit gut bewertet hat, zeigt ihre mehrjährige Anwendung in der Praxis, dass drängende Fragen des Datenschutzrechts unbeantwortet geblieben sind. Der fehlende Modernisierungsmut des europäischen Gesetzgebers zeigt sich nicht erst bei den ungelösten Problemen der Künstlichen Intelligenz. Eine moderne, die Nutzer schützende und zugleich innovationsfreundliche Regulierung, die die Interessen von Nutzern und Anbietern berücksichtigt und in Einklang bringt, enthält die Verordnung bedauerlicherweise nicht. Einige wenige bereichsspezifische Datenschutzdefizite versucht der europäische Gesetzgeber durch punktuelle Sonderregelungen zum Beispiel im Digital Markets Act und im Digital Services Act zu beheben. Dieser Ansatz ist erstens mit dem Nachteil verbunden, dass das europäische Datenschutzrecht erneut droht, in verschiedenen Gesetzen aufgesplittet zu werden. Darüber hinaus entstehen im föderalen deutschen System durch europäische Verordnungen, die unterschiedliche Regulierungsansätze von Marktregulierung, Verbraucher- und Datenschutz in einem Gesetz verfolgen, behördliche Zuständigkeitsprobleme für die Umsetzung und Kontrolle der Verordnungen.

Während des Gesetzgebungsverfahrens zur Datenschutz-Grundverordnung wurden vor allem die zahlreichen Öffnungsklauseln für nationale Sonderregelungen als erhebliches Risiko für die europaweiten Harmonisierungsbestrebungen eingestuft. Mittlerweile hat sich gezeigt, dass insbesondere drei andere Probleme die Harmonisierung behindern. Erstens zeigen die vom Europäischen Datenschutzausschuss zu verschiedenen Themen erarbeiteten Guidelines, dass es bei der Auslegung und Anwendung der Datenschutz-Grundverordnung sehr große Differenzen der europäischen Aufsichtsbehörden gibt, die letztlich nur in Kompromissen „auf dem kleinsten gemeinsamen Nenner“ eingefangen werden. Ungeachtet dessen behalten nationale Aufsichtsbehörden zum Teil ihre frühere, gegebenenfalls strengere Aufsichtspraxis bei, so dass bei der Rechtsdurchsetzung trotz der angestrebten Harmonisierung ein unterschiedliches Niveau bestehen bleibt. Zweitens, und dies wiegt wohl deutlich schwerer, ist die Rechtsdurchsetzung aufgrund der unterschiedlichen Ausstattung und Auslastung der nationalen Aufsichtsbehörden sehr uneinheitlich und langwierig. Die Konzentration der Zuständigkeit für die großen Internetplayer bei der irischen Aufsichtsbehörde mag hier mit hineinspielen, ist aber keinesfalls die Hauptursache. Drittens ergaben sich Schwierigkeiten bei der Rechtsdurchsetzung auch deshalb, da der Europäische Datenschutzausschuss die formalen Hürden in Streitbeilegungsverfahren der nationalen Aufsichtsbehörden sehr hoch gesetzt hat. Daher ist insbesondere das erste große Streitbeilegungsverfahren (Twitter EDPB Binding Decision 01/2020) an Formalien gescheitert. Wesentliche materiell-rechtliche Fragen sind folglich nicht durch den Ausschuss entschieden worden. In weiteren Verfahren ist der Europäische Datenschutzausschuss aber deutlich entschiedener aufgetreten. Er hat sowohl materiell-rechtliche Festlegungen getroffen als auch wesentlichen Einfluss auf die Bußgeldhöhen genommen.

Aus Sicht der datenverarbeitenden Unternehmen ist es in vielen Bereichen der Informationstechnologie und der Internetnutzung nach wie vor sehr schwierig, sich gerichtsfest rechtskonform zu verhalten. Dies gilt insbesondere in innovativen Projekten aber auch bei seit langem bekannten Verarbeitungsvorgängen wie beispielsweise dem Testen

Vorwort der Herausgeber

mit Echtdaten in komplexeren IT-Systemen. Angesichts des erheblich erweiterten Bußgeldrahmens zur Sanktionierung von – gegebenenfalls nicht eindeutig erkennbaren – Verstößen ist dies wirtschaftlich riskant. Allerdings zeigt die Bußgeldpraxis der letzten Jahre, dass die Aufsichtsbehörden den Handlungsspielraum der Datenschutz-Grundverordnung jedenfalls im mittelständischen Umfeld eher zurückhaltend nutzen. Bei der aktuellen KI-Forschung und -Entwicklung werden dennoch erneut Stimmen laut, die den Datenschutz und ergänzend die KI-Verordnung als Hemmnis für Innovationen in Europa bewerten. Denn erfolgreiche Entwicklungen und Webangebote stammen meist aus Drittländern, insbesondere aus den USA und China, und führen dann zu faktischen Auswirkungen auch in der Europäischen Union, allein aufgrund der großen Anzahl betroffener Nutzer.

Aufgrund der vorab beschriebenen Herausforderungen sind Auslegungs- und Argumentationshilfen wichtig für die Rechtsanwendung. Das Handbuch soll dieses Bedürfnis befriedigen und Rechtsanwendern aus Wissenschaft, Behörden, Unternehmen sowie Nutzern von Internet- und Webangeboten eine praktische Hilfestellung im Alltag geben. Dazu enthält es fundierte und wissenschaftlich untermauerte Beiträge mit Quellenangaben zu fast allen relevanten Bereichen des Datenschutzrechts im Internet. Eine besondere Berücksichtigung finden die zahlreichen Leitlinien und Stellungnahmen des Europäischen Datenschutzausschusses, in denen internetspezifische Datenschutzthemen konkretisiert werden. Die Autorinnen und Autoren haben verschiedene berufliche Hintergründe, alle lange Jahre Erfahrung im Datenschutzrecht und prägen die Materie in ihren Bereichen mit. Es sind Erfahrungen aus Wissenschaft, Aufsichtswesen und Unternehmen in das Handbuch eingeflossen. Der daraus folgende Mehrwert prägt dieses Handbuch und macht seinen Reiz aus.

Die Herausgeber und Autoren bedanken sich bei den Lesern für kritische Anmerkungen und wünschen Ihnen viel Freude beim Lesen.

Göttingen, Frankfurt, September 2024

Silke Jandt und Roland Steidle

Inhaltsübersicht

Vorwort der Herausgeber	5
Inhaltsverzeichnis	11
Abkürzungsverzeichnis	31
I. Grundlagen des Internets	43
II. Verfassungs- und europarechtliche Grundlagen	68
III. Verarbeitung personenbezogener Daten nach der Datenschutz- Grundverordnung	103
IV. Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz	192
V. Internetspezifische Datenverarbeitungen	237
VI. Technischer und organisatorischer Datenschutz	502
VII. Rechte der Betroffenen	584
VIII. Rechtsschutz für Betroffene	617
IX. Zusammenarbeit der europäischen Aufsichtsbehörden bei grenzüberschreitenden Verarbeitungen	656
X. Sanktionen	675
Literaturverzeichnis	697
Stichwortverzeichnis	743

Inhaltsverzeichnis

Inhaltsübersicht	9
Vorwort der Herausgeber	5
Verzeichnis der Autoren	29
Abkürzungsverzeichnis	31
I. Grundlagen des Internets (<i>Silke Jandt</i>)	43
1. Internet als technische Netzinfrastruktur	44
2. Internetdienste	49
3. Webdienste	52
4. Webtracking	57
5. Akteure des Internet	60
6. Geschäftsmodelle im Web	62
7. Zukunftsperspektiven	65
II. Verfassungs- und europarechtliche Grundlagen	68
1. Europäische und nationale Grundrechte (<i>Jens Ambrock</i>)	68
a) Datenschutz	69
aa) Schutz personenbezogener Daten gemäß Art. 8 Abs. 1 GRCh ...	70
bb) Recht auf informationelle Selbstbestimmung	75
b) Vertraulichkeit der Kommunikation	78
aa) Recht auf Achtung der Kommunikation gemäß Art. 7	
Var. 4 GRCh	78
bb) Fernmeldegeheimnis gemäß Art. 10 Abs. 1 Var. 3 GG	79
c) Recht am eigenen Bild und gesprochenen Wort	82
d) Vertraulichkeit und Integrität informationstechnischer Systeme	83
aa) Herleitung	83
bb) Schutzbereich	84
cc) Schranken	85
2. Anwendungsvorrang der europäischen Verordnungen (<i>Jens Ambrock</i>) ...	86
a) Harmonisierung des europäischen Datenschutzrechts	86
b) Anwendungsvorrang	88
c) Öffnungsklauseln	90
d) Beispiele für Öffnungsklauseln und mitgliedstaatliche	
Umsetzung	91
aa) Meinungsfreiheit und Presse	91
bb) Beschäftigtendatenschutz	92
cc) Scoring	94
dd) Einwilligung zu Diensten der Informationsgesellschaft	94

Inhaltsverzeichnis

e) Zusammenspiel von Datenschutz-Grundverordnung und Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz	95
3. Datenschutz-Grundverordnung und E-Privacy-Regulierung (<i>Silke Jandt</i>)	95
a) Stand der E-Privacy-Verordnung	96
b) Abgrenzung Datenschutz-Grundverordnung und E-Privacy-Richtlinie	97
c) Abgrenzung über den sachlichen Anwendungsbereich	98
aa) Öffentliche Kommunikationsnetze	98
bb) Kommunikationsdienste	99
cc) Merkmal der Zugänglichkeit des Dienstes	101
d) Schlussfolgerung für das Telekommunikation-Digitale-Dienste- Datenschutz-Gesetz	102
III. Verarbeitung personenbezogener Daten nach der Datenschutz- Grundverordnung	103
1. Personenbezug und Datenverarbeitungen im Internet, Pseudonymisierung und Anonymisierung (<i>Roland Steidle</i>)	103
a) Personenbezogene Daten	103
b) Kritik am Personenbezug als Anknüpfungspunkt	107
aa) Wandel der Bezugspunkte des Datenschutzrechts	107
bb) „Alles wird personenbezogen“	108
cc) Anonyme Datensammlungen und KI	110
dd) Lösungsansätze	110
c) Verarbeitung – „alles ist eine Verarbeitung“	110
d) Pseudonymisierung und Anonymisierung	111
e) Entfernen des Personenbezugs durch Verschlüsselung?	112
2. Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO (<i>Thomas Wilmer</i>)	114
a) Verhältnis zu anderen Normen	114
b) Geltungsbereich	115
c) Einzelne Vorgaben	115
aa) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	115
bb) Zweckbindung	116
cc) Datenminimierung	116
dd) Richtigkeit	117
ee) Speicherbegrenzung	117
ff) Integrität und Vertraulichkeit	117
gg) Rechenschaftspflicht	118

3. Rechtsgrundlagen der Verarbeitung in der Datenschutz-	
Grundverordnung	118
a) Rechtmäßige Verarbeitung gemäß Art. 6 DS-GVO	
<i>(Thomas Wilmer)</i>	118
aa) Geltungsbereich und Zweck	118
bb) Ausnahmen	119
cc) Einzelne Rechtsgrundlagen	119
dd) Öffnungsklausel nach Art. 6 Abs. 2 DS-GVO	123
ee) Rechtsgrundlagen für den öffentlichen Bereich gemäß Art. 6	
Abs. 3 DS-GVO	123
ff) Verarbeitung zu anderen Zwecken nach Art. 6 Abs. 4	
DS-GVO	124
b) Datenverarbeitung aufgrund berechtigter Interessen gemäß	
Art. 6 Abs. 1 S. 1 lit. f DS-GVO <i>(Philipp Richter)</i>	126
aa) Normgenese, Systematik und Funktion von	
Art. 6 Abs. 1 S. 1 lit. f DS-GVO	127
bb) Berechtigte Interessen	128
cc) Datenminimierung	129
dd) Interessen der betroffenen Personen	129
ee) Interessenabwägung	130
ff) Betroffenenrechte bei einer Verarbeitung nach	
Art. 6 Abs. 1 S. 1 lit. f DS-GVO	132
gg) Verhältnis von Art. 6 Abs. 1 S. 1 lit. f DS-GVO zu anderen	
Normen	132
c) Anforderungen an die datenschutzrechtliche Einwilligung	
<i>(Thomas Wilmer)</i>	132
aa) Allgemeine Voraussetzungen der Einwilligung	134
bb) Fortgeltung früherer Einwilligungen	142
cc) Technischer Einwilligungsprozess	142
d) Datenverarbeitung besonderer Kategorien personenbezogener	
Daten <i>(Silke Jandt)</i>	147
aa) Besondere Kategorien personenbezogener Daten im	
„Internet“	148
bb) Zulässigkeit der Verarbeitung besonderer Kategorien	
personenbezogener Daten	153
cc) Weitere datenschutzrechtliche Anforderungen	159
dd) Regelungen im Bundesdatenschutzgesetz	159
4. Datenverarbeitung im Auftrag und gemeinsam Verantwortliche	
<i>(Henry Krasemann)</i>	163
a) Voraussetzungen der Auftragsverarbeitung	165
aa) Vertrag oder anderes Rechtsinstrument	166

