

Datenschutz im Internet

Bearbeitet von
Herausgegeben von: Silke Jandt, und Dr. Roland Steidle, RA

1. Auflage 2018. Buch. 532 S. Gebunden
ISBN 978 3 8487 4856 3

[Recht > Handelsrecht, Wirtschaftsrecht > Telekommunikationsrecht, Postrecht, IT-Recht > Datenschutz, Postrecht](#)

schnell und portofrei erhältlich bei


DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beack-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Jandt | Steidle [Hrsg.]

Datenschutz im Internet

Rechtshandbuch zu DSGVO und BDSG



Nomos

NOMOSPRAXIS

Dr. habil. Silke Jandt,
Referatsteilleiterin LfD Niedersachsen, Hannover
Dr. Roland Steidle, Rechtsanwalt, Frankfurt a.M. [Hrsg.]

Datenschutz im Internet

Rechtshandbuch zu DSGVO und BDSG

Dr. Jens Ambrock, Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit | **Dr. Ubbo Aßmus,** Rechtsanwalt, Frankfurt a.M., Lehrbeauftragter an der Hochschule RheinMain | **Dr. Christian L. Geminn,** Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG), Universität Kassel | **Dr. Volker Hammer,** Consultant bei Secorvo, Karlsruhe | **Prof. Dr. Felix Hermonies, LL.M.,** Hochschule Darmstadt | **Dr. habil. Silke Jandt,** Referatsteilleiterin bei der Landesbeauftragten für den Datenschutz Niedersachsen, Privatdozentin Universität Kassel | **Dr. Moritz Karg,** Referent und Projektleiter, Digitale Agenda und zentrales IT Management, Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung des Landes Schleswig-Holstein | **Till Karsten, LL.M.,** Syndikus-Rechtsanwalt, Baden-Baden | **Henry Krasemann,** Referatsleiter beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, Jurafunk, Dozent an FH, WAK, Universität Kiel | **Dr. Philipp Richter,** Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz | **Annika Selzer,** Senior Researcher und Datenschutzrechtlerin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt | **Dr. Roland Steidle,** Fachanwalt für Informationstechnologierecht, Frankfurt a.M. | **Prof. Dr. Thomas Wilmer,** Hochschule Darmstadt



Nomos

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

ISBN 978-3-8487-4856-3

1. Auflage 2018

© Nomos Verlagsgesellschaft, Baden-Baden 2018. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten.

Zum Geleit

Obwohl das Internet aus dem Alltag jedes Unternehmens, jeder Behörde, jeder sonstigen Organisation oder sogar aus dem Leben jedes Bürgers und jeder Bürgerin in der Europäischen Union nicht mehr hinweg zu denken ist, hat die Datenschutz-Grundverordnung kein einziges der spezifischen Probleme des Datenschutzes im Internet angesprochen. Diese missverstandene Technikneutralität führt dazu, dass im Verordnungstext die Zulässigkeit der Verarbeitung personenbezogener Daten, die Grundsätze der Datenverarbeitung und die Rechte der betroffenen Personen ohne Unterschied danach geregelt werden, ob es sich etwa um eine harmlose Kundenliste einer Änderungsschneiderei oder um eine Vollerfassung aller Kontakte, Beziehungen, Präferenzen, Einstellungen und Kommunikationsakte im Rahmen eines Social Networks handelt.

Zwar erwähnt die Datenschutz-Grundverordnung auch Risiken für die Grundrechte und Freiheiten der betroffenen Person. Diese Bezugnahme auf Risiken beschränkt sich jedoch darauf, bestimmte Pflichten des Verantwortlichen „entsprechend der Risiken von Datenverarbeitungsprozessen“ zu reduzieren. Diese Einschränkung dürfte bewirken, dass nur ein Bruchteil der Verantwortlichen und Auftragsverarbeiter diese Pflichten erfüllen muss. Die Verordnung bestimmt jedoch nicht, was sie unter Risiko versteht und wie dieses festgestellt wird.

Da das Datenschutzrecht aber dazu dient, die Grundrechte und Freiheiten der jeweils betroffenen Personen zu schützen, muss im konkreten Fall immer festgestellt werden, welches Risiko von welchem Verantwortlichen beschränkt, reduziert oder vermieden werden muss und welche Rechte die betroffene Person hat, um ihre Risiken zu verringern. Für diese entscheidende Frage bietet die Datenschutz-Grundverordnung jedoch wenig Hilfestellung. Sie verursacht vielmehr für das Angebot und die Nutzung alltäglicher Internetdienste eine große Rechtsunsicherheit.

Diese Situation könnte durch die E-Privacy-Verordnung verbessert werden. Sie greift – zumindest nach den Entwürfen der Kommission und des Parlaments – spezifische Risiken der Datenverarbeitung in der elektronischen Kommunikation, des Trackings von betroffenen Personen und der Werbung im Internet auf. Diese risikoorientierten Regelungen betreffen aber nur Einzelfragen und können die weitgehende Rechtsunsicherheit des Datenschutzes im Internet nur bedingt beseitigen.

In dieser Situation ist es sehr verdienstvoll, dass das vorliegende Handbuch von den unterschiedlichen Dienstangeboten im Internet ausgehend die Rechtsfragen klärt, die die Datenschutz-Grundverordnung und die E-Privacy-Verordnung offenlassen. Sachkundig und risikoorientiert werden die abstrakten und unspezifischen Vorgaben untersucht, um Fragen zu Cloud Computing, zu Big Data, Web-Diensten, Suchalgorithmen, Social Networks sowie zu Datenschutz durch Systemgestaltung, technische Sicherheit sowie zu spezifischen Rechten der betroffenen Person zu beantworten. Damit bietet das Handbuch ein sicheres Fundament für diejenigen, die im Internet ihre Dienste anbieten, und für diejenigen, die sie nutzen und deren Daten im Internet verarbeitet und verwertet werden. Das Handbuch bietet somit eine wertvolle Unterstüt-

Zum Geleit

zung für die Beantwortung praktischer Fragen und für die dogmatische Durchdringung und Systematisierung des Internetdatenschutzrecht.

Kassel, Mai 2018

Alexander Roßnagel

Vorwort der Herausgeber

Am 25. Mai 2016 ist die europäische Datenschutz-Grundverordnung in Kraft getreten. Nach einer zweijährigen Übergangszeit ist sie seit dem 25. Mai 2018 europaweit vorrangig vor dem Datenschutzrecht der Mitgliedstaaten anzuwenden. Die Verordnung ist ein Meilenstein in der Entwicklung des europäischen Datenschutzrechts, das bislang auf der europäischen Datenschutz-Richtlinie aus dem Jahr 1995 basierte. Dem Erlass der Grundverordnung ging eine weit über ein Jahrzehnt dauernde politische und rechtliche Diskussion voraus. Dies verdeutlicht, wie verschieden die Interessen der Mitgliedstaaten aber auch der unterschiedlichen Interessenvertreter bezogen auf eine Datenschutzregulierung waren und sind. Nunmehr gilt jedenfalls ein weitgehend einheitliches europäisches Recht zum Schutz des Grundrechts auf Datenschutz, das die Charta der Grundrechte der Europäischen Union in Art. 8 schützt. Angesichts der bislang mit erheblichen Unterschieden in den Mitgliedstaaten umgesetzten Datenschutz-Richtlinie war dies ein längst überfälliger Schritt. Dies gilt insbesondere mit Blick auf das Internet und grenzüberschreitende Datenverarbeitungen, die wie kaum eine andere Materie im Datenschutzrecht harmonisierte und internationale Regelungen erfordern.

Eine Neuregelung war außerdem überfällig, um Antworten auf die neuen datenschutzrechtlichen Herausforderungen im Internet zu finden. Tatsächlich hat die heutige Realität der Informationstechnologie und der Datenverarbeitung im Internet nur noch wenig mit derjenigen aus dem Jahr 1995 gemein. Erheblich größere Bandbreiten ermöglichen eine performante und zugleich kostengünstige Übermittlung großer Datenvolumen. Dies hat zu zahlreichen neuen Diensten geführt, unter anderem zur Entwicklung von Streaming- und Mediendiensten, die früher so nicht denkbar waren. Die Standardisierung und Flexibilisierung von Speicher- und Infrastrukturleistungen hat eine „Vercloudung“ aller gängigen IT-Services, Internet- und Webangebote gefördert. Kaum mehr eine Anwendung ermöglicht es nicht, Inhalte über Cloud-Dienste und mobile Endgeräte zu verteilen und zu synchronisieren. Dies hat zu weltweit grenzüberschreitenden Verarbeitungen aller möglichen Daten geführt, die nur noch schwer nachvollziehbar, geschweige denn effektiv kontrollierbar sind. Die erheblich gestiegenen Datenmengen haben neue Branchen und Anbieter entstehen lassen, unter anderem im Bereich von Big Data und den damit einhergehenden Datenanalysen. Die daraus folgenden Risiken einer Diskriminierung einzelner Personen über Algorithmen, automatisierte Entscheidungen und statistische Ergebnisse, die – zumindest teilweise – ohne eine Verarbeitung personenbezogener Daten herbeigeführt werden, zwingen dazu, das Konzept des Personenbezugs zu hinterfragen, das bisher alleiniger Anknüpfungspunkt für die Geltung datenschutzrechtlicher Bestimmungen ist. Die Miniaturisierung von Prozessoren und Netzwerkkomponenten wird dazu führen, dass auch kleinste Alltagsgegenstände in absehbarer Zeit netzwerkfähig werden und mehr oder weniger über das Internet miteinander kommunizieren. Das Internet der Dinge wird einen weiteren Entwicklungssprung auf dem Weg zur Digitalisierung des Alltags darstellen. Es stellt sich die Frage, ob ein modernes Datenschutzrecht auch all diese nur flüchtigen und meist nicht längerfristig gespeicherten Daten erfassen soll.

Der Alltag würde dann nicht nur durch Datenverarbeitungen, sondern auch durch Datenschutzregelungen durchdrungen, deren Ursprung aus der Zeit der Großrechner und zentralen Datenverarbeitungen mit klar identifizierbaren Verantwortlichen stammt. Ob diese Datenschutzregelungen in einem künftigen Umfeld praktisch überhaupt noch anwendbar oder gar kontraproduktiv sind, ist diskussionswürdig. Dies betrifft etwa 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 wird das Verhältnis des Datenschutzrechts zur Meinungsfreiheit eine der großen Rechtsfragen der kommenden Jahre sein – nicht zuletzt wegen des Einflusses von Meinungen, Fakten oder „Fake News“ auf gesellschaftliche Entwicklungen und Wahlen. Letztlich zeigen sich die massiven Herausforderungen des Datenschutzrechts in einer digitalen Gesellschaft anhand vergangener und aktueller Datenschutzskandale, wie insbesondere den durch die Snowden Veröffentlichungen bekanntgewordenen Maßnahmen amerikanischer Geheimdienste, der Einflussnahme auf Wahlen über Social Networks und anhand intransparenter Datenverwertungen wie im Falle von Facebook und Cambridge Analytica.

Betrachtet man die europäische Datenschutz-Grundverordnung vor dem Hintergrund dieser Entwicklungen ist das Ergebnis freilich äußerst ernüchternd. Fast alle aktuellen und drängenden Fragen des Datenschutzrechts bleiben unbeantwortet. Meist werden sie nicht einmal in den Erwägungsgründen angesprochen. Die Verordnung übernimmt überwiegend das Bewährte und enthält nur wenige Neuerungen. Viele materiellrechtliche Regelungen der europäischen Datenschutz-Richtlinie aus 1995 wurden fast eins zu eins in die Verordnung geschrieben. Darüber hinaus enthält sie einige halbherzige Anpassungen, beispielsweise zur Auftragsverarbeitung und den Formerfordernissen, um klarzustellen, dass ein solcher Vertrag auch ohne die Verwendung von Papier abgeschlossen werden kann. Der große Innovationssprung ist ersichtlich nicht gelungen. Ergänzt wurde die Verordnung durch einen stark bürokratischen Ansatz mit insbesondere erheblichen Dokumentationspflichten, die viele kleine und mittlere Unternehmen überfordern und zudem in erster Linie Papier produzieren werden, aber keine aktuellen Datenschutzfragen lösen. Dazu treten zweifelhafte Haftungsregelungen und die Anforderung an Datenverarbeiter, sich zu rechtfertigen, wenn sie ihren – ebenfalls grundrechtlich geschützten – Gewerbebetrieb ausüben. Letztlich wird das Konzept einer selbstbestimmten Einwilligung durch ein strenges Kopplungsverbot begrenzt. 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.

Positiv hervorzuheben ist jedoch, dass es überhaupt gelungen ist, eine europaweite Regelung in Form einer Verordnung zu finden. Darauf muss in Zukunft aufgebaut werden, wenngleich die Innovationszyklen des europäischen Gesetzgebers nachdenklich stimmen. Schließlich wurde die europäische Datenschutz-Grundverordnung erst über zwanzig Jahre nach der europäischen Datenschutz-Richtlinie realisiert. Positiv