Inhaltsverzeichnis

bb) Konkrete Beschreibung der Verarbeitung	167
b) Typische Fälle von Auftragsverarbeitung	173
aa) Hosting	173
bb) Cloud Computing	174
cc) Tracking- und Analyse-Dienste	174
dd) Firewall	174
ee) Datenträgervernichtung	175
c) Streitfälle	175
d) Änderungsbedarf für Alt-Verträge nach der Datenschutz- Grundverordnung	177
e) Garantie durch genehmigte Verhaltensregeln oder Zertifizierung ...	178
f) Auftragnehmer im Ausland	178
g) Folgen bei Verstößen	179
h) Gemeinsam Verantwortliche	179
5. Internationale Datenverarbeitung (<i>Ubbo Aßmus/Roland Steidle</i>)	181
a) Datenverarbeitung in der Europäischen Union	181
b) EU-Verordnungen mit Datenschutzbezug	181
c) Übermittlung personenbezogener Daten in Drittländer	182
d) Anwendungsbereich der Datenschutz-Grundverordnung	184
e) Zweistufige Zulässigkeitsprüfung	184
f) Besondere Anforderungen an den Drittstaatentransfer	185
aa) Angemessenheitsbeschlüsse der Kommission	185
bb) EU-US Data Privacy Framework (DPF)	186
cc) Geeignete Garantien und wirksamer Rechtsschutz	187
dd) Nach Unionsrecht nicht zulässige Übermittlung oder Offenlegung	189
ee) Ausnahmen für bestimmte Fälle inklusive Einwilligung der betroffenen Person	190
IV. Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz	192
1. Verarbeitung von Verkehrs- und Standortdaten (<i>Tobias Stadler</i>)	192
a) Begriffsdefinitionen	192
aa) Funktionales Verständnis des „Telekommunikationsdienstes“ ...	193
bb) Begriffsverständnis Verkehrsdaten, Nutzungsdaten und Standortdaten	193
b) Schutz des Fernmeldegeheimnisses	194
c) Verarbeitungsbedingungen von Verkehrs- und Standortdaten	195
aa) Datengetriebene Dienste auf Basis von Verkehrsdaten	196
bb) Löschen von Verkehrsdaten	197
cc) Löschen durch Anonymisierung	197

dd) Verarbeitung zur Entgeltermittlung und Entgeltabrechnung	198
ee) Einzelverbindungsnachweis	198
(ff) Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten	200
gg) Verarbeitung von Standortdaten gemäß § 13 TDDDG	201
2. Cookies und Konsorten gemäß § 25 TDDDG (<i>Hendrik Skistims</i>)	203
a) Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz	204
b) Abgrenzung zur Datenschutz-Grundverordnung	205
aa) Konkurrenzverhältnis zwischen Telekommunikation-Digitale- Dienste-Datenschutz-Gesetz und Datenschutz- Grundverordnung	205
bb) Verdrängung der Datenschutz-Grundverordnung durch § 25 TDDDG	207
c) Schutz des Privatsphäre durch § 25 TDDDG	209
aa) Adressaten	209
bb) Endeinrichtungen	209
cc) Speicherung und Zugriff auf Informationen	210
dd) Einwilligung durch Endnutzer	212
d) Anforderungen an die Einwilligung	214
aa) Zeitpunkt	215
bb) Unmissverständliche und eindeutig bestätigende Handlung	215
cc) Bestimmtheitserfordernis und Bündelungsmöglichkeiten	218
dd) Freiwilligkeit	220
ee) Informiertheit	223
ff) Widerruf	224
e) Technische Gestaltungshinweise für Consent-Banner	224
f) Ausnahmen der Einwilligungsbedürftigkeit nach § 25 Abs. 2 TDDDG	225
aa) Durchführung der Übertragung einer Nachricht	226
bb) Unbedingt erforderlich für vom Nutzer gewünschte Dienste	226
cc) Ausgewählte Beispiele von Cookie-Kategorisierungen	229
3. Anerkannte Dienste zur Einwilligungsverwaltung (<i>Silke Jandt</i>)	230
V. Internetspezifische Datenverarbeitungen	237
1. Webdienste (<i>Henry Krasemann</i>)	237
a) Allgemeine Regelungen	238
aa) Datenschutzrechtliche Verantwortlichkeit	238
bb) Rechtsgrundlage	239
cc) Datenschutzzinformation („Datenschutzerklärung“)	241
dd) Datenminimierung	242
ee) Technisch-organisatorische Maßnahmen	242

Inhaltsverzeichnis

b) Whois-Abfragen bei ICANN und DENIC	244
2. Cloud Computing-Dienste (<i>Roland Steidle</i>)	246
a) Eigenschaften von Cloud-Diensten	246
b) Cloud-Angebote – „anything as a Service“	248
c) Private Cloud, Public Cloud und Hybrid Cloud	248
d) Datenschutzrechtliche Anforderungen	250
aa) Anforderungen an Cloud-Dienste im Zweipersonenverhältnis	250
bb) Anforderungen an Cloud-Dienste im Dreipersonenverhältnis ...	251
cc) Erfüllung der Anforderungen durch Cloud-Zertifizierung	253
dd) Anforderungen an Cloud-Anwender im Dreipersonenverhältnis	254
e) Cloud-Dienste und Datenübermittlungen in Drittländer	256
f) Zusammenfassung	258
3. Online-Suchmaschinen (<i>Silke Jandt/Moritz Karg</i>)	258
a) Verarbeitung personenbezogener Daten durch Suchmaschinenanbieter	262
b) Verantwortlichkeit	264
c) Rechtmäßigkeit der Verarbeitung personenbezogener Webinhalte ..	264
aa) Berechtigte Interessen der Suchmaschinenanbieter und Nutzer der Suchmaschine	265
bb) Verallgemeinerte Abwägung der Interessen und Grundrechte der betroffenen Person	266
cc) Verarbeitung besonderer Kategorien personenbezogener Daten	268
dd) Recht auf Löschung	271
d) Rechtmäßigkeit der Verarbeitung personenbezogener Daten der Suchmaschinennutzer	274
4. Webanalyse (<i>Silke Jandt/Moritz Karg</i>)	275
a) Rechtmäßigkeit gemäß § 25 TDDDG	277
b) Datenschutzrechtliche Bewertung der Webanalyse	281
aa) Datenschutzrechtliche Verantwortlichkeit	281
bb) Rechtsgrundlage für Webanalyse nach Datenschutz- Grundverordnung	283
cc) Transparenz- und Informationspflichten	287
dd) Pflicht zur Pseudonymisierung	288
5. Werbung (<i>Roland Steidle/Hendrik Skistims</i>)	288
a) Bedeutung der Werbung	289
b) Begriff der Werbung	291
c) Begriff der Direktwerbung	292

d) Rechtsgrundlagen der Datenschutz-Grundverordnung	293
aa) Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DS-GVO	293
bb) Vertragserfüllung nach Art. 6 Abs. 1 S. 1 lit. b DS-GVO	296
cc) Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO inklusive vernünftiger Erwartungen	297
dd) Zweckänderung nach Art. 6 Abs. 4 DS-GVO	301
e) Möglichkeiten und Grenzen der Auftragsverarbeitung nach Art. 28 DS-GVO	301
f) Informationspflichten	303
g) Rechtsgrundlagen des Entwurfs der E-Privacy-Verordnung	304
h) Wettbewerbsrechtliche Implikationen	305
i) Einzelne Werbemaßnahmen	306
aa) Direktwerbung	306
bb) Nicht-personalisierte Werbung, Banner- und Videowerbung	306
cc) E-Mail, Personal Messages, SMS	306
dd) Werbeanrufe über das Internet	307
ee) Monetarisierung von Daten über Werbenetzwerke	307
ff) Affiliate Marketing und Influencer Marketing	309
gg) Kundenbindungs- und Bonuspunktesysteme, Empfehlungsmarketing	311
hh) Werbemaßnahmen unter Nutzung von KI	313
ii) Abo-Modelle, PUR-Abo-Modelle und Cookie-Walls	314
jj) Real Time Bidding (RTB) und Transparency & Consent Framework (TCF)	319
j) Spezielle Vorgaben für Online-Plattformen nach DSA und für Torwächter nach DMA	322
k) Fazit und Ausblick	323
6. Social Networks (<i>Ubbo Aßmus</i>)	324
a) Personenbezogene Daten in Social Networks	326
b) Verantwortlichkeiten der Beteiligten	329
c) Zulässigkeit der Datenverarbeitung durch den Anbieter	331
d) Zulässigkeit der Datenverarbeitung durch den Nutzer	337
aa) Content des Nutzers	337
bb) Content mit Drittbezug	337
7. Internetbasierte Kommunikationsdienste, Messenger Dienste (<i>Ubbo Aßmus</i>)	339
a) Internationalität von OTT-Kommunikationsdiensten	340
b) Vertraulichkeit während der Kommunikation	340
c) Datenverarbeitung nach Ende des Kommunikationsvorganges	342
d) Datenverarbeitung durch die Nutzer	343

Inhaltsverzeichnis

e) Umsetzung von Informationspflichten bei OTT-Diensten	343
f) Zusammenfassung	344
8. Office-Tools im Internet (<i>Henry Krasemann</i>).....	344
a) Auftragsverarbeitung	346
b) Gemeinsame Verantwortlichkeit	347
c) Datenverarbeitung außerhalb der Europäischen Union	347
d) Datenübertragbarkeit	349
e) Verarbeitung besonderer Kategorien personenbezogener Daten	350
f) Diagnose- und Telemetriedaten	351
9. Verwaltungsleistungen im Web (<i>Anna Pokutnev</i>)	352
a) Verwaltungsportale	353
aa) Verarbeitung personenbezogener Daten in einem Verwaltungsportal	354
bb) Verantwortlicher für die Verarbeitung	354
cc) Rechtsgrundlagen für die Verarbeitung	354
b) Elektronische Verwaltungsleistungen und länderübergreifende Onlinedienste	355
c) Einer-für-Alle (EfA)-Prinzip	356
aa) Verarbeitung personenbezogener Daten in einem länderübergreifenden Onlinedienst	357
bb) Verantwortlicher für die Verarbeitung	357
cc) Rechtsgrundlagen für die Verarbeitung	359
d) Nutzerkonto, BundID und DeutschlandID	359
aa) Verarbeitung personenbezogener Daten in einem Nutzerkonto	360
bb) Verantwortlicher für die Verarbeitung	360
cc) Rechtsgrundlagen für die Verarbeitung	361
e) Registermodernisierung	363
aa) Registerführende Stellen	364
bb) Registermodernisierungsbehörde	364
cc) Bundeszentralamt für Steuern	365
dd) Nachweisübermittelnde und nachweisanfordernde Stellen und Once Only-Prinzip	365
ee) Betreiber des Datenschutzcockpits	366
f) Verarbeitungsschritte und Rechtsgrundlagen der Verarbeitung im Rahmen einer elektronischen Verwaltungsleistung	367
g) Dokumentationspflichten des Verantwortlichen	368
10. Datenschutz im eSport (<i>Tim Bagger von Grafenstein/Louisa Endrös</i>)	369
a) eSport – Hintergründe, begriffliche und strukturelle Einordnung ...	369

b) Akteure im eSport.....	371
aa) Verbände	371
bb) Publisher	372
cc) Third Party-Veranstalter	373
dd) Clubs und Clans	373
ee) eSportler	373
ee) Medien	374
ff) Rezipienten	374
c) Datenschutzrechtliche Rollenverteilung und Grundlagen	374
aa) Anwendungsbereich	374
bb) Datenschutzrechtlich Verantwortliche	375
cc) Datenschutzrechtlich Betroffene	376
d) eSport-spezifische Datenverarbeitungen	377
aa) Accounts und Spielbetrieb	377
bb) Training	383
cc) Streaming	387
dd) Anti-Cheat-Lösungen	390
11. Online-Partnervermittlungen	
(<i>Sophie Victoria Knebel/Stefanie Wegener</i>)	395
a) Verarbeitung besonderer Kategorien von Daten	397
aa) Anforderungen des Europäischen Gerichtshofs	397
bb) Praxisansicht der norwegischen Datenschutzbehörde	400
cc) Umsetzung bei Online-Partnervermittlungen	401
dd) Exkurs: Angabe des Raucherstatus – (k)ein sensibles Datum?	403
b) Minderjährigenschutz und Altersverifikation	405
aa) Digital Services Act	405
bb) Nationale Regelungen	407
cc) Bedeutung für Online-Partnervermittlungen	409
dd) Verhängte Bußgelder	410
c) Automatisierte Entscheidungen gemäß Art. 22 DS-GVO	411
aa) Preissegmentierung als automatisierte Entscheidung?	412
bb) Content Moderation	416
cc) Missbrauchs- und Betrugsprävention	420
12. Netz- und Informationssicherheit (<i>Roland Steidle</i>)	429
a) Hintergrund: Cybersicherheit in der Europäischen Union	430
b) Sicherheit der Verarbeitung: Pflicht oder Interesse?	432
c) Adressaten möglicher Maßnahmen	433
d) Risiken für die Netz- und Informationssicherheit	436
e) Datenverarbeitung gemäß Art. 6 Abs. 1 S. 1 DS-GVO	438

Inhaltsverzeichnis

f) Berechtigte Interessen zur Datenverarbeitung zwecks Abwehr von Risiken	439
aa) Präventive Maßnahmen und Tests	439
bb) Zutritts-, Zugangs- und Zugriffskontrolle	439
cc) Protokollieren von IP-Adressen	440
dd) Verhinderung der Verbreitung von Malware und Spam	441
ee) Potenziell gefährliche E-Mails und Attachments	442
g) Unbedingte Erforderlichkeit	443
h) Überwiegende Interessen der betroffenen Person	443
i) Grad der Zuverlässigkeit als Maßstab	444
j) Ausgewählter Maßnahmen	445
k) Zusammenspiel mit anderen Regelungen	446
l) Bedeutung des Erwgr. 49 für die künftige Rechtspraxis	447
13. Betrugsverhinderung und Auskunftfeien (<i>Roland Steidle</i>)	447
a) Grundsätzliches zu Erwgr. 47 DS-GVO und den vernünftigen Erwartungen	449
b) Gesetzlich Verpflichtete zur Betrugsverhinderung im Internet	450
c) Betrugsrisiken für Webdienste	451
d) Datenverarbeitung zur Betrugsverhinderung nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO	452
e) Berechtigte Interessen und Einflussnahme auf die vernünftigen Erwartungen	452
f) Einzelne berechtigte Interessen zur Betrugsverhinderung	454
aa) Datenverarbeitung bei Auskunftfeien im Internet inklusive Scoring	455
bb) Geoscoring	457
cc) Pooling	458
dd) Verwendung von Positivdaten	458
ee) Anreichern personenbezogener Daten mit Daten aus öffentlichen Quellen	459
ff) Verhinderung von Identitätsdiebstahl und -betrug mittels Geräte-ID, 2-Faktor-Authentifizierung und PKI	460
gg) Nutzen von Logdaten und Zugriffsprotokollen	463
g) Ausgewählte Maßnahmen zur Verhinderung von Betrug im Internet	464
h) Zusammenspiel mit anderen bereichsspezifischen Datenschutzvorschriften	464
i) Ausblick	465

14. Online-Banking: Deckungsabfragen, Zahlungsauslöse- und Kontoinformationsdienste (<i>Roland Steidle</i>)	465
a) Verhältnis der PSD2 zur DS-GVO und des ZAG zum BDSG	467
b) Beteiligte und Begrifflichkeiten nach dem ZAG	468
c) Deckungsabfragen beim kontoführenden Zahlungsdienstleister	469
aa) Bestätigung der Verfügbarkeit eines Geldbetrags	469
bb) Spezifische Anforderungen an die technische und organisatorische Sicherheit	470
d) Zahlungsauslösedienste	471
aa) Zugang zu Zahlungskonten	471
bb) Spezifische Anforderungen an die technische und organisatorische Sicherheit	471
e) Kontoinformationsdienste	472
aa) Zugang zu Zahlungskonten	472
bb) Spezifische Anforderungen an die technische und organisatorische Sicherheit	473
f) Spezifische Datenschutzfragen	473
aa) Verantwortlichkeit der Zahlungsdienstleister	474
bb) Ausdrückliche Zustimmung versus ausdrückliche Einwilligung	474
cc) Datenschutzrechtliche Rechtsgrundlagen zur Verarbeitung personenbezogener (Konto-)Daten	475
dd) Zweckänderung bei Kontoinformationsdiensten	476
ee) Screen Scraping versus Nutzung standardisierter Schnittstellen	476
ff) Verarbeitung zwecks Verhütung, Ermittlung und Feststellung von Betrugsfällen im Zahlungsverkehr	477
gg) Verarbeitung von Daten Dritter aus Kontobewegungen (Silent Party Data)	478
hh) Verarbeitung besonderer Kategorien personenbezogener Daten	478
15. Big Data (<i>Philipp Richter</i>)	479
a) Big Data und statistische Datenverarbeitung	480
b) Besondere Herausforderungen für den Datenschutz	482
c) Big Data als Verarbeitung für berechtigte Interessen Art. 6 Abs. 1 S. 1 lit. f DS-GVO	483
d) Interessenabwägung	484
e) Zweckbindung	484
aa) Statistische Zwecke	485
bb) Vereinbarkeit nach Art. 6 Abs. 4 DS-GVO	486
f) Automatisierte Entscheidungen und Scoring	487