ist weiterhin, dass durch eine Verordnung zumindest versucht wurde, die schon in einzelnen Mitgliedstaaten nicht mehr überschaubare Zersplitterung des Datenschutzrechts zu beenden. Allerdings führen die zahlreichen Öffnungsklauseln, die dem europaweiten Harmonisierungsprozess geschuldet sind, nach wie vor dazu, dass es in allen Mitgliedstaaten eine Fülle spezifischer nationaler Datenschutzvorschriften geben kann. Voraussichtlich für einen längeren Zeitraum besteht zudem erst einmal eine unübersichtliche, vom europäischen Ordnungsgeber allein freilich nicht lösbare Parallelgeltung zwischen den Bestimmungen der Verordnung und dem nicht an diese angepassten Datenschutzrecht der Mitgliedstaaten. Dies führt zu neuen Abgrenzungsfragen und zu einer erheblichen Unsicherheit bei der Rechtsanwendung. Dazu treten in Deutschland gesetzgeberische Aktivitäten mit dem Ziel, das alte Datenschutzrecht in die Gegenwart hinüberzuretten. Dafür werden die Öffnungsklauseln der Verordnung denkbar weit ausgelegt, wenn nicht sogar europarechtswidrig überdehnt. Die ersten Versionen des neuen Bundesdatenschutzgesetzes lasen sich in Teilen wie eine Kopie seines Vorgängers. Dieses Ansinnen ist vor dem Hintergrund verständlich, dass dieselben Personen und Organisationen in Politik, Behörden und Unternehmen mit der Anwendung des neuen Datenschutzrechts betraut sind. Es verwundert daher nicht, dass einerseits politisch versucht wird, das hohe Datenschutzniveau in Deutschland zu erhalten, und dass andererseits selbst Unternehmen, die in der Vergangenheit einige Datenschutzregelungen kritisiert haben, angesichts der aktuellen Rechtsunsicherheit lieber auf festem Grund und nach bewährtem Konzept fortfahren möchten. Es steht allerdings zu erwarten, dass der Europäische Gerichtshof und der Europäische Datenschutzausschuss dem einen Riegel vorschieben werden. Der Preis der europaweiten Harmonisierung und notwendigen Internationalisierung ist auch im Datenschutzrecht, dass die Rechtsauslegung künftig nach europäischen Maßstäben zu beurteilen ist und nicht nach den Vorstellungen eines einzelnen Mitgliedstaats oder dessen Ländern.

Noch ungelöst, aber dem Prinzip einer Verordnung immanent, ist der Verlust an konkreten, vorhersehbaren Detailregelungen. Die damit erzeugte Rechtsunsicherheit dürfte noch auf Jahre bestehen bleiben. Kurzfristig ist weder mit Urteilen des Europäischen Gerichtshofs zu rechnen, noch mit konkretisierenden Empfehlungen und Leitlinien des Europäischen Datenschutzausschusses in größerem Umfang. Selbst die sehr zu begrüßenden Auslegungshilfen der Datenschutzkonferenz und einzelner deutscher Landesaufsichtsbehörden stehen unter dem Vorbehalt einer später abweichenden europäischen Rechtsauslegung. Aus Sicht der datenverarbeitenden Unternehmen ist es damit in vielen Bereichen der Informationstechnologie und der Internetnutzung praktisch unmöglich, sich gerichtsfest rechtskonform zu verhalten, insbesondere in innovativen Projekten. Angesichts des erheblich erweiterten Bußgeldrahmens zur Sanktionierung von – gegebenenfalls nicht eindeutig erkennbaren – Verstößen ist dies wirtschaftlich riskant. Für die Forschung und Entwicklung bleibt zu hoffen, dass Innovationen vor diesem Hintergrund nicht vermehrt in Drittländer und damit ohne direkte Einflussnahmemöglichkeit der europäischen Institutionen ausgelagert werden. Denn alle erfolgreichen Entwicklungen und Webangebote aus Drittländern, insbeson-

Vorwort der Herausgeber

dere den USA, haben bislang zu tatsächlichen Auswirkungen auch in der Europäischen Union geführt, allein aufgrund der großen Anzahl betroffener Nutzer.

Die nun anstehenden ersten Jahre mit der neuen Datenschutz-Grundverordnung werden daher äußerst spannend. Aus Sicht der datenverarbeitenden Anbieter von Internet- und Webdiensten ist es angesagt, „auf Sicht zu fahren“. Viele Bereiche sind „rechtliches Neuland“ und entweder in der Rechtspraxis unklar oder von der Verordnung gleich gar nicht erfasst. Dies betrifft auch die Auswirkungen der noch anstehenden E-Privacy-Verordnung sowie nationale Ergänzungen oder Konkretisierungen der europäischen Datenschutz-Grundverordnung. Insofern haben einzelne Auslegungsfragen auch dieses Handbuchs noch einen gewissen Prognosecharakter. Aus Sicht der Herausgeber und der Autoren bedeutet dies, dass sie die Rechtspraxis mit Blick auf Neuerungen und weitere Auflagen des Handbuchs laufend beobachten und dies in künftigen Auflagen berücksichtigen werden.

Gerade wegen der beschriebenen Herausforderungen sind allerdings Auslegungs- und Argumentationshilfen wichtig für die künftige 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 zu fast allen relevanten Bereichen des Datenschutzrechts im Internet. Die 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, Mai 2018

Silke Jandt und Roland Steidle

Inhaltsübersicht

Zum Geleit	5
Vorwort der Herausgeber	7
Verzeichnis der Autoren	33
Abkürzungsverzeichnis	35
Literaturverzeichnis	41
 Einleitung	 63
 A. Technische und rechtliche Grundlagen	 65
 I. Technische und strukturelle Grundlagen des Internet (<i>Silke Jandt</i>)	 65
1. Internet als technische Netzinfrastruktur	66
2. Internetdienste	70
3. Webdienste	73
4. Webtracking	76
5. Akteure des Internet	79
6. Geschäftsmodelle im Web	81
7. Zukunftsperspektiven	83
 II. Rechtliche Grundlagen	 84
1. Grundrechte der Europäischen Charta der Grundrechte und des Grundgesetzes (<i>Jens Ambrock</i>)	 85
a) Datenschutz	86
b) Vertraulichkeit der Kommunikation	93
c) Recht am eigenen Bild und gesprochenen Wort	97
d) Vertraulichkeit und Integrität informationstechnischer Systeme ...	98
e) Abwägung mit widerstreitenden Grundrechtspositionen	101
2. Anwendungsvorrang der europäischen Verordnungen (<i>Jens Ambrock</i>)	 102
a) Harmonisierung des europäischen Datenschutzrechts	102
b) Anwendungsvorrang des Unionsrechts	104
c) Normwiederholungsverbot	105
d) Öffnungsklauseln und deren Umsetzung	106
e) Unionsrechtswidrige nationale Abweichungen	112

Inhaltsübersicht

3. Datenschutz-Grundverordnung und E-Privacy-Regulierung (<i>Silke Jandt/Moritz Karg</i>)	114
a) Abgrenzung über den sachlichen Anwendungsbereich	116
b) Inhaltsdaten versus Nutzungs- und Verkehrsdaten	122
c) Rechtslage ab dem 25.5.2018 bis zum Erlass der E-Privacy- Verordnung	122
B. Internetspezifisches Datenschutzrecht	126
I. Begriffsbestimmungen (<i>Annika Selzer</i>)	126
1. Begriffsbestimmungen der Datenschutz-Grundverordnung	126
a) Personenbezogene Daten	126
b) Besondere Kategorien personenbezogener Daten	128
c) Verarbeitung und Einschränkung der Verarbeitung	129
d) Profiling	132
e) Pseudonymisierung	132
f) Dateisystem	133
g) Verantwortlicher und Auftragsverarbeiter	133
h) Empfänger und Dritter	135
i) Einwilligung	136
j) Verletzung des Schutzes personenbezogener Daten	138
k) Genetische, biometrische Daten und Gesundheitsdaten	138
l) Hauptniederlassung, Vertreter, Unternehmen und Unternehmensgruppe	140
m) Verbindliche interne Datenschutzvorschriften	142
n) Aufsichtsbehörde und betroffene Aufsichtsbehörde	142
o) Grenzüberschreitende Verarbeitung	143
p) Maßgeblicher und begründeter Einspruch	143
q) Dienst der Informationsgesellschaft	144
r) Internationale Organisation	145
2. Begriffsbestimmungen des Entwurfs einer E-Privacy-Verordnung	145
a) Elektronisches Kommunikationsnetz	145
b) Elektronischer Kommunikationsdienst	145
c) Interpersoneller Kommunikationsdienst	146
d) Endnutzer, Anruf und Endeinrichtung	147
e) Elektronische Kommunikationsdaten	147
f) Öffentlich zugängliches Verzeichnis	148
g) E-Mail	148
h) Direktwerbung und persönliche Direktwerbeanrufe	149
i) Automatische Anruf- und Kommunikationssysteme	149