Inhaltsverzeichnis

g) Amtliche Statistik	488
h) Zusammenfassende Bewertung	488
16. Künstliche Intelligenz bei Webanwendungen (<i>Thomas Wilmer</i>)	489
a) Spannungsverhältnis zwischen KI und Datenschutz	489
b) Umsetzung der Vorgaben der Datenschutz-Grundverordnung	490
aa) Verantwortliche für den KI-Einsatz	490
bb) Einhaltung der Datenschutzgrundsätze beim KI-Einsatz	491
cc) Rechtsgrundlagen für den KI-Einsatz	495
dd) Scoring	497
ee) Umgang mit besonderen Kategorien personenbezogener Daten	498
c) Betroffenenrechte bei Verarbeitungen durch KI-Systeme	499
d) Datenschutz-Folgenabschätzung bei KI	499
e) Spezifische Regelungen der KI-Verordnung	500
f) Empfehlungen zum KI-Einsatz	501
VI. Technischer und organisatorischer Datenschutz	502
1. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (<i>Philipp Richter</i>)	502
a) Datenschutz durch Technik	502
b) Datenschutzgrundsätze gemäß Art. 5 DS-GVO	503
c) Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen	504
aa) Art. 25 Abs. 1 DS-GVO	504
bb) Art. 25 Abs. 2 DS-GVO	509
cc) Art. 25 Abs. 3 DS-GVO	510
d) Sicherheit der Verarbeitung	510
aa) Art. 32 Abs. 1 und 2 DS-GVO	510
bb) Art. 32 Abs. 3 DS-GVO	513
cc) Art. 32 Abs. 4 DS-GVO	513
e) § 19 TDDDG	513
f) Zertifizierung	515
aa) Zertifizierung, Freiwilligkeit, Dynamik der Zertifizierung	515
bb) Festlegung von Zertifizierungsverfahren, Prüfzeichen und Siegeln	516
cc) Zertifizierungsstellen	517
dd) Zuständigkeit für die Zertifizierung	517
ee) Ablauf der Zertifizierung	518
g) Sanktionen und Haftung im Bereich Datenschutz durch Technik ...	520
h) Verhältnis zu Art. 24 DS-GVO	521

2. Datenschutz-Folgenabschätzung (<i>Annika Selzer</i>)	521
a) Durchführungspflicht	521
aa) Hohes Risiko als Bewertungskriterium	522
bb) Positivliste der Aufsichtsbehörde	522
cc) Bewertung des hohen Risikos	523
dd) Zweistufige Risikobewertung	525
ee) Konsequenzen der Durchführungsentscheidung	526
b) Ausnahmen von der Durchführungspflicht	526
aa) Negativliste der Aufsichtsbehörde	526
bb) Keine Datenschutz-Folgenabschätzung aufgrund spezieller Rechtsgrundlage	527
c) Durchführung der Datenschutz-Folgenabschätzung	527
aa) Inhalte der Datenschutz-Folgenabschätzung	527
bb) Phasen der Datenschutz-Folgenabschätzung	533
cc) An der Datenschutz-Folgenabschätzung Beteiligte	533
dd) Dokumentationspflicht	535
ee) Kumulierte Datenschutz-Folgenabschätzung	536
d) Vorherige Konsultation der Aufsichtsbehörde	536
3. Technische Umsetzung von Löschpflichten bei Providern (<i>Volker Hammer</i>)	537
a) Löschen? Löschen. Löschen!	538
aa) Ausgangssituation, Zielsetzung und Begriffe	538
bb) Erwartungshorizont: Löschen (nur) im Internet?	540
b) Überblick über Vorgaben zum Löschen in der Datenschutz- Grundverordnung	542
aa) Vorgaben zur Regellöschung	543
bb) Technisch-organisatorischer Aufwand	543
cc) Informationspflichten	544
dd) Löschung und Nicht-Löschung im Einzelfall	544
ee) Mitteilungspflichten	545
ff) Dokumentationserfordernisse	545
gg) Überwachung der Löschmaßnahmen	545
hh) Weiterentwicklung des Löschkonzepts	546
ii) Löschen beim Auftragsverarbeiter	546
c) Rechtliche Vorgaben für das Löschen aus anderen Quellen	546
d) Rahmenbedingungen für ein Löschkonzept	547
aa) Anforderungen an ein Löschkonzept	547
bb) Löschen bei Providern und bei anderen Verantwortlichen	548
cc) Handlungsoptionen: Löschen, Anonymisieren, Sperren	549
dd) Exkurs: Löschen ist technisch (nicht?) möglich	550

Inhaltsverzeichnis

ee) Praxistauglichkeit eines Löschkonzepts	551
e) Umsetzen der Regellöschung nach Art. 5 Abs. 1 lit. e DS-GVO gemäß DIN 66398	552
aa) Gegenstand und Aufbau der Norm	553
bb) Löschregeln festlegen	554
cc) Steuern der Umsetzung	557
dd) Weitere Aufgabenstellungen aus der Praxis	558
ee) Dokumente und Pflege des Löschkonzepts	560
f) Anwendung der DIN 66398	562
g) Umsetzen der Rechte auf Löschung und Einschränkung nach Art. 17 und 18 DS-GVO	563
aa) Löschen durch »Self-Service des Benutzers«	564
bb) Löschen durch den Verantwortlichen bei Art. 17-Anfragen	567
cc) Aussetzen der Löschung auf der Grundlage von Art. 18 DS-GVO und aus eigenen Gründen des Verantwortlichen	570
h) Nutzen eines Löschkonzeptes	572
i) Projekt »Löschkonzept«	573
j) Technische Aspekte von Löschen und Anonymisieren	573
aa) Identifikation von löschfähigen Datenobjekten	573
bb) Löschfähige Datenobjekte aus dem Verarbeitungskontext lösen	575
cc) Sicheres Löschen	576
dd) »Gutes« Anonymisieren	579
k) Kontrolle über Inhalte – auch im Internet	582
VII. Rechte der Betroffenen	584
1. Recht auf Information (<i>Annika Selzer</i>)	584
a) Informationspflichten bei Direkterhebung	584
aa) Inhalt der Informationspflicht	585
bb) Zeitpunkt der Informationspflicht	589
cc) Weiterverarbeitung für andere Zwecke	590
dd) Ausnahmen von der Informationspflicht	590
b) Informationspflichten bei Dritterhebung	592
aa) Inhalt der Informationspflicht	592
bb) Zeitpunkt der Informationspflicht	593
cc) Weiterverarbeitung für andere Zwecke	594
dd) Ausnahmen von der Informationspflicht	594
c) Weitere Anforderungen an die Information bei Direkt- und Dritterhebung	596
2. Auskunftsrecht (<i>Felix Hermonies</i>)	597
a) Inhaltliche Grundlagen	597

b) Verfahren und Form	599
c) Identifizierung	600
3. Berichtigungsrecht (<i>Felix Hermonies</i>).....	602
4. Löschungsrecht und „Recht auf Vergessenwerden“ (<i>Felix Hermonies</i>)	602
a) Löschungsrecht	602
b) „Recht auf Vergessenwerden“	604
c) Ausnahmen des Löschungsrechts	606
5. Einschränkung der Verarbeitung (<i>Felix Hermonies</i>)	607
6. Mitteilungspflicht und Unterrichtsrecht (<i>Felix Hermonies</i>)	608
7. Datenübertragbarkeit (<i>Felix Hermonies</i>)	609
8. Widerspruchsrecht (<i>Felix Hermonies</i>).....	612
9. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (<i>Felix Hermonies</i>).....	613
10. Einschränkung von Betroffenenrechten (<i>Felix Hermonies</i>)	615
VIII. Rechtsschutz für Betroffene (<i>Christian Geminn</i>).....	617
1. Recht auf Beschwerde bei der Aufsichtsbehörde	618
a) Geltendmachung des Beschwerderechts	618
aa) Adressat der Beschwerde	619
bb) Beschwerdebefugnis	622
cc) Form und Frist	622
dd) Inhaltliche Anforderungen	623
b) Pflichten der Aufsichtsbehörden	624
aa) Pflicht zur Befassung mit der Beschwerde	625
bb) Pflicht zur Unterrichtung des Beschwerdeführers	627
cc) Pflicht zur Belehrung des Beschwerdeführers	628
dd) Weitere Pflichten der Aufsichtsbehörden	628
c) Grenzüberschreitende Beschwerden	629
d) Zusammenfassung	629
2. Haftung und Recht auf Schadensersatz	630
a) Anspruchsberechtigte	631
b) Anspruchsgegner und Haftung	632
c) Verstoß	633
d) Schaden	634
e) Haftungsbefreiung	638
f) Zusammenfassung	639
3. Gerichtliche Durchsetzbarkeit	639
a) Gerichtlicher Rechtsbehelf gegen eine Aufsichtsbehörde	641
aa) Gerichtlicher Rechtsbehelf des Betroffenen gegen Beschlüsse einer Aufsichtsbehörde	642

Inhaltsverzeichnis

bb) Gerichtlicher Rechtsbehelf bei Nichtbefassung oder bei Verletzung der Informationspflicht	643
b) Gerichtlicher Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	644
c) Parallele Verfahren	647
d) Die Rolle des Europäischen Gerichtshofs	648
aa) Nichtigerklärung eines Beschlusses des Ausschusses	649
bb) Vorabentscheidung	649
e) Zusammenfassung	650
4. Vertretung von betroffenen Personen, Verbandsbeschwerde und Verbandsklage	651
5. Rechtsschutz nach der Datenschutz-Grundverordnung	653
IX. Zusammenarbeit der europäischen Aufsichtsbehörden bei grenzüberschreitenden Verarbeitungen (<i>Henning Dehnert</i>)	656
1. Der Anwendungsbereich des Kooperationsverfahrens gemäß Art. 60 DS-GVO	657
a) Bestehen einer einzigen Niederlassung oder einer Hauptniederlassung im EWR	658
b) Durchführung einer grenzüberschreitenden Verarbeitung	660
2. Ablauf des Kooperationsverfahrens gemäß Art. 60 DS-GVO	661
a) Bestimmung der federführenden und der betroffenen Aufsichtsbehörden	661
b) Durchführung der Untersuchung und Vorlage des Beschlussentwurfes	662
c) Einspruchsverfahren	664
d) Abschluss des Kooperationsverfahrens	666
3. Streitbeilegungsverfahren gemäß Art. 65 Abs. 1 lit. a DS-GVO	666
a) Allgemeines und Prüfungskompetenz des EDSA	667
b) Ablauf des Streitbeilegungsverfahrens	668
c) Rechtsschutz gegen verbindliche Beschlüsse des EDSA in Streitbeilegungsverfahren	668
d) Resümee der bislang durchgeführten Streitbeilegungsverfahren	669
4. Dringlichkeitsverfahren gemäß Art. 66 DS-GVO	669
5. Auswirkungen der EU-Gesetzgebung zur Fortentwicklung des digitalen Binnenmarktes	672
6. Ausblick	673
X. Sanktionen (<i>Jens Ambrock</i>)	675
1. Aufsichtsbehörden	675
a) Aufgaben der Aufsichtsbehörden	675

b) Untersuchungsbefugnisse der Aufsichtsbehörden	676
c) Zuständigkeit der Aufsichtsbehörden	677
aa) Sachliche Zuständigkeit	677
bb) Örtliche Zuständigkeit	679
2. Verwaltungsrechtliche Maßnahmen	680
a) Anordnungsbefugnisse	680
aa) Warnung und Verwarnung	680
bb) Anweisung	683
cc) Untersagung	684
b) Rechtsschutz	684
3. Geldbußen	685
a) Bußgeldtatbestände	687
aa) Hoher Bußgeldrahmen der Datenschutz-Grundverordnung	687
bb) Niedriger Bußgeldrahmen der Datenschutz- Grundverordnung	688
cc) Bußgeldtatbestände des Bundesdatenschutzgesetzes	689
dd) Bußgeldtatbestände des Telekommunikation-Digitale-Dienste- Datenschutz-Gesetzes	689
b) Bußgeldverfahren	690
aa) Bestimmung der Tat	690
bb) Unternehmensbegriff	691
cc) Kriterien für die Verhängung von Bußgeldern	693
dd) Bußgeldhöhe	693
c) Rechtsschutz	694
4. Strafrechtliche Sanktionen	695
5. Wettbewerbsrechtliche Sanktionen	695
6. Verbraucherschutzrechtliche Verbandsklage	695
Literaturverzeichnis	697
Stichwortverzeichnis	743

Verzeichnis der Autoren

Dr. Jens Ambrock	Referatsleiter beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
Dr. Ubbo Aßmus	Rechtsanwalt und Fachanwalt für Informationstechnologierecht; Geschäftsführer und Co-Founder der lawcode GmbH, Lehrbeauftragter an der Hochschule RheinMain
Dr. Tim Bagger von Grafenstein	Rechtsanwalt und Fachanwalt für Sportrecht und Partner bei Lentze Stopper Rechtsanwälte in München
Dr. Henning Dehnert	Referent beim Landesbeauftragten für den Datenschutz Niedersachsen
Louisa Endrös	Rechtsanwältin für Sport- und Datenschutzrecht bei Lentze Stopper Rechtsanwälte in München
Dr. habil. Christian L. Geminn	Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) und Privatdozent an der Universität Kassel
Dr. Volker Hammer	Editor der DIN 66398 „Leitlinie Löschkonzept“ und Co-Editor der ISO/IEC 27555, freiberuflicher Berater für Löschprojekte (loeschprojekte.de)
Prof. Dr. Felix Hermonies	Mag. rer. publ. LL.M. (R.L.), Professor für Datenschutz- und Medienrecht an der Hochschule Darmstadt
Dr. habil. Silke Jandt	Stellvertretende Referatsleiterin beim Landesbeauftragten für den Datenschutz Niedersachsen
Dr. Moritz Karg	Staatskanzlei Schleswig Holstein, Referatsleiter Grundsatzangelegenheiten der Digitalisierung und des EGovernments
Dr. Sophie Victoria Knebel	Senior Legal Counsel (Syndikusrechtsanwältin bei der Parshipmeet Group), Rechtsanwältin, Fachanwältin für Informationstechnologierecht sowie zertifizierte Informationssicherheitsbeauftragte (ISO 27001)
Henry Krasemann	Referatsleiter Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Dozent, Jurafunk, Kiel

Verzeichnis der Autoren

Dr. Philipp Richter	Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Anna Pokutnev	Referentin beim Landesbeauftragten für den Datenschutz Niedersachsen
Dr. Annika Selzer	Abteilungsleiterin für IT-Recht am Fraunhofer SIT und Co-Forschungsbereichsleiterin für IT-Recht in ATHENE
Dr. Hendrik Skistims	Rechtsanwalt und Syndikusanwalt bei Union Investment, Frankfurt a.M.
Dr. Tobias Stadler	Referatsleiter bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)
Dr. Roland Steidle, LL.M.	Rechtsanwalt und Fachanwalt für Informationstechnologierecht und Partner bei SWM Rechtsanwälte in Frankfurt am Main, Lehrbeauftragter an der Hochschule Darmstadt
Dr. Stefanie Wegener	Rechtsanwältin und Fachanwältin für Arbeits- und Informationstechnologierecht
Prof. Dr. Thomas Wilmer	Professor für Informationsrecht an der Hochschule Darmstadt

I. Grundlagen des Internets

Eine bereichsspezifische Betrachtung des Datenschutzrechts erfordert einen konkreten Untersuchungsgegenstand.¹ Daher ist es erforderlich, zunächst eine Beschreibung „des Internets“ zu versuchen, um als Basis der datenschutzrechtlichen Ausführungen ein einheitliches Verständnis zu erzielen.