II. Zulässigkeit der Verarbeitung personenbezogener Daten	149
1. Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DSGVO (<i>Thomas Wilmer</i>)	150
a) Verhältnis zu anderen Normen	150
b) Geltungsbereich	150
c) Einzelne Vorgaben	151
2. Rechtsgrundlagen der Verarbeitung in der Datenschutz-Grundverordnung	154
a) Rechtmäßige Verarbeitung gemäß Art. 6 DSGVO (<i>Thomas Wilmer</i>)	154
b) Datenverarbeitung aufgrund berechtigter Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO (<i>Philipp Richter</i>)	162
c) Anforderungen an die datenschutzrechtliche Einwilligung (<i>Thomas Wilmer</i>)	169
d) Datenverarbeitung besonderer Kategorien personenbezogener Daten (<i>Silke Jandt</i>)	177
e) Datenverarbeitung im Auftrag (<i>Henry Krasemann</i>)	191
3. Internationale Datenverarbeitung (<i>Ubbo Aßmus/Roland Steidle</i>)	204
a) Datenverarbeitung in der Europäischen Union	204
b) Übermittlung personenbezogener Daten in Drittländer	204
c) Anwendungsbereich	205
d) Zweistufige Zulässigkeitsprüfung	205
e) Besondere Anforderungen des 5. Kapitels der Datenschutz-Grundverordnung	206
4. Zulässigkeitsvorschriften oder Beschränkungen der E-Privacy-Regulierung (<i>Till Karsten</i>)	211
a) Entstehungsgeschichte der E-Privacy-Verordnung	211
b) Begriffsbestimmungen des Entwurfs der E-Privacy-Verordnung	214
c) Zulässigkeitsvorschriften und Verarbeitungsbeschränkungen	214
d) Einwilligung gemäß Art. 9 E-Privacy-VO-E	226
e) Beschränkungen nach Art. 11 E-Privacy-VO-E	228
5. Besondere Bedeutung des Schutzes der Informationen in Endeinrichtungen (<i>Moritz Karg</i>)	228
a) Vorläuferregelung des Art. 5 Abs. 3 E-Privacy-RL	228
b) Folgeregelung des Art. 8 E-Privacy-VO-E	232
III. Internetspezifische Datenverarbeitungen	236
1. Webdienste (<i>Henry Krasemann</i>)	236
a) Allgemeine Regelungen	237
b) Whois-Abfragen bei ICANN und DENIC	242
2. Cloud Computing-Dienste (<i>Roland Steidle</i>)	244
a) Eigenschaften von Cloud-Diensten	244

Inhaltsübersicht

b)	Gegenstand von Cloud-Diensten – „anything as a Service”	246
c)	Risiken der Private Cloud, Public Cloud und Hybrid Cloud	246
d)	Datenschutzrechtliche Anforderungen	247
e)	Entfernen des Personenbezugs durch Verschlüsselung?	253
f)	Cloud-Dienste mit Sitz im Drittland	255
g)	Zugriffe mit Auslandsbezug	255
h)	Zusammenfassung	257
3.	Office-Tools im Internet (<i>Henry Krasemann</i>)	257
a)	Auftragsverarbeitung	259
b)	Datenverarbeitung außerhalb der Europäischen Union	260
c)	Datenübertragbarkeit	261
d)	Verarbeitung besonderer Kategorien	262
4.	Suchmaschinen (<i>Moritz Karg</i>)	263
a)	Verarbeitung personenbezogener Daten durch Suchmaschinenanbieter	264
b)	Verantwortlichkeit	265
c)	Verarbeitung von Nutzungsdaten durch Suchmaschinenanbieter	266
d)	Verarbeitung von Inhaltsdaten durch Suchmaschinenbetreiber	268
5.	Webanalyse (<i>Moritz Karg</i>)	274
a)	Datenschutzrechtliche Verantwortlichkeit – Third-Party- Tracking	274
b)	Datenschutzrechtliche Betrachtung der Webanalyse und Rechtsgrundlagen	276
c)	Transparenz- und Informationspflichten	282
d)	Widerspruchsrecht	282
e)	Pflicht zur Pseudonymisierung	283
f)	Datenschutz-Folgenabschätzung	284
6.	Werbung (<i>Roland Steidle</i>)	284
a)	Bedeutung der Werbung	286
b)	Rechtsgrundlagen der Datenschutz-Grundverordnung	287
c)	Rechtsgrundlagen des Entwurfs der E-Privacy-Verordnung	292
d)	Wettbewerbsrechtliche Implikationen	293
e)	Einzelne Werbemaßnahmen	293
f)	Ausblick	296
7.	Social Networks (<i>Ubbo Aßmus</i>)	297
a)	Personenbezogene Daten in Social Networks	298
b)	Verantwortlichkeiten der Beteiligten	301
c)	Zulässigkeit der Datenverarbeitung durch den Anbieter	304
d)	Zulässigkeit der Datenverarbeitung durch den Nutzer	308
8.	Big Data (<i>Philipp Richter</i>)	309
b)	Big Data und statistische Datenverarbeitung	310
c)	Besondere Herausforderungen für den Datenschutz	312
d)	Big Data als Verarbeitung für berechnigte Interessen Art. 6 Abs. 1 S. 1 lit. f DSGVO	313

e) Interessenabwägung	313
f) Zweckbindung	314
g) Automatisierte Entscheidungen und Scoring	316
h) Amtliche Statistik	317
i) Zusammenfassende Bewertung	318
9. Kommunikations- und Over the Top-Dienste (<i>Ubbo Aßmus</i>)	318
a) Internationalität von OTT-Kommunikationsdiensten	320
b) Vertraulichkeit von Kommunikationsdaten	320
c) Verarbeitungstatbestände während des Kommunikationsvorganges	322
d) Löschungspflichten des Betreibers nach Ende des Kommunikationsvorganges	324
e) Schutz von in Endgeräten der Nutzer gespeicherten Daten	325
f) Umsetzung von Informationspflichten bei OTT-Diensten	325
10. Netz- und Informationssicherheit (<i>Roland Steidle</i>)	325
a) Hintergrund: Cybersicherheitsstrategie der Europäischen Union ..	326
b) Sicherheit der Verarbeitung nach Art. 32 DSGVO	327
c) Adressaten möglicher Maßnahmen	328
d) Risiken für die Netz- und Informationssicherheit	331
e) Datenverarbeitung gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO	332
f) Berechtigte Interessen zur Datenverarbeitung zwecks Abwehr von Risiken	333
g) Unbedingte Erforderlichkeit	336
h) Überwiegende Interessen der betroffenen Person	337
i) Grad der Zuverlässigkeit als Maßstab	337
j) Ausgewählter Maßnahmen	338
k) Zusammenspiel mit anderen Regelungen	339
l) Bedeutung des Erwgr. 49 für die künftige Rechtspraxis	340
11. Betrugsverhinderung, Auskunftfeien, vernünftige Erwartungen der Nutzer (<i>Roland Steidle</i>)	341
a) Grundsätzliches zu Erwgr. 47	341
b) Adressaten	342
c) Betrugsrisiken für Webdienste	343
d) Datenverarbeitung zur Betrugsverhinderung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO	344
e) Berechtigte Interessen und Einflussnahme auf die vernünftigen Erwartungen	345
f) Berechtigte Interessen zur Datenverarbeitung zwecks Betrugsverhinderung	347
g) Ausgewählte Maßnahmen zur Verhinderung von Betrug im Internet	354
h) Zusammenspiel mit anderen bereichsspezifischen Datenschutzvorschriften	355
i) Ausblick	356

Inhaltsübersicht

IV. Technischer und organisatorischer Datenschutz	356
1. Datenschutz durch Technik und datenschutzfreundliche Voreinstellung (<i>Philipp Richter</i>)	356
a) Datenschutz durch Technik	356
b) Datenschutzprinzipien gemäß Art. 5 DSGVO	357
c) Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen	358
d) Sicherheit der Verarbeitung	365
e) Zertifizierung	368
f) Sanktionen und Haftung im Bereich Datenschutz durch Technik	373
g) Verhältnis zu Art. 24 DSGVO	374
2. Datenschutz-Folgenabschätzung (<i>Annika Selzer</i>)	374
a) Durchführungspflicht	375
b) Ausnahmen von der Durchführungspflicht	380
c) Durchführung der Datenschutz-Folgenabschätzung	381
d) Vorherige Konsultation der Aufsichtsbehörde	389
3. Informationspflichten (<i>Annika Selzer</i>)	390
a) Informationspflichten bei Direkterhebung	391
b) Informationspflichten bei Dritterhebung	398
c) Informationspflichten bei in Verkehr bringen von elektronische Kommunikation erlaubender Software	403
d) Informationspflichten bei öffentlich zugänglichen Verzeichnissen mit Suchfunktion	405
e) Informationspflichten über erkannte Sicherheitsrisiken bei elektronischen Kommunikationsdiensten	406
4. Technische Umsetzung von Löschpflichten bei Providern (<i>Volker Hammer</i>)	406
a) Löschen? Löschen. Löschen!	407
b) Überblick über Vorgaben zum Löschen in der Datenschutz-Grundverordnung	411
c) Rechtliche Vorgaben für das Löschen aus anderen Vorschriften	414
d) Rahmenbedingungen für ein Löschkonzept	415
e) DIN 66398 – ein Vorschlag zum Aufbau und zur Umsetzung von Löschkonzepten	420
f) Anwendung der DIN 66398	430
g) Technische Aspekte von Löschen und Anonymisieren	433
h) Kontrolle über Inhalte – auch im Internet	441
V. Rechte der Betroffenen (<i>Felix Hermonies</i>)	443
1. Auskunftsrecht	443
a) Grundlagen	443

b) Verfahren	444
c) Identifizierung	445
2. Berichtigungsrecht	446
3. Löschungsrecht und „Recht auf Vergessenwerden“	447
a) Löschungsrecht	447
b) „Recht auf Vergessenwerden“	448
c) Ausnahmen des Löschungsrechts	450
4. Recht auf Einschränkung der Verarbeitung	451
5. Mitteilungspflicht und Unterrichtsrecht	452
6. Recht auf Datenübertragbarkeit	453
7. Widerspruchsrecht	456
8. Verbot automatisierter Entscheidungen im Einzelfall einschließlich Profiling	456
9. Einschränkung von Betroffenenrechten	458
VI. Rechtsschutz für Betroffene (<i>Christian Geminn</i>)	458
1. Recht auf Beschwerde bei der Aufsichtsbehörde	459
a) Geltendmachung des Beschwerderechts	460
b) Pflichten der Aufsichtsbehörden	465
c) Zusammenfassung	469
2. Haftung und Recht auf Schadensersatz	470
a) Anspruchsberechtigte	471
b) Anspruchsgegner und Haftung	471
c) Verstoß	472
d) Schaden	473
e) Haftungsbefreiung	474
f) Zusammenfassung	475
3. Gerichtliche Durchsetzbarkeit	475
a) Gerichtlicher Rechtsbehelf gegen eine Aufsichtsbehörde	476
b) Gerichtlicher Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	480
c) Parallele Verfahren	482
d) Die Rolle des Europäischen Gerichtshofs	484
e) Zusammenfassung	486
4. Vertretung von betroffenen Personen, Verbandsbeschwerde und Verbandsklage	486
5. Rechtsschutz nach der Datenschutz-Grundverordnung	488
VII. Sanktionen (<i>Jens Ambrock</i>)	489
1. Verwaltungsrechtliche Sanktionen und Anordnungen	490
a) Aufgaben der Aufsichtsbehörden	490
b) Untersuchungsbefugnisse der Aufsichtsbehörden	490

Inhaltsübersicht

c) Zuständigkeit der Aufsichtsbehörden	492
2. Verwaltungsrechtliche Sanktionen und Anordnungen	495
a) Anordnungsbefugnisse	495
b) Rechtsschutz	499
3. Ordnungswidrigkeitsrechtliche Sanktionen	500
a) Bußgeldtatbestände	501
b) Bußgeldverfahren	503
c) Rechtsschutz	507
4. Strafrechtliche Sanktionen	508
5. Wettbewerbsrechtliche Sanktionen	509
6. Verbraucherschutzrechtliche Verbandsklage	509
Stichwortverzeichnis	511

Inhaltsverzeichnis

Zum Geleit	5
Vorwort der Herausgeber	7
Verzeichnis der Autoren	33
Abkürzungsverzeichnis	35
Literaturverzeichnis	41
 Einleitung	 63
 A. Technische und rechtliche Grundlagen	 65
I. Technische und strukturelle Grundlagen des Internet	65
1. Internet als technische Netzinfrastruktur	66
2. Internetdienste	70
3. Webdienste	73
4. Webtracking	76
5. Akteure des Internet	79
6. Geschäftsmodelle im Web	81
7. Zukunftsperspektiven	83
 II. Rechtliche Grundlagen	 84
1. Grundrechte der Europäischen Charta der Grundrechte und des Grundgesetzes	 85
a) Datenschutz	86
aa) Schutz personenbezogener Daten gemäß Art. 8 Abs. 1 GRCh	 87
(1) Konkretisierung durch das Sekundärrecht	87
(2) Schutzbereich	87
(3) Schranken	89
bb) Recht auf informationelle Selbstbestimmung	90
(1) Schutzbereich	91
(2) Schranken	92
b) Vertraulichkeit der Kommunikation	93
aa) Recht auf Achtung der Kommunikation gemäß Art. 7 Var. 4 GRCh	 93
(1) Schutzbereich	94
(2) Schranken	94
bb) Fernmeldegeheimnis gemäß Art. 10 Abs. 1 Var. 3 GG	95
(1) Schutzbereich	95