Abstrakt beschrieben ist das „Internet“ die technische Innovation, durch die Datenverarbeitung allgegenwärtig geworden und in jeden Lebensbereich eingedrungen ist. Hinter der **Bezeichnung „Internet“** verbergen sich jedoch unterschiedliche Begriffe und ein unterschiedliches Verständnis. Auf die Frage, wie das „Internet“ definiert oder was darunter zu verstehen ist, wird es viele unterschiedliche Antworten geben, je nachdem ob sie von einem Laien, versierten Internetnutzer oder einem Informatiker stammen und auch davon abhängig, in welchem Kontext die Bezeichnung verwendet wird. Formulierungen wie „ins Internet gehen“, „im Internet surfen“, „per Internet“ oder auch schlicht „das Internet“ weisen deutlich auf die Mehrdeutigkeit des Begriffes hin. Im allgemeinen Sprachgebrauch ist keine Formulierung falsch oder missverständlich. Sie ergänzen sich und beschreiben zusammengekommen eben nicht eine konkrete Technik oder einen technischen Gegenstand, sondern ein soziotechnisches System, welches als übergeordnete Bezeichnung die gesamte Innovation des „Internets“ umfasst.

Für die datenschutzrechtliche Betrachtung bietet es sich an, das „Internet“ durch eine **Dreiteilung** differenziert zu beschreiben, die in Anlehnung an die technische Perspektive erfolgt.² Die erste Ebene ist das **physikalische Netz** als infrastrukturelle Übertragungstechnik, die unter anderem aus Festnetz, Funk, Satellit und Mobilfunknetzen von General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE) bis zunehmend aus 5G-Netzen besteht. Durch dieses und auf Basis eines einheitlichen **Netzwerkprotokolls** sind zahlreiche Rechner miteinander verbunden. Die technische Netzinfrastruktur auf erster Ebene wird nachfolgend als Internet bezeichnet.³ Hierauf baut die digitale, transportierende IP-Schicht auf, durch die unterschiedliche sogenannte Overlay-Dienste oder **Internetdienste**, wie das World Wide Web (im Folgenden Web)⁴ und E-Mail-Dienste, ermöglicht werden. Die Internetdienste bilden im folgenden Kontext zusammengekommen die zweite Ebene.⁵ Schließlich soll als dritte Ebene das Web als Ausschnitt des „Internets“ – oder genauer gesagt dieser spezifische Internetdienst – aufgrund seiner gesellschaftlichen Bedeutung vertiefend hinsichtlich seiner konkreter **Webdienste** betrachtet werden, wie **Webseiten, Suchmaschinen, Social Networks, Onlineshops, Wikis, Videoplattformen** und vie-

1 Einen besonderen Dank möchte ich an Frau Elena Richter aussprechen, die als Informatikerin beim Landesbeauftragten für Datenschutz in Niedersachsen arbeitet, und mit ihrer technischen Expertise die Ausführungen zur Technik des „Internet“ geprüft und erforderlichenfalls ergänzt und korrigiert hat.

2 S. Klopfer Netzneutralität in der Informationsgesellschaft/Ceulic, S. 20.

3 Eine begriffliche Ungenauigkeit wird im Folgenden teilweise bei der Verwendung umgangssprachlich üblicher Wortverknüpfungen mit Internet, wie zum Beispiel Internetadressen oder Internetnutzer nicht zu vermeiden sein.

4 Die korrekte Abkürzung für das World Wide Web ist „WWW“. Für eine bessere Lesbarkeit wird dennoch die Kurzform „Web“ verwendet.

5 Klopfer Netzneutralität in der Informationsgesellschaft/Ceulic, S. 20 unterscheidet die drei Ebenen physikalisches Netz, IP-Schicht sowie Dienste und Applikation.

I. Grundlagen des Internets

les mehr. Im Folgenden wird diesbezüglich die Bezeichnung **Webdienst, Web-Service oder Webanwendung** verwendet.

- 4 Die Erstellung und Gestaltung von Webseiten – das **Webdesign** – kann mittlerweile sehr vielschichtig sein. Sie beschränkt sich schon lange nicht mehr auf das Layout bestehend aus insbesondere Struktur und Aufbau, Farbschema, Typografie durch Schriftarten (Fonts), Bilder und Grafiken, Navigation, die Inhalte – den Content – und integrierte Interaktionselemente, wie Schaltflächen, Bestell- und Kontaktformulare, Zahlungsfunktionen, Chatfunktionen und die Optionen für nutzergenerierte Inhalte. Neben diesen gestalterischen und visuellen Elementen einer Webseite sind in die meisten Webseiten zahlreiche funktionelle Elemente und Dienste implementiert. Diese dienen dem Zweck die Funktionalität und Bedienbarkeit der Webseite für den Nutzer zuverlässig zu gewährleisten. Dazu gehören unter anderem die jederzeitige Verfügbarkeit und schnelle Ladezeiten, die zum Beispiel durch die Content Management Systeme, Content Delivery Networks, Analyse-Tools, Bot-Prototection, Captchas, JavaScripte, Plugins und vieles mehr umgesetzt werden können. Hinzu treten Consent Management Tools für die Abfrage und Speicherung rechtlich erforderlicher Einwilligungen. Schließlich hat auch das Tracking der Nutzer im Web mittlerweile eine solche Bedeutung erlangt, dass sowohl die unterschiedlichen technischen Umsetzungsmöglichkeiten als auch die verschiedenen Auswertungszwecke aufgezeigt werden.
- 5 Entsprechend der unterschiedlichen Ebenen des „Internets“ sind zu dessen Realisierung zahlreiche Akteure, neben den Internetkonsumenten Internetdienstleister und sogenannte **Internet-Mediäre** erforderlich, die funktionsbezogen differenziert werden. Es werden ökonomische Besonderheiten aufgeführt, da diese häufig für normative Entscheidungen insbesondere über die Auflösung von Interessenkollisionen relevant sein können.

1. Internet als technische Netzinfrastruktur

- 6 Technisch beschrieben ist das Internet ein **dezentral organisiertes, globales Rechnernetzwerk**, das aus beliebig vielen miteinander verbundenen und eindeutig adressierten lokalen und nationalen Netzen besteht und auf einem **einheitlichen und offenen Netzwerkprotokoll** basiert.⁶ Das Internet kann als das Straßennetz der Informationsgesellschaft bezeichnet werden.⁷ Genau genommen, handelt es sich beim Internet nicht um ein physikalisches Netz, sondern eine Ansammlung verschiedener Netze, die bestimmte gängige Protokolle nutzen und bestimmte allgemeine Dienste zur Verfügung stellen.
- 7 Die technische Netzinfrastruktur besteht aus **kabelbasierten und kabellosen Techniken**, die grundsätzlich unterschieden werden können. Zu der ersten Gruppe gehören ein für das Internet ausgebautes Glasfaserkabelnetz, das herkömmliche Telefonnetz mit Kupferkabeln und das Kabelfernsehtnetz aus Glasfaser- und Koaxialkabeln. Zu den

6 S. BVerfGE 120, 274 (276); Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 1; Kilian/Heussen ComputerR-HdB/Polenz Teil 13 Rn. 29 sowie zur Geschichte des Internets Strömer, Online-Recht, S. 3 ff. Der Gesetzgeber beschreibt das Internet sehr abstrakt und funktionsbezogen als „elektronisches Informations- und Kommunikationssystem“, BT-Drs. 14/6468, 5.

7 Roßnagel KJ 1990, 267 (268) hat diese Bezeichnung zuvor für die Telekommunikationstechnik gewählt.

nicht kabelbasierten Internet-Techniken für das sogenannte „mobile Internet“ gehören Mobilfunk- und Satellitennetze sowie Wireless Area Network (WLAN). Im Anschluss an die analogen Mobilfunknetze der ersten Generation, die keine praktische Relevanz mehr aufweisen, folgte Global System for Mobile Communications (GSM) als zweite, UMTS⁸ als dritte, Long Term Evolution (LTE) als vierte und 5G als fünfte Generation der Mobilfunkstandards.⁹ Die Entwicklung des nächsten Mobilfunkstandards 5G ist bereits so weit fortgeschritten, dass seit 2019 in Europa mit dem kommerziellen Ausbau begonnen wurde.

In Bezug auf den Vorgang der Datenübertragung zwischen zwei Rechnern wird die Internet-architektur als **Client-Server-Infrastruktur** beschrieben.¹⁰ Diese Beschreibung differenziert funktionsbezogen zwischen dem Server als Dienst oder Daten zur Verfügung stellendes System und dem Client als das den Dienst oder Daten anfordernde System.¹¹ Die Besonderheit im Internet ist, dass jedes Computersystem sowohl als Server als auch als Client fungieren kann. Die Bezeichnung ist abhängig davon, welche Rolle das Computersystem in einem konkreten Kommunikationsprozess einnimmt. In **Peer-to-Peer Netzwerken** vernetzen sich die einzelnen Netzwerkteilnehmer ohne zentrale Server-Komponenten und agieren gleichzeitig als Server und als Client (Servent).¹²

Jeder an das Internet angeschlossene Rechner muss zu einem Zeitpunkt eine individuelle Kennung aufweisen, um für den Prozess der Datenübertragung zwischen zwei Rechnern über die technische Infrastruktur eindeutig angesprochen werden zu können. Diese eindeutige Kennung ist im Internet-Netzwerk die **Internet Protocol (IP)-Adresse**.¹³ IP-Adressen sind numerisch und bestehen nach der noch hauptsächlich verwendeten IPv4-Spezifikation aus 32 Bits – vier jeweils durch einen Punkt voneinander abgetrennten Zahlenblöcken – mit jeweils einer maximal dreistelligen Zahl (8 Bit) im Wert zwischen null und 255 (Bytes). Die IPv4-Spezifikation wird nach und nach (sogenanntes Dual Stack) durch die seit 1998 existierende IPv6-Spezifikation abgelöst, die insgesamt 128 Bits umfasst und in acht Zahlenblöcken von je vier Ziffern (16 Bit) dargestellt wird. In Europa wurden die letzten IPv4-Adressen von der zuständigen Vergabestelle im November 2019 vergeben.¹⁴ Die IPv6-Spezifikation bietet eine deutlich größere Anzahl möglicher Adressen und ermöglicht weitere Funktionalitäten.

Um zu gewährleisten, dass jede IP-Adresse tatsächlich eindeutig einem Rechner zugewiesen ist, muss es Regeln und Verantwortliche für die Zuweisung der IP-Adressen geben. Die Koordination der **Vergabe von IP-Adressen** übernimmt die amerikanische **Internet Corporation for Assigned Names and Numbers (ICANN)**. Eine geregelte

8 UMTS wurde in Deutschland Ende 2021 abgeschaltet, s. <https://www.lte-anbieter.info/lte-news/umts-abschaltung-g-das-sind-die-termine-die-sie-kennen-muessen>.

9 Zur Entwicklung der 5G-Netzabdeckung in Deutschland, s. die Informationen der Bundesnetzagentur zum Mobilfunk-Monitoring, <https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Breitband/MobilesBreitband/start.html#Anker>.

10 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 8.

11 Hoeren/Sieber/Holzagal MMR-HdB/Sieber Teil I Rn. 20; Erlhofer, Suchmaschinen-Optimierung, S. 183 f.

12 S. die Vortragsfolien von Schiller, Telematics Chapter 10: Peer-to-Peer Networks, Nr. 10.59 f., https://www.mi.fu-berlin.de/inf/groups/ag-tech/teaching/2011-12_WS/L_19531_Telematics/10_P2P-Networks.pdf.

13 S. Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 7; Erlhofer, Suchmaschinen-Optimierung, S. 186. Die IP-Adresse kann mit einer Anschrift oder einer Telefonnummer verglichen werden, die ebenfalls mittelbar einer oder mehreren Personen zugeordnet werden können. Zum Beispiel lautet die IP-Adresse der Domain des Bundesverfassungsgerichts 77.87.229.25.

14 S. <https://www.teltarif.de/internet-ipv4-adressen-mangel/news/78790.html>.

I. Grundlagen des Internets

Vergabe selbst erfolgt durch eine der ältesten Institutionen des Internets, die Internet Assigned Numbers Authority (IANA), eine Abteilung der ICANN. Die IANA verteilt in den Anfangsjahren des Internets IPv4-Adressen in großen Adressblöcken direkt an Organisationen, Firmen oder Universitäten, die dann die weitere Verteilung selbstständig übernehmen. Seit Februar 2005 sind fünf regionale Vergabestellen, die Regional Internet Registries (RIR), eingerichtet, denen nunmehr Adressblöcke – typischerweise $/8$ in CIDR-Notation – zugewiesen werden. Die Vergabe an die Endnutzer erfolgt nach deren eigenen Regelungen für die Zuweisung von Adressen an Provider oder Organisationen, die wiederum ihre IP-Adressen selbst verwalten. Für Europa ist die **Réseaux IP Européens (RIPE)** zuständig. Die Vergabe der IP-Adresse ist damit über eine hierarchische Baumstruktur organisiert und stellt eine Ausnahme der Dezentralität des Internets da.