Inhaltsverzeichnis

(2) Schranken	96
c) Recht am eigenen Bild und gesprochenen Wort	97
d) Vertraulichkeit und Integrität informationstechnischer Systeme ...	98
aa) Herleitung	98
bb) Schutzbereich	99
cc) Schranken	101
e) Abwägung mit widerstreitenden Grundrechtspositionen	101
2. Anwendungsvorrang der europäischen Verordnungen	102
a) Harmonisierung des europäischen Datenschutzrechts	102
b) Anwendungsvorrang des Unionsrechts	104
c) Normwiederholungsverbot	105
d) Öffnungsklauseln und deren Umsetzung	106
aa) Zwingende Regelungsaufträge	107
bb) Regelungsoptionen zur Beschränkung oder Abweichung	108
cc) Regelungsoption zur Verstärkung des Datenschutzes	111
dd) Regelungsoptionen zur Konkretisierung und Präzisierung	112
e) Unionsrechtswidrige nationale Abweichungen	112
aa) Beispiele abweichender nationaler Gesetzgebung	112
bb) Folgen abweichender nationaler Gesetzgebung	114
3. Datenschutz-Grundverordnung und E-Privacy-Regulierung	114
a) Abgrenzung über den sachlichen Anwendungsbereich	116
aa) Kommunikationsnetze	117
bb) Kommunikationsdienste	117
cc) Merkmal der Zugänglichkeit des Dienstes	120
b) Inhaltsdaten versus Nutzungs- und Verkehrsdaten	122
c) Rechtslage ab dem 25.5.2018 bis zum Erlass der E-Privacy- Verordnung	122
B. Internetspezifisches Datenschutzrecht	126
I. Begriffsbestimmungen	126
1. Begriffsbestimmungen der Datenschutz-Grundverordnung	126
a) Personenbezogene Daten	126
b) Besondere Kategorien personenbezogener Daten	128
c) Verarbeitung und Einschränkung der Verarbeitung	129
d) Profiling	132
e) Pseudonymisierung	132
f) Dateisystem	133
g) Verantwortlicher und Auftragsverarbeiter	133
h) Empfänger und Dritter	135
i) Einwilligung	136
j) Verletzung des Schutzes personenbezogener Daten	138
k) Genetische, biometrische Daten und Gesundheitsdaten	138

l) Hauptniederlassung, Vertreter, Unternehmen und Unternehmensgruppe	140
m) Verbindliche interne Datenschutzvorschriften	142
n) Aufsichtsbehörde und betroffene Aufsichtsbehörde	142
o) Grenzüberschreitende Verarbeitung	143
p) Maßgeblicher und begründeter Einspruch	143
q) Dienst der Informationsgesellschaft	144
r) Internationale Organisation	145
2. Begriffsbestimmungen des Entwurfs einer E-Privacy-Verordnung	145
a) Elektronisches Kommunikationsnetz	145
b) Elektronischer Kommunikationsdienst	145
c) Interpersoneller Kommunikationsdienst	146
d) Endnutzer, Anruf und Endeinrichtung	147
e) Elektronische Kommunikationsdaten	147
f) Öffentlich zugängliches Verzeichnis	148
g) E-Mail	148
h) Direktwerbung und persönliche Direktwerbeanrufe	149
i) Automatische Anruf- und Kommunikationssysteme	149
II. Zulässigkeit der Verarbeitung personenbezogener Daten	149
1. Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DSGVO	150
a) Verhältnis zu anderen Normen	150
b) Geltungsbereich	150
c) Einzelne Vorgaben	151
aa) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	151
bb) Zweckbindungsgrundsatz	151
cc) Datenminimierung	152
dd) Richtigkeit	152
ee) Speicherbegrenzung	153
ff) Integrität und Vertraulichkeit	153
gg) Rechenschaftspflicht	153
2. Rechtsgrundlagen der Verarbeitung in der Datenschutz-Grundverordnung	154
a) Rechtmäßige Verarbeitung gemäß Art. 6 DSGVO	154
aa) Geltungsbereich und Zweck	154
bb) Ausnahmen	154
cc) Einzelne Rechtsgrundlagen	155
(1) Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO	155
(2) Vertragserfüllung nach Art. 6 Abs. 1 S. 1 lit. b DSGVO ...	156
(3) Rechtliche Verpflichtung nach Art. 6 Abs. 1 S. 1 lit. c DSGVO	157

Inhaltsverzeichnis

(4) Lebenswichtige Interessen nach Art. 6 Abs. 1 S. 1 lit. d DSGVO	157
(5) Öffentliche Interessen nach Art. 6 Abs. 1 S. 1 lit. e DSGVO	158
dd) Öffnungsklausel nach Art. 6 Abs. 2 DSGVO	158
ee) Rechtsgrundlagen für den öffentlichen Bereich gemäß Art. 6 Abs. 3 DSGVO	159
ff) Verarbeitung zu anderen Zwecken nach Art. 6 Abs. 4 DSGVO	159
(1) Zweckverbindung und Weiterverarbeitungszwecke	160
(2) Erhebungszusammenhang	161
(3) Art der personenbezogenen Daten	161
(4) Folgen der beabsichtigten Weiterverarbeitung	161
(5) Vorhandensein geeigneter Garantien	162
b) Datenverarbeitung aufgrund berechtigter Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO	162
aa) Normgenese, Systematik und Funktion von Art. 6 Abs. 1 S. 1 lit. f DSGVO	162
bb) Berechtigte Interessen	164
cc) Datenminimierung	165
dd) Interessen der betroffenen Personen	165
ee) Interessenabwägung	166
ff) Betroffenenrechte bei einer Verarbeitung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO	168
gg) Verhältnis von Art. 6 Abs. 1 S. 1 lit. f DSGVO zu anderen Normen	168
c) Anforderungen an die datenschutzrechtliche Einwilligung	169
aa) Allgemeine Voraussetzungen der Einwilligung	169
(1) Zweckbezug	169
(2) Informiertheit und Verständlichkeit	170
(3) Freiwilligkeit	171
(4) Nachweisbarkeit	171
(5) Kopplungsverbot	171
(6) Besonderheiten im Beschäftigungsverhältnis	172
(7) Besonderheiten gemäß Art. 8 DSGVO	173
(8) Widerruflichkeit ohne Nachteile	174
bb) Fortgeltung früherer Einwilligungen	175
cc) Technischer Einwilligungsprozess	175
(1) Mögliche technische Formen des Opt-In im elektronischen Verkehr	176
(2) Anforderungen an die Darstellung	176
d) Datenverarbeitung besonderer Kategorien personenbezogener Daten	177
aa) Besondere Kategorien personenbezogener Daten im „Internet“	178