- 11 Einen engen Zusammenhang zur IP-Adresse weist das **Domain Name System (DNS)** auf. Jedem Domain-Namen ist eine numerische IP-Adresse eindeutig zugeordnet. Während für den technischen Zugriff auf einen Server ausschließlich die IP-Adresse erforderlich ist, ist der zusätzliche Domain-Name ein Zugeständnis an die Merkfähigkeit der Menschen, die sich eher einen begrifflichen Domain-Namen als numerische Adressen merken können, und damit an die Nutzerfreundlichkeit. Domains sind Teilbereiche des hierarchischen DNS. Vergleichbar der Situation der IP-Adressen erfolgt die Zuteilung von Domains über ein Vergabeverfahren, da diese ebenfalls im Internet weltweit einmalig und eindeutig sein müssen. Im Unterschied zum Vergabeverfahren für IP-Adressen werden Domains jedoch nicht zugewiesen, sondern sie sind unter Berücksichtigung vorgegebener Regeln frei wählbar. Die Vorgaben erfassen zunächst den Aufbau von Domains, der hierarchisch¹⁵ ist und sich in festgelegter Reihenfolge aus Top-Level-Domain (TLD),¹⁶ Second-Level-Domain (SLD)¹⁷ zusammensetzt, und können durch Verzeichnis- und Dateinamen ergänzt werden.¹⁸ Die weiteren Regeln für die Domain-Gestaltung sind von der konkreten TLD abhängig, da sie jeweils von der Vergabestelle der TLD – dem Network Information Center (NIC)¹⁹ – festgelegt werden. Die Verwaltung der Länderkennung für Deutschland *-.de* – obliegt dem **Deutschen Network Information Center eG** – oder kurz **DENIC**.²⁰ Diese hat insbesondere Regelungen für die Verwendung von Buchstaben, Umlauten und Zeichen im Domain-Namen festgelegt.²¹ Des Weiteren erfolgt die Vergabe der Domain nach dem Grundsatz „first come, first served“, so dass unter Voraussetzung der Einhaltung der weiteren Domainrichtlinien für

15 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 27.

16 TLD sind entweder geografisch und verweisen auf die Zuordnung der Webseite zu einem bestimmten Land, zum Beispiel *de*, *fr*, *uk*, oder generisch und sind einer bestimmten Gruppe zugeordnet, zum Beispiel *com*, *org*, *net*, *gov*. Eine Liste der generischen Domains findet sich bei der ICANN, s. <https://www.icann.org/en/registry-agreements>.

17 Bei der Domain <http://www.bundesverfassungsgericht.de> ist der zweite Teil – Bundesverfassungsgericht – die SLD.

18 Wie zum Beispiel */index.html*.

19 Diese wird auch Domain Name Registry genannt. Sie verwaltet eine oder mehrere Top-Level-Domains im DNS, betreibt hierfür den Nameserver und den Whois-Service mit Kontaktdaten der Domaininhaber.

20 Zu weiteren Informationen s. <https://www.denic.de/ueber-denic/>.

21 S. die von der DENIC veröffentlichte IDN-Zeichenliste, <https://www.denic.de/wissen/idn-domains#code-192-0>.

den Antragsteller die gewünschte Domain registriert wird, sofern sie noch verfügbar ist.²²

In **Overlay-Netzwerken**, wie zum Beispiel Tor (onion), GNUnet (.gnu) oder in dem für die Blockchain-Technologie verwendeten Lightning Netzwerk wird das oben genannte hierarchisch aufgebaute DNS umgangen, in dem Netzwerkverbindungen stattdessen dezentral über eigene Adressräume, Adressierungsregeln und mit Einsatz eigener Routingregeln zustande kommen. Für die Verbindung zu den im Internet verfügbaren Webdiensten werden Proxy-Server oder Outproxy genutzt. 12

In seinem bisherigen Erscheinungsbild weist das „Internet“ **vier prägende Charakteristika** auf, die allerdings nicht alle technisch zwingend sind. Dies sind im Einzelnen die **Dezentralität, Globalität, Zugangsoffenheit und Neutralität**.²³ 13

Die beiden Charakteristika der Dezentralität und der Globalität finden sich bereits in der technischen Definition des Internets wieder. **Dezentralität** bedeutet in diesem Zusammenhang, dass die technische Infrastruktur nicht über eine oder mehrere zentrale Einheiten verfügt, über die letztlich alle Rechner miteinander verbunden wären. Es existieren somit keine zentralen technischen Knotenpunkte, die als „Zugangstore“ für den Anschluss an das Rechnernetzwerk fungieren, und der Bestand des Internets hängt nicht von einer einzigen funktionierenden Zentrale ab.²⁴ Entsprechend kann das Netzwerk auch nicht durch einen zentralen Angriff in seiner grundsätzlichen Funktionsfähigkeit beeinträchtigt werden, so dass es eine geringe Verletzbarkeit und damit hohe Zuverlässigkeit aufweist.²⁵ 14

Globalität bedeutet, dass die technische Infrastruktur weltumspannend ist. Geografische oder natürliche Grenzen können die Ausbreitung der Netzwerkarchitektur nicht beeinträchtigen. 15

Das Charakteristikum der **Zugangsoffenheit** meint, dass grundsätzlich jede Person die Möglichkeit hat, den eigenen Rechner an das Internet anzuschließen und so zum Bestandteil des Rechnernetzwerks zu werden. Die Notwendigkeit, die Dienste eines Zugangsanbieters – oder auf Englisch Access-Provider – in Anspruch nehmen zu müssen, steht der Zugangsoffenheit nicht entgegen. Es bestehen technisch grundsätzlich keine begrenzten Anschlusskapazitäten, die eine Regulierung des Zugangs zum Internet erfordern würden, und der Anschluss ist unabhängig von den verwendeten Betriebssystemen und Netzwerktechniken möglich. Das Rechnernetzwerk kann beliebig ausgeweitet werden und die Anzahl der angeschlossenen Einzelrechner ist faktisch unendlich. Der Zugang zum Internet ist daher insbesondere weder staatlichen Einrichtungen, Unternehmen oder bestimmten Organisationen vorbehalten, noch existieren weitere Zugangsbeschränkungen, wie zum Beispiel Nationalität oder eine allgemeingültige Altersgrenze der Anschlussinhaber. 16

22 S. die Domainrichtlinien der DENIC unter <https://www.denic.de/domains/de-domains/domainrichtlinien/>.

23 Ursprünglich entwickelt wurde das Internet mit dem Ziel der Hochverfügbarkeit eines Kommunikationsweges, Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 10.

24 Nach Mecklenburg ZUM 1997, 525 (528) ist das Gegenstück der Netz- oder Sterntypologie die Baumtypologie der klassischen Medien.

25 S. hierzu ausführlich die Geschichte zur Entwicklung des Internets Tanenbaum/Wetherall, Computernetzwerke, S. 80 ff.

- 17 Während Dezentralität, Globalität und Zugangs Offenheit Eigenschaften des Netzwerks sind, bezieht sich die **Neutralität** auf die Datenübertragung durch dieses Kommunikationsnetz. Im Kern wird die wertneutrale, technische Funktionsweise der Datenübertragung im Internet durch den Begriff der Netzneutralität zusammengefasst.²⁶ Der zu übermittelnde Datensatz wird in einzelne Datenpakete zerlegt, die nach dem **Store-and-Forward-Prinzip** transportiert werden. Dies bedeutet, dass die Datenpakete nicht unmittelbar an den Zielrechner geschickt werden, sondern über verschiedene Zwischenrechner, auf denen sie jeweils bis zur nächsten Weiterleitung zwischengespeichert und auf Integrität geprüft werden.²⁷ Dieses Prinzip hat den Vorteil, dass Blockierungen auf Teilstrecken umgangen werden können und eine Optimierung der Netzwerkauslastung erreicht wird. Nachteil des Verfahrens sind Verzögerungen beim Transport über Teilstrecken mit Zwischenspeicherungen. Es entscheidet über den Weg, den die einzelnen Datenpakete durch das Internet zum Empfängerserver nehmen. Ergänzt wird das Store-and-Forward-Prinzip durch das **Best-Effort-Prinzip**. Danach werden alle Datenpakete gleichberechtigt übertragen, so wie es aufgrund der technischen Bedingungen am schnellsten möglich ist. Die Übermittlung der Datenpakete erfolgt immer über den schnellsten Weg für diese Methode, der nicht gleichzeitig der Kürzeste sein muss. Kommt es an einer Stelle im Netzwerk aus welchen Gründen auch immer zu einer Übermittlungsstörung, werden die Datenpakete automatisch über andere Knotenpunkte weitergeleitet.²⁸ Im Gegensatz dazu wird für wenig verzögerungstolerante Dienste wie Videostreamings oder Internettelefonie das sog. **Cut-Through-Prinzip** umgesetzt, bei dem auf Integritätsprüfungen zugunsten einer höheren Übertragungsgeschwindigkeit verzichtet wird, wenngleich mit einer höheren Fehlerrate. Zwischen den verschiedenen Prinzipien bestehen auch Mischformen.
- 18 Technisch wird die **Netzneutralität** durch den Aufbau des Datenpakets und die Regeln für deren Übertragung gewährleistet. Ein Datenpaket setzt sich aus mehreren Bestandteilen zusammen, die verschiedenen Schichten (sogenannte Layer) zugeordnet sind. Das sogenannte **DoD-Schichtenmodell** definiert vier Schichten und wird auch als **TCP/IP-Referenzmodell** bezeichnet.²⁹ Es ist ein theoretisches Denkmodell, das die systematische Darstellung des komplizierten Prozesses der Datenübertragung ermöglicht, indem auf den einzelnen Schichten die verschiedenen definierten Aufgaben dargestellt

26 S. zum Beispiel Bullinger, Netzneutralität– Wissenschaftliche Dienste des Bundestages 2010 S. 4. An dieser Stelle ist die rein technische Netzneutralität gemeint, so dass hier auf Ausführungen zur politischen und rechtlichen Diskussion der Netzneutralität verzichtet wird. S. zum technisch-traditionellen Begriff sowie zu weiteren Begriffsverständnissen Jäkel, Netzneutralität, S. 5 ff. mwN.

27 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 39.

28 Kröger/Kuner, Internet für Juristen, S. 2 f.; Sieber JZ 1996, 430.

29 RFC 760 – DoD standard Internet Protocol, <http://www.faqs.org/rfcs/rfc760.html>. Zum Transmission Control Protocol (TCP) s. Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 19 f. Die Abkürzung DoD als Bezeichnung des Schichtenmodells bedeutet Department-of-Defence und beruht darauf, dass das Internet vom amerikanischen Verteidigungsministerium entwickelt worden ist. Neben diesem vierschichtigen Modell wird häufig auf das OSI-Schichtenmodell verwiesen, dass später von der International Organization for Standardization (ISO) entwickelt wurde. Insgesamt sind vier Schichten im DoD-Schichtenmodell definiert, die sich mit dem siebenschichten OSI-Schichtenmodell (Open Systems Interconnection Reference Model) vergleichen lassen. Das DoD-Schichtenmodell stellt eine vereinfachte Variante des OSI-Schichtenmodells dar, die in diesem Kontext als ausreichend erachtet wird. In dem ab 1977 entstandenen OSI-Schichtenmodell wurden die Netzzugangs- und die Anwendungsschicht des DoD-Modells granularer dargestellt und mit den damit insgesamt definierten sieben Schichten eine flexiblere und abwärtskompatible Zuordnung der in Computer- und Netzwerk-Technik zu definierenden Vorgänge ermöglicht.

werden. Eine Konkretisierung dieser Aufgaben in Bezug auf ihre Realisierung erfordert darüber hinaus die Definition von Regeln und Konventionen, wie diese Aufgaben auf der jeweiligen Schicht zu erfüllen sind und die Kommunikation zwischen den Schichten zu erfolgen hat. Diese Regeln sind in den sogenannten Protokollen festgelegt.³⁰

Die Charakteristika der Dezentralität, Globalität und Zugangs Offenheit führen dazu, dass das Internet insgesamt technisch **heterarchisch** aufgebaut ist. Die technische Infrastruktur bedarf weder zentraler Einheiten oder zentraler Zugangsschnittstellen noch folgt – bisher – die Datenübermittlung hierarchischen Regeln. Lediglich die Vergabe von IP-Adressen und Domain-Namen erfolgt nach festgelegten Regeln und das DNS ist hierarchisch aufgebaut, um die eindeutige Zuordenbarkeit von einmaliger IP-Adresse und Domain-Namen zu gewährleisten. Hiervon unterscheidet sich das sogenannte **Darknet**, das – vereinfacht dargestellt – ein-anonymes abgeschirmtes Netzwerk darstellt, das auf einem dezentralen Overlay-Netzwerk basiert und deshalb ohne zentrale Verwaltungsinstanzen wie das Domain Name System (DNS) auskommt. Für den Zugang zu einem Darknet, beispielsweise in Tor, werden ein spezifischer Browser – TOR-Browser – sowie Zugangsinformationen benötigt. Für die Anonymisierung des kompletten Datenverkehrs leitet der Dienst „The Onion Routing“ jedes ein- und ausgehende Datenpaket mit einer zufällig ausgewählten Route über das Tor-Server-Netzwerk um.³¹ 19

2. Internetdienste

Die technische Infrastruktur des Internets wird erst durch die zahlreichen **Internetdienste** zum Leben erweckt. Sie stellen das Internet in einen – wenn auch noch sehr abstrakten – Anwendungskontext und ermöglichen dem Menschen die Nutznießung der reinen Internettechnik. Auf dieser hohen Abstraktionsebene kann das „Internet“ als Medium zur Kommunikation zwischen Menschen beschrieben werden. Es handelt sich wie bei den Ursprüngen der Telekommunikation über Festnetztelefonie um eine Form technisch vermittelter Kommunikation. Dies allerdings mit dem wesentlichen Unterschied, dass jegliche Inhalte multimedial vermittelt werden können. 20

Grundvoraussetzung für die Nutzung aller Internetdienste ist, dass mit einem Rechner ein Zugang zum Internet als technische Netzinfrastruktur aufgebaut werden kann; es wird ein Internetzugang – auch Internetverbindung oder Internetanschluss – benötigt. Neben der technischen Ausstattung, wie zum Beispiel einem Router, wird für die Datenverbindung eines Computers oder eines Netzwerkes mit dem Internet vor allem eine IP-Adresse benötigt. Die meisten Teilnehmer erreichen die Internetverbindung über einen Internetzugangsdienst (**Access Providing**).³² Diese Dienstleistung besteht in der Bereitstellung sogenannter Internet-Konnektivität, das bedeutet dem Transfer von IP-Paketen ins und aus dem Internet. 21

30 Hoeren/Sieber/Holznapel MMR-HdB/Sieber Teil 1 Rn. 40.

31 S. Hoffmann, Darknet: So funktioniert es, PC-Magazin vom 13.9.2016, <http://www.pc-magazin.de/ratgeber/dark-net-funktionsweise-nutzen-3196735-15344.html>.

32 S. auch → Rn. 46 f. Im Jahr 2023 waren 91,7 % der Haushalte in Deutschland mit einem Internetzugang ausgestattet, s. <https://de.statista.com/statistik/daten/studie/153257/umfrage/haushalte-mit-internetzugang-in-deutschland-seit-2002/>.