bb)	Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten	182
cc)	Weitere datenschutzrechtliche Anforderungen	187
dd)	Regelungen im Bundesdatenschutzgesetz	187
e)	Datenverarbeitung im Auftrag	191
aa)	Voraussetzungen	193
	(1) Vertrag oder anderes Rechtsinstrument	194
	(2) Konkrete Beschreibung der Verarbeitung	194
bb)	Typische Fälle von Auftragsverarbeitung	199
	(1) Hosting	199
	(2) Cloud Computing	199
	(3) Tracking- und Analyse-Dienste	200
	(4) Firewall	200
	(5) Datenträgervernichtung	200
cc)	Streitfälle	200
dd)	Änderungsbedarf für Alt-Verträge nach der Datenschutz- Grundverordnung	202
ee)	Garantie durch genehmigte Verhaltensregeln oder Zertifizierung	203
ff)	Auftragnehmer im Ausland	203
gg)	Folgen bei Verstößen	204
3.	Internationale Datenverarbeitung	204
a)	Datenverarbeitung in der Europäischen Union	204
b)	Übermittlung personenbezogener Daten in Drittländer	204
c)	Anwendungsbereich	205
d)	Zweistufige Zulässigkeitsprüfung	205
e)	Besondere Anforderungen des 5. Kapitels der Datenschutz- Grundverordnung	206
aa)	Angemessenheitsbeschlüsse der Kommission	206
bb)	EU-US Privacy Shield	207
cc)	Geeignete Garantien und wirksamer Rechtsschutz	208
dd)	Nach Unionsrecht nicht zulässige Übermittlung oder Offenlegung	209
ee)	Ausnahmen für bestimmte Fälle inklusive Einwilligung der betroffenen Person	210
ff)	Anforderungen nach der E-Privacy-Verordnung	211
4.	Zulässigkeitsvorschriften oder Beschränkungen der E-Privacy- Regulierung	211
a)	Entstehungsgeschichte der E-Privacy-Verordnung	211
b)	Begriffsbestimmungen des Entwurfs der E-Privacy-Verordnung ...	214
c)	Zulässigkeitsvorschriften und Verarbeitungsbeschränkungen	214
aa)	Vertraulichkeit elektronischer Kommunikation gemäß Art. 5 E-Privacy-VO-E	214

Inhaltsverzeichnis

bb)	Verarbeitung elektronischer Kommunikationsdaten nach Artikel 6 E-Privacy-VO-E	215
(1)	Elektronische Kommunikationsdaten nach Art. 6 Abs. 1 E-Privacy-VO-E	215
(2)	Elektronischer Kommunikationsmetadaten nach Art. 6 Abs. 2 E-Privacy-VO-E	217
(3)	Elektronische Kommunikationsinhalte nach Art. 6 Abs. 3 E-Privacy-VO-E	220
cc)	Speicherung und Löschung elektronischer Kommunikationsdaten nach Art. 7 E-Privacy-VO-E	220
dd)	Schutz von Endeinrichtungen nach Art. 8 E-Privacy-VO-E ...	221
(1)	Erhebung von Informationen aus Endeinrichtungen nach Art. 8 Abs. 1 E-Privacy-VO-E	222
(2)	Erhebung von Informationen von Endeinrichtungen nach Art. 8 Abs. 2 E-Privacy-VO-E	225
(3)	Standardisierte Bildsymbole nach Art. 8 Abs. 3 E-Privacy-VO-E	226
d)	Einwilligung gemäß Art. 9 E-Privacy-VO-E	226
e)	Beschränkungen nach Art. 11 E-Privacy-VO-E	228
5.	Besondere Bedeutung des Schutzes der Informationen in Endeinrichtungen	228
a)	Vorläuferregelung des Art. 5 Abs. 3 E-Privacy-RL	228
aa)	Technologische Implikation des Art. 5 Abs. 3 E-Privacy-RL	229
bb)	Rechtliche Implikation des Art. 5 Abs. 3 E-Privacy-RL	230
b)	Folgerregelung des Art. 8 E-Privacy-VO-E	232
aa)	Technologische Implikationen des Art. 8 E-Privacy-VO-Entwurf	232
bb)	Rechtliche Implikationen bezüglich des Schutzes der Endeinrichtung	233
cc)	Rechtliche Implikationen für das Offline-Tracking	235
III.	Internetspezifische Datenverarbeitungen	236
1.	Webdienste	236
a)	Allgemeine Regelungen	237
aa)	Rechtsgrundlage	237
bb)	Datenschutzrechtliche Verantwortlichkeit	239
cc)	Datenschutzerklärung	240
dd)	Datenminimierung	240
ee)	Technisch-organisatorische Maßnahmen	241
b)	Whois-Abfragen bei ICANN und DENIC	242
2.	Cloud Computing-Dienste	244
a)	Eigenschaften von Cloud-Diensten	244
b)	Gegenstand von Cloud-Diensten – „anything as a Service“	246

c)	Risiken der Private Cloud, Public Cloud und Hybrid Cloud	246
d)	Datenschutzrechtliche Anforderungen	247
aa)	Anforderungen an Cloud-Dienste im Zweipersonenverhältnis	248
bb)	Anforderungen an Cloud-Dienste im Dreipersonenverhältnis	249
cc)	Erfüllung der Anforderungen durch Cloud-Zertifizierung	250
dd)	Anforderungen an Cloud-Nutzer im Dreipersonenverhältnis	251
e)	Entfernen des Personenbezugs durch Verschlüsselung?	253
f)	Cloud-Dienste mit Sitz im Drittland	255
g)	Zugriffe mit Auslandsbezug	255
h)	Zusammenfassung	257
3.	Office-Tools im Internet	257
a)	Auftragsverarbeitung	259
b)	Datenverarbeitung außerhalb der Europäischen Union	260
c)	Datenübertragbarkeit	261
d)	Verarbeitung besonderer Kategorien	262
4.	Suchmaschinen	263
a)	Verarbeitung personenbezogener Daten durch Suchmaschinenanbieter	264
b)	Verantwortlichkeit	265
c)	Verarbeitung von Nutzungsdaten durch Suchmaschinenanbieter	266
d)	Verarbeitung von Inhaltsdaten durch Suchmaschinenbetreiber	268
aa)	Berechtigtes Interesse bei Suchmaschinenbetreibern und der Nutzer der Suchmaschine	269
bb)	Verallgemeinerte Abwägung der Interessen und Grundrechte der betroffenen Person	270
cc)	Verarbeitung besonderer Kategorien personenbezogener Daten	271
dd)	Recht auf Widerspruch	272
5.	Webanalyse	274
a)	Datenschutzrechtliche Verantwortlichkeit – Third-Party- Tracking	274
aa)	First-Party-Anbieter und Auftragsverarbeitung	275
bb)	Gemeinsame Verantwortlichkeit bei der Webanalyse	275
b)	Datenschutzrechtliche Betrachtung der Webanalyse und Rechtsgrundlagen	276
aa)	Mustererkennung und Profiling	276
bb)	Rechtsgrundlage für Webanalyse nach Datenschutz- Grundverordnung	277
cc)	Interessenausgleich gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO ...	279
(1)	Berechtigte Interessen bei der Webanalyse	279
(2)	Beachtung der schutzwürdigen Interessen	280