I. Grundlagen des Internets

- 22 Einer der bekanntesten und wohl auch bedeutendsten Internetdienste ist das **World Wide Web (WWW)**,³³ das eine Übertragung von multimedialen Webseiten auf der Grundlage des **Hypertext Transfer Protocol (HTTP)** ermöglicht.³⁴ Diese Webseiten können theoretisch von jeder Person, die technischen Zugang zum Internet hat, zur Verfügung gestellt³⁵ und grundsätzlich von jedem Nutzer des Internets – sei es über einen eigenen oder fremden Internetzugang – abgerufen werden.
- 23 Eine Schlüsselfunktion für die Nutzung des Webdienstes nehmen **Webbrowser**³⁶ ein. Der Webbrowser ist eine Software für den Aufruf und die Darstellung von Webseiten und stellt die Benutzeroberfläche für Webanwendungen dar. Im Web stehen verschiedene Webbrowser zum kostenlosen Download zur Verfügung. Sie besitzen regelmäßig eine definierte Startseite, die beim Programmstart angezeigt wird. Wesentliche Bestandteile sind neben einer großen Ansichtsfläche für die Darstellung der Webseiten eine Adressleiste, in die der Domain-Name oder die URL der aufzurufenden Webseite eingegeben wird, und ein Eingabefenster für Suchbegriffe, die direkt eine Suchmaschine ansprechen.³⁷ Daneben verfügen Webbrowser über zahlreiche weitere Schaltflächen und Funktionen, die das Navigieren im Web erleichtern sollen, wie zum Beispiel die Darstellung eines Verlaufsprotokolls (Chronik), ein Verzeichnis mit Lesezeichen, und den Client vor Maßnahmen des Servers schützen sollen, wie die Steuerung der Verwendung von Cookies und Proxy-Servern, Sicherheitskontrollen mit Warnhinweisen auf Malware- und Phishing-Angriffe sowie Anti-Tracking-Funktionen. Die in einigen Webbrowsern vorhandene Konfigurationsmöglichkeit für die Proxy-Einstellung ermöglicht einen Zugang zu den außerhalb des regulären Internets erreichbaren Overlay-Netzwerken wie Tor, Freenet und I2P.
- 24 Ein weiterer sehr wichtiger Internetdienst ist die **E-Mail** als elektronisches Gegenstück zum Brief.³⁸ **Die Versendung von E-Mails basiert im Internet auf dem Simple Mail Transfer Protocol (SMTP)**.³⁹ Für den Empfang von E-Mails stehen mit dem Internet Message Access Protocol (IMAP) und Post Office Protocol (POP) zwei verschiedene

33 Die Bezeichnung Internet, auch teils „Clear Web“ genannt, wird sehr häufig nicht in Bezug auf die technische Infrastruktur, sondern als Synonym für das Web verwendet, wie zum Beispiel bei der umgangssprachlichen Formulierung, „im Internet suchen“. In der Entscheidung des LG Mannheim Urteil – 8.3.1996 - 7 O 60/96 CR 1996, 353 (354) wird das Web korrekt als Teilbereich des Internets beschrieben. Als Deep Web bezeichnete Netzwerke sind hingegen Teile des World Wide Webs, die mit allen Browsern ohne Proxy-Dienste erreichbar, aber als abgeschlossenes Netzwerk nur für autorisierte Benutzer oder Endgeräte zugänglich sind, u.a. zum Beispiel Firmen- oder Banknetzwerke. Aus diesem Grund sind Inhalte des Deep Webs auch nicht indexierbar für Suchmaschinen. Laut BSI „handelt es sich dabei um „90 % des gesamten Internets“. Webseiten im Darknet stellen einen eher kleineren Teil des Deep Web dar. Deren Adressen werden nicht über den DNS-Server verwaltet, weshalb sie nur durch spezifische Suchmaschinen und Zugangspunkte des jeweiligen Overlay-Netzwerks oder Darknets auffindbar sind.

34 S. Moritz/Dreier E-Commerce-HdB/Federrath/Pfützmann Teil A Rn. 42 ff.

35 Mittlerweile ist das Erstellen – zumindest einer professionellen – Webseite allerdings sehr komplex geworden. Eine Domain kann noch relativ einfach erworben werden, sofern die Wunschdomain noch nicht belegt ist. Im Web stehen zahlreiche, auch kostenlose Programme für das Webdesign zur Verfügung, um u.a. Layoutvorlagen, Kontaktformulare und Suchfunktionen sowie Tools um Fotos, Videos, Hyperlinks usw. einzubinden. Um die Auffindbarkeit der Webseite zu gewährleisten, empfiehlt sich die Suchmaschinenoptimierung und die Webseite muss rechtliche Anforderungen, wie zum Beispiel die Impressumspflicht, erfüllen.

36 Vereinzelt wird im Folgenden auch die Kurzbezeichnung Browser verwendet.

37 Regelmäßig ist bei jedem Browser eine Suchmaschine vorausgewählt. Diese kann aber vom Nutzer beliebig konfiguriert werden.

38 S. Moritz/Dreier E-Commerce-HdB/Federrath/Pfützmann Teil A Rn. 38 ff.

39 Die Übertragung im Internet erfolgt ebenfalls nach dem Store-and-Forward-Prinzip.

Protokolle zur Verfügung. Mittels einer E-Mail kann über das Internet eine Nachricht von einem Absender an einen oder mehrere Empfänger übermittelt werden. E-Mail-Dienste werden von E-Mail-Providern (oder auch E-Mail-Service-Providern) angeboten. Diese verwalten und veröffentlichen Mail Exchange Resource Records (MX-RR) der für die E-Mail-Konten genutzten Domains und verfügen über einen Mailserver, auf dem die E-Mail-Konten (oder auch E-Mail-Postfächer) der Nutzer gespeichert werden.⁴⁰ Jedes E-Mail-Konto wird durch eine E-Mail-Adresse, die dem Nutzer eindeutig zugewiesen wird, repräsentiert. Die E-Mail-Adresse, die für den Informationsaustausch benötigt wird, ist weder an eine bestimmte Örtlichkeit noch an einen bestimmten Rechner gebunden. Über die von den E-Mail-Providern angebotenen Webseiten können die einer E-Mail-Adresse zugeordneten Nachrichten von überall und mit beliebigen Endgeräten, insbesondere Desktops, Notebooks und Smartphones, die an das Internet angeschlossen sind, gelesen werden. Weitere Beispiele für Internetdienste sind Chat, Dateiübertragung, Internettelefonie und Internetrundfunk.

Durch den **Europäischen Kodex für elektronische Kommunikation (EKEK)**⁴¹ wurde eine neue Unterkategorie von Internetdiensten definiert, die entsprechend in die deutsche Definition der Telekommunikationsdienste übernommen worden ist.⁴² Die Definition der elektronischen Kommunikationsdienste gemäß Art. 2 Nr. 4 EKEK umfasst nunmehr neben der Unterkategorie „Internetzugangsdienste“, die Unterkategorie **„interpersonelle Kommunikationsdienste“**.⁴³ Die interpersonellen Kommunikationsdienste werden häufig auch als **Over-the-Top-Kommunikationsdienste (OTT-Kommunikationsdienste)** (→ V. Rn. 292 ff.) bezeichnet. Diese Bezeichnung macht ihre Zwitterstellung zwischen den Internet- und den Webdiensten deutlich. OTT-Kommunikationsdienste sind zu herkömmlichen Übermittlungsdiensten funktional gleichwertige Online-Dienste, die eine interpersonelle (Individual-)Kommunikation ermöglichen.⁴⁴ Beispielhaft genannt werden regelmäßige **VoIP-Telefonie**, **Nachrichtenübermittlung (Messaging)** und **webgestützte E-Mail-Dienste**. Mobile Instant Messaging-Dienste wie Signal, WhatsApp und Threema haben zu einem sehr starken Rückgang von SMS und MMS geführt und dienen teilweise als Äquivalent für E-Mails. Vor allem haben sie aber insgesamt einen starken Anstieg von Kommunikationsvorgängen bewirkt, insbesondere da unterschiedliche Nachrichtenformen – Bild-, Text-, Video- und Sprachnachrichten möglich und kombinierbar sind. Spätestens seit der Corona-Pandemie und dem ersten „Lockdown“ in Deutschland im März 2020 haben zudem **Videokonferenzdienste** eine große Bedeutung erlangt und werden in Unternehmen, Behörden, Schulen, Universitäten und sogar Gerichten als Ersatz für Präsenzveranstaltungen oder Telefonate eingesetzt. Um die Einordnung von Videokonferenzdiensten als individuelle Kommuni-

40 IdR bieten E-Mail-Provider weitere Zusatzdienste wie insbesondere den Schutz vor Spam-E-Mails und Computerviren an.

41 RL (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung)/Text von Bedeutung für den EWR, s. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018L1972>.

42 S. ausführlich zur Ausweitung der rechtlichen Definition der Telekommunikationsdienste, → IV. Rn. 5.

43 Eine dritte Unterkategorie bilden die an dieser Stelle nicht relevanten „Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden“.

44 S. Engeler/Felber ZD 2017, 251 (254).

I. Grundlagen des Internets

kationsdienste hat sich allerdings – anscheinend ausschließlich – in Deutschland eine neue rechtliche Diskussion entfacht.⁴⁵

- 26 Charakteristisch für das Internet sind noch weitere, ergänzende Dienstleistungen, die für die Realisierung der Internetnutzung erforderlich und in diese eingebunden sind. Der **DNS-Service** wandelt den als Internetadresse bezeichneten Domain-Namen in die generische IP-Adresse um, die für den technischen Zugriff auf einen Server notwendig sind.⁴⁶ Im Web besteht die Internetadresse oder genauer gesagt der **Uniform Resource Locator (URL)** aus der Domain gegebenenfalls ergänzt um weitere Verzeichnisse und Dateizeichnungen.⁴⁷ Die URL dient der Vereinheitlichung der Bezeichnung der Dokumente im Internet. Bei der E-Mail-Kommunikation ist jede individuelle E-Mail-Adresse einer Domain zugeordnet. Auf einer dem Aufruf der Internetseite über die URL oder der Übermittlung der E-Mail an den Empfänger vorgelagerten abstrakten Ebene „entscheidet“ der DNS-Service, ob der durch den Domain-Namen bezeichnete Server der Internetseite oder des E-Mail-Providers tatsächlich dem Nutzer angezeigt oder Daten an ihn übermittelt werden. Fehler oder gezielte Veränderungen bei der Zuordnung einer Domain zu der korrekten IP-Adresse hätten zur Folge, dass der Zugriff auf bestimmte Server über den Domain-Namen nicht realisiert wird. Sofern IP-Adressen nicht mehrfach genutzt werden, wie zum Beispiel beim Shared Hosting, können Internetseiten im Web in der Regel auch durch die direkte Eingabe der IP-Adresse im Browser aufgerufen werden. Dann erfolgt der Aufruf der Internetseite unmittelbar und ohne den technischen Zwischenschritt über den DNS-Server.
- 27 Während der Begriff Internet das technische System beschreibt, sind die Kategorien der **Internetdienste** die Grundlagen der Nutzung durch den Menschen. Sie decken im Wesentlichen jeweils eine oder mehrere von vier Funktionen ab, die einen gemeinsamen Nenner bilden. Dies sind im Einzelnen der Austausch von Informationen, die Kommunikation, die Interaktion sowie der Aufbau und die Pflege sozialer Beziehungen.

3. Webdienste

- 28 Eine weitere Konkretisierung der Beschreibung des „Internets“ kann durch eine nähere Betrachtung der Inhaltsebene, insbesondere der **Webdienste** erreicht werden, indem erstens eine generelle Beschreibung eines Webdienstes vorgenommen wird und zweitens beispielhaft Kategorien von Webdiensten funktional und entsprechend ihrer Zweckbestimmung qualifiziert werden.
- 29 Das Web ist in seiner Gesamtheit eine Sammlung unzähliger Dokumente, die als **Webseiten** auf Webservern abgelegt sind und auf die über das Internet und den Webbrowser zugegriffen werden kann.⁴⁸ Das Aufrufen von Webseiten erfolgt als Datenübertragung

45 S. Roßnagel NJW 2023, 400 sowie → Rn. 77.

46 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 25 ff.

47 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 43. Auf der Domain der Universität Kassel (uni-kassel.de) findet sich zum Beispiel die Unterseite des Wissenschaftlichen Zentrums für Informationstechnikgestaltung durch die Ergänzung um die Verzeichnisse eecs, iteg und startseite, s. <http://www.uni-kassel.de/eecs/iteg/startseite.html>.

48 Hoeren/Sieber/Holzsnagel/ MMR-HdB/Sieber Teil 1 Rn. 80.

Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragraphen (Beitrag), die mageren auf die Randnummer.

- 1 & 1 **X** 36
- § 25 Abs. 2 TDDDG
 - Ausnahmetatbestand **IV** 111
 - Missbrauchsgefahr **IV** 111
- § 25 TDDDG
 - Schutzzweck **IV** 59
- § 26 TDDDG **IV** 61
- § 2 Abs. 2 Nr. 1 TDDDG **IV** 89
- ABBO Projekt **V** 565
- Ablichtung **II** 35
- Abo-Modelle **IV** 84
- Abrechnung **IV** 15
- Abschreckung **VIII** 55
- Abwägung
 - Kriterien **III** 100 f.
- Account **V** 377 ff.
- Act **II** 44
- Affiliate-Marketing
 - Transaktionszuordnung **V** 208
 - Transaktionszuweisung **V** 209
- Aktualisierung **VI** 45
- Aktuelle Situation **V** 33
- Alexa **II** 36
- Algorithmen **V** 644, 646
- Allgemeine Geschäftsbedingungen
 - V** 260, 547
- Allgemeine Handlungsfreiheit **II** 3
- Allgemeine Nutzungsbedingungen
 - V** 280
- Allgemeines Persönlichkeitsrecht
 - II** 3, 17
 - Vertraulichkeit und Integrität **II** 38
- Allgemeinzugänglichkeit **V** 96
- Alphabet Inc. **X** 48
- Altersverifikation **V** 441
- Altersverifikationssysteme **V** 439
- Altvertrag **III** 227
- Amazon **X** 35
- Amazon Alexa **II** 36
- Amtliche Statistik **V** 627, 654
- Amtsgericht **X** 56 f.
- Amtshilfe **IX** 12
- Amtshilfeersuchen **IX** 26
- Anbieter digitaler Dienste
 - Marktmacht **V** 224 ff.
- Anfangsverdacht **X** 4
- Angemessenes Datenschutzniveau
 - III** 257 ff.
- Angemessenes Entgelt
 - gleichwertige Alternative **V** 228
- Angemessene Sicherheit **V** 490
- Angemessenes Schutzniveau **V** 490
- Angemessenheitsbeschluss **II** 11
- Angemessenheitsbeschlüsse der Kommission
 - Andorra **III** 251 ff.
 - Argentinien **III** 251 ff.
 - Färöer-Inseln **III** 251 ff.
 - Guernsey **III** 251 ff.
 - Isle of Man **III** 251 ff.
 - Israel **III** 251 ff.
 - Japan **III** 251 ff.
 - Jersey **III** 251 ff.
 - Kanada **III** 251 ff.
 - Neuseeland **III** 251 ff.
 - Schweiz **III** 251 ff.
 - Südkorea **III** 251 ff.
 - Uruguay **III** 251 ff.
 - Vereinigten Staaten von Amerika (EU-US Data Privacy Framework „DPF“)
 - III** 251 ff.
 - Vereinigtes Königreich **III** 251 ff.
- Anlassfreie Prüfung **X** 4
- Anonyme Daten **III** 25, **V** 626 f.
- Anonyme Datensammlungen **III** 18 f.
- Anonymisieren **VI** 126, 272 ff.
 - Generalisierung **VI** 276 ff.

Stichwortverzeichnis

- informationelle Selbstbestimmung **III** 25
- Maßnahmen **VI** 273 ff.
- Qualitätskriterien **VI** 274 ff.
- Rechtsgrundlage **III** 25
- sicheres Löschen **VI** 273 ff.
- Verarbeitung **III** 25
- Vorgaben im Katalog der Löschregeln **VI** 279
- Anordnung **X** 18 ff.
- Anspruch auf Unterlassung **VIII** 106
- Anwälte **V** 322
- Anweisung **X** 26 ff.
- Anwendbares Datenschutzrecht
- Suchmaschine **V** 76
- Anwendungsvorrang **II** 44, 49 ff., **IV** 35, 37
- europäisches Sekundärrecht **IV** 38
- App
- Kinder **II** 64
- Application Service Providing **V** 42
- Äquivalenzklasse **VI** 277
- Arbeitnehmer **II** 59 ff.
- Art. 1 Abs. 1 lit. b Info-RL **IV** 110
- Art. 27 DSA
- Empfehlungssysteme **V** 463
- Art. 5 Abs. 1 lit. b DS-GVO **IV** 76
- Art. 5 Abs. 3 S. 2 E-Privacy-Richtlinie **IV** 106
- Art. 6 Abs. 1 DS-GVO **IV** 40
- Art. 6 Abs. 1 lit. f DS-GVO **IV** 107
- Art. 7 Abs. 3 S. 3 DS-GVO **IV** 89
- Ärzte **V** 322
- Ärztewertung **II** 23
- Audiodatei **II** 36
- Aufenthalt, gewöhnlicher **VIII** 84
- Aufsicht **X** 1 ff.
- Aufsichtsbehörden **VI** 60, **X** 2 ff.
- Aufgaben **X** 3
- Aufklärung des Sachverhalts **VIII** 27
- Beratung **X** 3
- Betroffene **VIII** 11
- Informationen über Sachverhalte **VIII** 15
- Personalbedarf **VIII** 23
- Pflichten **VIII** 22 ff.
- Pflicht zur Befassung mit der Beschwerde **VIII** 25 ff.
- Pressearbeit **X** 3
- Rechtsschutz **X** 32, 56
- Untersuchungsbefugnis **X** 4
- Verschwiegenheitspflicht **VIII** 39
- Zuständigkeit **VIII** 11, **X** 8 ff.
- Auftragsdatenverarbeitung **III** 182
- Auftragsverarbeiter **III** 91, **VI** 38, **X** 46
- Auftragsverarbeitung **V** 6, 8, 121, 309
- Adressdatenbereinigung **V** 180
- Aggregation Kundenstamm **V** 179
- Analyse **III** 219
- Cloud Computing **III** 218
- Datenträgervernichtung **III** 221
- Dienstleister **III** 182
- DIN 66399 **III** 221
- Dritter **III** 184
- Firewall **III** 220
- Geldbuße **III** 234
- Hosting **III** 217
- Logging **III** 217
- Privilegierung **III** 184
- Selektionskriterien **V** 178
- Shredder **III** 221
- Tracking **III** 219
- Wartungsdienstleistung **III** 222
- Waschabgleiche **V** 180
- Weisungsgebundenheit **V** 178
- Auftragsverarbeitungsvertrag
- Arten der Verarbeitung **III** 195
- Art personenbezogener Daten **III** 197
- Auskunft **III** 208
- Dauer **III** 194
- Format **III** 191
- Frist **III** 194
- Gegenstand der Verarbeitung **III** 193
- Pflichten **III** 208
- Standarddatenschutzklauseln **III** 192
- Technische und organisatorische Maßnahmen **III** 210

- unbefristet **III** 194
- Unterstützung **III** 208
- Vertrag **III** 191
- Weisungsrecht **III** 200
- Zweck **III** 196
- Auftragsverhältnis **V** 291
- Innenverhältnis **III** 183
- Auskunft **II** 10, 20
- Auskunfteien **II** 63
- Anfragedaten **V** 550
- Anreichern von Daten **V** 558
- Einmeldung **V** 550 ff.
- Geringfügigkeitsschwelle bei Einmeldung **V** 553
- offene Forderung **V** 551
- Öffentliche Quellen **V** 558
- Positivdaten **V** 557
- Restschuldbefreiung **V** 558
- Rücklastschriften **V** 552
- Schutz vor Forderungsausfällen **V** 549
- Scorewert **V** 552
- Scoring **V** 549
- unsichere Zahlart **V** 549
- Wahrscheinlichkeitswert **V** 552
- Zahlartensteuerung **V** 549
- Zahlungsrückstände **V** 552
- Auskunftsrecht **VII** 37 ff.
- Entgelt **VII** 43
- Fernzugang **VII** 44
- Format **VII** 43
- Grundlagen **VII** 38 f.
- Identifizierung **VII** 45 ff.
- Informationen **VII** 38 f.
- Online-Auskunft **VII** 45
- Verfahren **VII** 42 ff.
- Wahrnehmung **VII** 41
- Ausland **III** 232, **V** 315
- Ausländerdiskriminierung **X** 44
- Auslandsübermittlung **X** 31
- Auslegungsregeln **IV** 107
- Auslistung **V** 92, 97 ff.
- Ausnahmen vom Minderjährigenschutz **V** 447
- Außergewöhnliche Umstände **IX** 26 f.
- Aussetzen der Regellöschung
- Einschränkung der Verarbeitung **VI** 243
- umsetzen **VI** 244 ff.
- Authentifizierung **V** 561
- 2-Faktor-Authentifizierung **V** 561
- biometrische Merkmale **V** 561
- Google Authenticator **V** 561
- mobile TAN **V** 561
- QR Code **V** 561
- Automatisierte Einzelentscheidung **III** 173, **V** 650 f.
- Automatisierte Entscheidungen **V** 451, 459, 652
- Content Moderation **V** 458
- Missbrauchsprävention **V** 450
- Backup
- Löschen **VI** 202
- Banklizenz und Erlaubnis **V** 580
- Banner **V** 133
- Basis- und Zusatzdienste
- Gesamtangebot **IV** 112
- Bedingungen der elektronischen Datenverarbeitung
- allgegenwärtiges Computing **III** 15
- Digitalisierung **III** 15
- Großrechner **III** 15
- Internet der Dinge **III** 15
- Maschine-zu-Maschine-Kommunikation **III** 15
- Bedingungen des Datenschutzrechts
- Digitalisierung **III** 16 f.
- IP-Adressen **III** 17
- MAC-Adressen **III** 17
- Metaverse **III** 17
- Zunahme personenbezogener Verarbeitungen **III** 17
- Begriffsbestimmungen der DS-GVO **III** 2
- Belangloses Datum **II** 18
- Belastbarkeit **VI** 43
- Beratung durch Aufsichtsbehörde **X** 3

Stichwortverzeichnis

- Berechtigte Interessen **III** 83, 87 f.
 - Cheating **V** 413
 - Dienstverhältnis **V** 544
 - Drittinteresse **V** 85
 - Interessenabwägung **V** 87
 - Kundenverhältnis **V** 544
 - Maßgebliche Beziehung **V** 544
 - Öffentlichkeit **V** 85
 - Subjektiver Erwartungshorizont **V** 544
 - Suchmaschine **V** 85 ff.
 - Vernünftige Erwartungen **V** 544
- Bereicherungsabsicht **X** 58
- Berichtigung **II** 10, 20, **V** 633, **VII** 49
- Berufsgeheimnisträger **III** 226
- Beschäftigtendatenschutz **II** 59 ff.
- Beschäftigtendatenschutzgesetz **II** 62
- Beschäftigungsverhältnis **III** 178
- Beschluss des Ausschusses
 - Nichtigerklärung **VIII** 95 f.
- Beschlussentwurf
 - Bindungswirkung **IX** 15, 17
 - überarbeiteter **IX** 17
 - unverzügliche Vorlage **IX** 13
- Beschwerden
 - anonyme **VIII** 18
 - Datenschutzverstöße auf Webseiten **VIII** 28
 - exzessive **VIII** 20
 - grenzüberschreitende **VIII** 39a
- Beschwerdeverfahren
 - DSA **V** 462
- Besondere Kategorien personenbezogener Daten **III** 147 ff., **V** 422
 - kontextbezogene Analyse **V** 423
 - Suchmaschine **V** 91 ff.
 - zweckbezogene Auslegung **V** 423
- Bestandsdaten **VIII** 3a
- Bestandsdatenauskunft **II** 65
- Bestätigung Geldbetrag **V** 591 ff.
- Bestimmbarkeit **II** 8
- Bestimmtheit **X** 28
- Bestimmtheitsgebot **X** 38
- Betroffene **III** 198, **V** 321
- Betroffene Aufsichtsbehörde **IX** 10
- Betroffenenrechte **II** 10, 20, **III** 103, **VII** 1
 - Einschränkung der Verarbeitung **VI** 152, 216, 241 ff.
 - Recht auf Löschung **VI** 151, 216 ff.
- Betroffene Person
 - Rechte der Erben **III** 6
 - Verstorbene **III** 6
- Betrug
 - Beleidigung **V** 541
 - Fake-Bewertung **V** 541 f.
 - Nutzungsbedingungen **V** 541
 - Wettbewerbsrecht **V** 541
- Betrugsverhinderung **V** 532, 535 ff.
 - Tracking **V** 565
- Betrugsverhinderung im Zahlungsverkehr **V** 615 ff.
- Beweismittel
 - des Betroffenen nicht löschen **VI** 241
 - des Verantwortlichen nicht löschen **VI** 242
- Bewertung **VI** 45
- Bewertungsportal **II** 3, 23
- BFStrMG
 - Löschen **VI** 163
- Big Data **II** 13, 15, 18, **V** 619
- Bild **II** 35 f.
- Bildveröffentlichung **II** 59
- Binding Corporate Rules **III** 258
- Biometrische Daten **III** 149, 152 ff.
- Blacklist **V** 524
- Blockchain **III** 34 f.
- Blog **II** 58
- Bonität **II** 63
- Bonitätsauskünfte **V** 534, 569
- Briefwechsel **II** 26 ff.
- Browser
 - Chronik **IV** 54
- Browserdaten **IV** 34
- Browser-Fingerprint **V** 560
- Browserfingerprinting **V** 111 f.

- Browsersequenzen
 - Rückschlüsse **IV** 34
- Browser-Sniffing
 - Google Topics **IV** 29
- BSI-Grundschutz **V** 58, 524
- Bundesamt für Sicherheit in der Informationstechnik **V** 503
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) **V** 576
- Bundesdatenschutzgesetz **III** 174 ff.
- Bundeskartellamt **X** 60
- Bundesnetzagentur **X** 11
- Business Process Outsourcing **V** 62
- Bußgeld **X** 33 ff.
 - Bestimmtheitsgebot **X** 38
 - Höhe **X** 40 ff., 53 ff.
 - Kriterien **X** 51
 - Tatbestände **X** 37 ff.
 - Unverhältnismäßigkeit **X** 23 f.
 - Verfahren **X** 46 ff.
- Bußgelder **V** 448
 - Berechnung **IX** 24
- Bußgeldkonzept **X** 54
- Cache
 - Speicherung **V** 80
- Charta der Digitalen Grundrechte **II** 2
- Charta der Grundrechte **II** 2 ff.
- Chat **II** 31
- Chatbot **II** 15
- China **III** 257
- Client-Service-Infrastruktur **I** 8
- Cloud **II** 20
- Cloud Computing **II** 41, **III** 90, **V** 34 ff., **X** 46
 - Abhängigkeit **V** 46
 - Anything as a Service **V** 42
 - Application Service Providing **V** 42
 - Auftragsverarbeitung **V** 49
 - BSIG **V** 54
 - Business Process Outsourcing **V** 62
 - CLOUD Act **V** 69
 - Dreipersonenverhältnis **V** 48 ff.
 - Drittland **V** 65
 - eigenes Geschäftsinteresse **V** 56
 - Einwilligung **V** 63
 - Ende-zu-Ende Verschlüsselung **III** 29
 - EU-US Data Privacy Framework (DPF) **V** 68
 - Executive Order 12333 (EO 12333) **V** 69
 - Executive Order vom 7.10.2022 **V** 68
 - Flexibilität **V** 38
 - Foreign Intelligence Surveillance Act (FISA) **V** 69
 - gemeinsame Verantwortung **V** 55
 - Grid Computing **V** 35
 - Hybrid Cloud **V** 44
 - Infrastructure as a Service **V** 42
 - Kontrollen **V** 57
 - Kostenersparnis **V** 39
 - Mandantenfähigkeit **V** 40
 - Microsoft Deutschland Cloud **V** 70
 - Muttergesellschaft **V** 67
 - Off-Premise **V** 42
 - On-Premise **V** 42
 - Patriot Act **V** 69
 - Platform as a Service **V** 42
 - Private Cloud **V** 43
 - Pseudonymisierung **III** 28
 - Public Cloud **V** 44
 - Rechtsgrundlage **V** 60 ff.
 - Risikomanagement **V** 46
 - Skalierbarkeit **V** 38
 - Software as a Service **V** 42
 - Standardisierung **V** 35 ff.
 - Standardisierungsgrad **V** 37
 - Standardvertragsklauseln **V** 68
 - Subunternehmer **V** 45
 - Support **V** 45
 - Synchronisation **V** 41
 - Treuhänder-Modell **V** 70
 - Verschlüsselung **III** 28
 - Virtualisierung **V** 35
 - Zertifizierung **V** 57 f.
 - Zugriff von Sicherheitsbehörden **V** 68
 - Zwecke und Mittel **V** 48
 - Zweipersonenverhältnis **V** 48 ff.

Stichwortverzeichnis

- Cloud Computing Dienst V 34 ff., 308, 501
- Clubs V 365
- CNIL X 35
- Community Guidelines V 280
- Computer Emergency Response Team (CERT) V 492, 498
- Computergrundrecht II 38
- Computer Security Incident Response Teams (CSIRT) V 492
- Conditional Access V 560
- Connected Car II 36
- Consent-Banner
 - Ablehnungsmöglichkeit IV 97
 - alles Akzeptieren IV 98
 - Dropdown-Menü IV 99
 - Einstellungsverwaltung IV 97
 - farbliche Gestaltung der Schaltflächen IV 95
 - Gestaltungsvorschlägen IV 94
 - keine bedingungslose Aufwands-gleichheit IV 96
 - praktische Relevanz IV 94
 - Schaltflächen IV 98
 - Schieberegler IV 98
 - Zwecke, kurz und prägnant IV 99
- Content Moderation
 - Algorithmen V 458
- Conversion-Tracking V 109
- Cookie-Banner
 - Ablehnungsmöglichkeit IV 73
 - alle Akzeptieren IV 74
 - Bestätigung der Kästchen IV 74
 - Bestätigung der Schieberegler IV 74
 - Dropdown-Menü IV 68, 70
 - Einstellungsverwaltung IV 73
 - Extreme Farbgestaltungen IV 68
 - Farbhervorhebungen IV 66
 - Grafische Gestaltung IV 66
 - Größenunterschiede IV 66
 - irreführende Kennzeichnungen IV 73
 - Lenkungswirkung IV 67
 - Manipulation IV 67
 - Multilayer-Ansätze IV 68, 70
 - Unmissverständlich IV 73
 - Verlinkungen IV 91
- Costa/ENEL II 49
- Counter Speech V 624
- Credentials V 560
- Criteo X 35
- Crypto Shredding VI 269
- Customer Relationship Management V 52
- Customer Tracking V 107
- Cyberabwehr
 - Einwilligung V 485
- Darlehen X 44
- Data Act III 241 ff.
- Data Governance Act X 11
- Adressaten IV 46
- Authentifizierung IV 121
- Betrugsprävention IV 119
- Device Fingerprinting IV 54
- Einstellungen verwalten IV 71
- Endeinrichtung IV 47
- Fehleranalyse IV 119, 121
- First-Party-Cookie V 107
- First Party ~ I 42
- Funktions- oder Speicherdauer IV 90
- Gewährleistung von IT-Sicherheit IV 119, 121
- Hidden Identifiers IV 53
- irreführender Charakter IV 71
- Schnittstelle IV 47
- Smartphones IV 48
- Speichern und Auslesen von IV 51
- Spyware IV 53
- Third Party IV 52
- Third-Party-Cookie V 107
- Third Party ~ I 42
- Transparenz IV 79
- Web-Bugs IV 53
- Webserver IV 51
- weitere Informationen IV 71
- Zugriffsmöglichkeiten Dritter IV 116
- zusätzliche Hürde IV 71

- Data Protection by Design II 54
- Datenart VI 132, 185
- Datenbestand VI 131
- Datenbrille II 35
- Daten Dritter V 274
- Datengetriebene Dienste IV 12
- Datengetriebene Geschäftsmodelle IV 27
- Datenminimierung III 43 f., 92, V 18, 517, 631, VI 14 f., 144 ff.
- Datenobjekt VI 131
- Datenschutzaufsichtsbehörde IX 1 ff.
- Datenschutzausschuss II 4
- Datenschutzbeauftragter II 22
- Datenschutzbehörde X 2
- Datenschutz durch Technik VI 3, 10
- Datenschutzzerklärung II 20, IV 104, V 14, X 29
- Datenschutz-Folgenabschätzung III 229, VI 80
- Ausnahmen von der Durchführungspflicht VI 96
 - Beteiligte VI 113 ff.
 - Dokumentationspflicht VI 119
 - Durchführung VI 99
 - Durchführungspflicht VI 82
 - Einsatz KI-Technologie V 483
 - Konsultation der Aufsichtsbehörden VI 121 ff.
 - Negativliste VI 97
 - Phasen VI 112
 - Positivliste VI 84 f.
 - Risikomatrix VI 107
- Datenschutzfreundliche Voreinstellungen VI 10, 30
- Datenschutz-Grundrecht II 4 ff.
- Datenschutzgrundsätze V 631, VI 6
- Datenschutzgrundverordnung IV 3
- Datenschutzniveau III 250 ff.
- Datenschutzrichtlinie II 7
- Datenschutzvereinbarung III 258
- Datensicherung
- Löschen VI 202
- Datensparsamkeit II 22
- Datentreuhänder V 70, 307
- Datenübertragbarkeit V 319
- Datenverarbeitung II 9
- Datenverarbeitung durch KI-Systeme V 480
- Datenvermeidung und Datensparsamkeit V 631, VI 15 f.
- DDG V 442
- DDG-E
- Benehmen IX 28
- Deckungsabfragedienst V 588 ff.
- Deepfake II 35
- Definitionen der DS-GVO III 2
- Delegierte Verordnung (EU) 2018/389 V 578
- Deutsche Wohnen X 49
- Deutschland V 308
- Device-Fingerprinting IV 55
- aktive Methode IV 28
 - passive Methode IV 28
- Diagnosedaten V 325
- Dienste der Informationsgesellschaft II 64, 74 ff.
- Digital-Charta II 2
- Digitale Dienste II 69 ff., V 54, 501
- Alternativangebote IV 87
 - alternative Version IV 84
 - ausdrücklich wünschen IV 109
 - Suchmaschine V 102
 - unbedingt erforderlich IV 109
- Digitale-Dienste-Gesetz IV 30 f., V 253
- Digitale Produkte V 386
- Digitales Erbe
- Fernmeldegeheimnis III 6
 - Zugriff durch andere Berechtigte III 6
 - Zugriff durch Erben III 6
- Digital Services Act III 166, 241 ff., V 252
- Host-Provider-Privileg V 253
 - sehr große Online-Plattformen V 252
 - sehr große Online-Suchmaschinen V 252
- Diktiersystem V 323

Stichwortverzeichnis

- DIN 66398 VI 181 ff.
 - Anhänge VI 186
 - Nutzen der Norm VI 212
- DIN 66399 VI 271
- Direkterhebungsgebot V 558
- Direktwerbung V 137 ff.
- DMA IX 28
- DNS-Service I 26
- DNT V 90
- DoD-Schichtenmodell I 18
- Dokumentation III 201
 - Löschen VI 156
- Dokumentationspflichten V 354
- Dokumentieren III 201
- Domain-Name V 28
- Domain Name System
 - DENIC I 11
- DOSB V 358 f., 361
 - Aufnahmeordnung V 357
- Dringender Handlungsbedarf IX 26
- Dringlichkeitsverfahren IX 25
- Drittinteressen V 85
- Drittland III 202, 232 f., 248, V 316
- Drittlandübermittlung III 243
 - andere Form der Bereitstellung III 245
 - Bereitstellung personenbezogener Daten III 245
 - Fernzugriff III 245
 - Gesellschaftsrechtliche Herausgabeanprüche III 244
 - Gewährung von Zugriffsrechten III 245
 - Muttergesellschaft im ~ III 244
 - Onward Transfer III 249
 - Weiterübermittlung III 249
- Drittstaatentransfer X 31, 47
- Drittwirkung II 43
- DSA V 442, 450, IX 28
 - Digitale-Dienste-Gesetz V 443
- DS-GVO
 - Anwendungsbereich IV 33 ff.
- Echtzeitmarketing V 622
- E-Commerce-Richtlinie V 282
- E-Evidence-Verordnung
 - elektronische Beweismittel III 241 ff.
 - Europäische Herausgabeanordnung III 241 ff.
 - Europäische Sicherungsanordnung III 241 ff.
- EfA V 337
- EfA-Onlinedienst V 338 ff.
 - datenschutzrechtliche Verantwortlichkeit V 339
 - Kettenverantwortlichkeit V 339
 - Rechtsgrundlagen der Verarbeitung V 340
 - Verarbeitung personenbezogener Daten V 338
- E-Geld
 - PayPal V 580 ff.
- Eigenes Bild II 35 f.
- Eigentumsverhältnisse
 - des Endgeräts IV 59
- Einer-für-Alle V 337 ff.
- Einfache Sprache III 114 f.
- Eingrenzung
 - des persönlichen Anwendungsbereiches von § 25 TDDDG IV 58
- Ein-Platz-Prinzip V 359 ff.
- Einschränkung der Verarbeitung VI 173
 - beim Aussetzen der Regellöschung VI 243
- Einschränkung von Betroffenenrechten VII 93 ff.
 - Fallgestaltungen VII 94
- Einspruch V 312, IX 15, X 56
- Einspruchseinlegung IX 16
- Einstweilige Maßnahmen IX 25
- Einwilligung III 56 ff., 105 ff., 181, IV 62 ff., V 111 ff., 322, 390, 399 f., X 41
 - Abgrenzungsschwierigkeiten IV 56
 - Abhängigkeit III 121
 - AGB III 117
 - Altersverifizierung III 128
 - anerkannte Dienste zur Einwilligungsverwaltung III 144

- Anklicken **III** 137
- Arbeitsverhältnis **III** 121
- Auftragsverarbeiter **III** 116
- Ausnahme **V** 112 ff.
- Behinderung **III** 136
- bei Endeinrichtungen **IV** 60
- Beschäftigte **II** 61
- bestimmter Fall **IV** 79
- Bestimmtheitserfordernis **IV** 75 f.
- Cheating **V** 415
- Consent Management tools **III** 140
- Cookie Pop-Up **III** 142 ff.
- Dienste der Informationsgesellschaft **III** 128 f.
- Dienst zur Einwilligungsverwaltung **IV** 93
- Digital Markets Act **III** 145
- Dokumentation **III** 138 f.
- Empfänger der Daten **IV** 90
- Endnutzer **IV** 61
- Entscheidungsmacht **V** 151
- explizite Erklärung **IV** 65
- Form **III** 106, 125 f.
- Fortgeltung früherer **III** 134 f.
- freiwillig **IV** 82, **V** 431, 474
- Freiwilligkeit **III** 118 ff., **IV** 75
- gebündelte Zustimmung **IV** 81
- gezwungen **IV** 82
- Granularität der Zwecke **IV** 76
- Informiertheit **III** 115 f.
- Kinder **II** 64
- Kommunikationseffekt **IV** 69
- Koppelung **V** 431
- Layered Approach **III** 142
- mehrere Sachverhalte **III** 106
- mehrere Verantwortliche **III** 116
- Mehrstufige Einwilligung **III** 142
- Minderjährige **III** 96 ff., 126 ff.
- Mitnutzer **IV** 60
- nach § 25 TDDDG **IV** 80
- Nachteile **V** 227
- Nutzungsverhältnis **IV** 61
- Opt-In **III** 135 ff.
- pauschale Gesamteinwilligungen **IV** 84
- Pop-Up-Fenster **III** 143
- Prozess **III** 138
- Rechtsgeschäftlicher Wille **IV** 69
- Registrierungsprozess **V** 432
- separate Erklärung **IV** 79
- Torwächter **III** 145
- Touchscreen **III** 139 f.
- Ungleichgewicht **IV** 87
- Verarbeitungszweck **III** 110 f.
- Vertragsverhältnis **IV** 61
- Voraussetzungen **III** 109 ff.
- Wahlmöglichkeit **III** 123 f., **V** 426
- Winternutzung **V** 133
- Widerruf **III** 107, **IV** 82, **V** 151
- Widerrufsfolgen **III** 130 ff.
- Wirksamkeitsvoraussetzung **IV** 84, 92
- Zeitpunkt der Erteilung **IV** 63
- Zugriff und Preisgabe **IV** 56
- Zweckänderung **III** 113 f.
- Einwilligung bei Online-Partnervermittlungen
- Freiwilligkeit **V** 428
- Informiertheit **V** 428
- Koppelungsverbot **V** 428
- Transparenz **V** 428
- Einwilligungsbanner **IV** 131 f.
- Einwilligungserklärung
- Hervorrufen gezielter Verunsicherung **IV** 88
- repetitive identische Bitte **IV** 88
- Einwilligungsverwaltungsdienst **IV** 122 ff., 129 ff.
- anerkannte **IV** 122 ff.
- Einwilligungsbanner **IV** 124 ff.
- Funktionsweise **IV** 129
- Einwilligungsvorbehalt **V** 438
- Einzelbindungsnachweis **IV** 16 ff.
- Elektronischer Kommunikationsdienst **IV** 36, **V** 495, 539
- Elektronisches Kommunikationsnetz **V** 494
- Elektronische Verwaltungsleistung
- Verarbeitungsschritte und Rechtsgrundlagen **V** 353

Stichwortverzeichnis

- E-Mail II 26, 31 f.
 - Simple Mail Transfer Protocol (smtp) I 24
- Empfänger
 - Löschen im Einzelfall nach Information durch Dritte VI 154 f.
- Empfängerkategorien IV 103
- Empfehlungssystem V 273, 464 f.
- Endeinrichtung V 110 ff.
 - Alarmsystem IV 50
 - technologieneutral IV 48
 - Virtual Private Network IV 48
- Endgerät IV 36
- Endgültige Maßnahmen IX 25
 - Geltungsbereich IX 27
- Enforcement Tracker X 35
- Entgelt IV 15
 - Marktbeobachtung V 230
- Entscheidung
 - rechtliche Wirkung V 454
- Entscheidungskriterien V 457
- E-Privacy-Regulierung II 66 ff.
- E-Privacy-Richtlinie II 66 f., 69 ff., IV 1 ff., V 4
 - lex specialis II 71
 - sachlicher Anwendungsbereich II 71
- E-Privacy-RL II 48, 65
- E-Privacy-Verordnung II 67 ff., IV 3
 - Abgrenzung DS-GVO II 68
 - sachlicher Anwendungsbereich II 70
- E-Privacy-VO II 48
- Erforderlichkeit V 631, VI 144
 - Allgemeine Geschäftsbedingungen IV 114
 - objektiv unerlässlich V 161 f.
 - technisches Verständnis IV 113
 - Vertragsdurchführung V 161 f.
 - wirtschaftliche Notwendigkeit IV 114
- Erlaubnistatbestand V 151 f.
 - Rangfolge V 152
- Ermessen, pflichtgemäßes VIII 29
- Ermittlung der Identität
 - des Endnutzers IV 61
- Ermittlungsbefugnis der Aufsichtsbehörde X 4
- Ermittlungsbehörde II 34, 38 f.
- Erwartung II 63
- Erwgr. 32 DS-GVO IV 76
- ESBD V 358 f., 361
- eSport V 356 ff.
 - Account V 388 f., 391
 - Akteure V 360 ff.
 - allgemeines Persönlichkeitsrecht V 407
 - Auftragsverarbeiter V 391
 - Auftragsverarbeitung V 401
 - Auskunftsrecht V 402
 - Benutzername V 383
 - Betroffene V 375 f.
 - Cheating V 410 f.
 - Clans V 366
 - Clubs V 365
 - Datenschutz-Folgenabschätzung V 402
 - datenschutzrechtliche Rollenverteilung V 370 ff.
 - Datenverarbeitung V 371 f.
 - Disziplinen V 359
 - Erforderlichkeit Vertragserfüllung V 385
 - eSport-spezifische Datenverarbeitungen V 376 ff.
 - Gesundheitsdaten V 402
 - Internet V 359
 - Leistungsdaten V 402
 - Nickname V 383, 413
 - Recht am eigenen Bild V 407
 - Speicherbegrenzung V 416
 - Spielergebnisse V 388
 - Spitzname V 383, 413
 - Verantwortliche V 373 f.
 - Verbände V 361
- eSportler V 367
 - Account V 378 ff.
 - Arbeitnehmer V 367, 396
 - Auskunftsrecht V 417
 - berechtigtes Interesse V 414
 - Gesundheitsdaten V 398 ff.
 - Leistungsdaten V 398 ff.