Inhaltsverzeichnis

c)	Transparenz- und Informationspflichten	282
d)	Widerspruchsrecht	282
e)	Pflicht zur Pseudonymisierung	283
f)	Datenschutz-Folgenabschätzung	284
6.	Werbung	284
a)	Bedeutung der Werbung	286
b)	Rechtsgrundlagen der Datenschutz-Grundverordnung	287
aa)	Einwilligung und Vertragserfüllung nach Art. 6 Abs. 1 S. 1 lit. a und b DSGVO	287
bb)	Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO	289
cc)	Zweckänderung nach Art. 6 Abs. 4 DSGVO	291
c)	Rechtsgrundlagen des Entwurfs der E-Privacy-Verordnung	292
d)	Wettbewerbsrechtliche Implikationen	293
e)	Einzelne Werbemaßnahmen	293
aa)	Direktwerbung	293
bb)	Nicht-personalisierte Werbung, Banner- und Videowerbung	294
cc)	E-Mail, Personal Messages, SMS	294
dd)	Werbeanrufe	295
ee)	Kundenbindungs- und Bonuspunktesysteme, Empfehlungsmarketing	295
f)	Ausblick	296
7.	Social Networks	297
a)	Personenbezogene Daten in Social Networks	298
b)	Verantwortlichkeiten der Beteiligten	301
c)	Zulässigkeit der Datenverarbeitung durch den Anbieter	304
d)	Zulässigkeit der Datenverarbeitung durch den Nutzer	308
8.	Big Data	309
b)	Big Data und statistische Datenverarbeitung	310
c)	Besondere Herausforderungen für den Datenschutz	312
d)	Big Data als Verarbeitung für berechtigte Interessen Art. 6 Abs. 1 S. 1 lit. f DSGVO	313
e)	Interessenabwägung	313
f)	Zweckbindung	314
aa)	Statistische Zwecke	315
bb)	Vereinbarkeit nach Art. 6 Abs. 4 DSGVO	316
g)	Automatisierte Entscheidungen und Scoring	316
h)	Amtliche Statistik	317
i)	Zusammenfassende Bewertung	318
9.	Kommunikations- und Over the Top-Dienste	318
a)	Internationalität von OTT-Kommunikationsdiensten	320
b)	Vertraulichkeit von Kommunikationsdaten	320
c)	Verarbeitungstatbestände während des Kommunikationsvorganges	322

d) Löschungspflichten des Betreibers nach Ende des Kommunikationsvorgangs	324
e) Schutz von in Endgeräten der Nutzer gespeicherten Daten	325
f) Umsetzung von Informationspflichten bei OTT-Diensten	325
10. Netz- und Informationssicherheit	325
a) Hintergrund: Cybersicherheitsstrategie der Europäischen Union ..	326
b) Sicherheit der Verarbeitung nach Art. 32 DSGVO	327
c) Adressaten möglicher Maßnahmen	328
d) Risiken für die Netz- und Informationssicherheit	331
e) Datenverarbeitung gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO	332
f) Berechtigte Interessen zur Datenverarbeitung zwecks Abwehr von Risiken	333
aa) Präventive Maßnahmen und Tests	333
bb) Zutritts-, Zugangs- und Zugriffskontrolle	334
cc) Protokollieren von IP-Adressen	334
dd) Verhinderung der Verbreitung von Malware und Spam	335
ee) Nur potenziell gefährliche E-Mails und Attachments	336
g) Unbedingte Erforderlichkeit	336
h) Überwiegende Interessen der betroffenen Person	337
i) Grad der Zuverlässigkeit als Maßstab	337
j) Ausgewählter Maßnahmen	338
k) Zusammenspiel mit anderen Regelungen	339
l) Bedeutung des Erwgr. 49 für die künftige Rechtspraxis	340
11. Betrugsverhinderung, Auskunftfeien, vernünftige Erwartungen der Nutzer	341
a) Grundsätzliches zu Erwgr. 47	341
b) Adressaten	342
c) Betrugsrisiken für Webdienste	343
d) Datenverarbeitung zur Betrugsverhinderung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO	344
e) Berechtigte Interessen und Einflussnahme auf die vernünftigen Erwartungen	345
f) Berechtigte Interessen zur Datenverarbeitung zwecks Betrugsverhinderung	347
aa) Datenverarbeitung bei Auskunftfeien inklusive Scoring	347
bb) Geoscoring	349
cc) Pooling	349
dd) Verwendung von Positivdaten	350
ee) Anreichern mit Daten aus öffentlichen Quellen	351
ff) Verhinderung von Identitätsdiebstahl und -betrug mittels Geräte-ID, 2-Faktor-Authentifizierung und PKI	351
gg) Zugriffsprotokolle	354
g) Ausgewählte Maßnahmen zur Verhinderung von Betrug im Internet	354

Inhaltsverzeichnis

h) Zusammenspiel mit anderen bereichsspezifischen Datenschutzvorschriften	355
i) Ausblick	356
IV. Technischer und organisatorischer Datenschutz	356
1. Datenschutz durch Technik und datenschutzfreundliche Voreinstellung	356
a) Datenschutz durch Technik	356
b) Datenschutzprinzipien gemäß Art. 5 DSGVO	357
c) Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen	358
aa) Art. 25 Abs. 1 DSGVO	358
bb) Art. 25 Abs. 2 DSGVO	364
cc) Art. 25 Abs. 3 DSGVO	365
d) Sicherheit der Verarbeitung	365
aa) Art. 32 Abs. 1 und 2 DSGVO	365
bb) Art. 32 Abs. 3 DSGVO	368
cc) Art. 32 Abs. 4 DSGVO	368
e) Zertifizierung	368
aa) Zertifizierung, Freiwilligkeit, Dynamik der Zertifizierung	369
bb) Festlegung von Zertifizierungsverfahren, Prüfzeichen und Siegeln	370
cc) Zertifizierungsstellen	371
dd) Zuständigkeit für die Zertifizierung	371
ee) Ablauf der Zertifizierung	372
f) Sanktionen und Haftung im Bereich Datenschutz durch Technik	373
g) Verhältnis zu Art. 24 DSGVO	374
2. Datenschutz-Folgenabschätzung	374
a) Durchführungspflicht	375
aa) Hohes Risiko als Bewertungskriterium	376
bb) Positivliste der Aufsichtsbehörde	376
cc) Bewertung des hohen Risikos	376
dd) Zweistufige Risikobewertung	378
ee) Konsequenzen der Durchführungsentscheidung	380
b) Ausnahmen von der Durchführungspflicht	380
aa) Negativliste der Aufsichtsbehörde	380
bb) Keine Datenschutz-Folgenabschätzung aufgrund spezieller Rechtsgrundlage	380
c) Durchführung der Datenschutz-Folgenabschätzung	381
aa) Inhalte der Datenschutz-Folgenabschätzung	381
(1) Beschreibung der geplanten Verarbeitungsvorgänge	381
(2) Bewertung der Notwendigkeit der Verarbeitungsvorgänge	382

(3) Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen	383
(4) Beschreibung der Abhilfemaßnahmen zur Bewältigung der Risiken	385
bb) Phasen der Datenschutz-Folgenabschätzung	386
cc) An der Datenschutz-Folgenabschätzung zu Beteiligende	387
(1) Beteiligung des Datenschutzbeauftragten	387
(2) Beteiligung von Auftragsverarbeitern	387
(3) Einholung der Standpunkte der betroffenen Personen	387
dd) Dokumentationspflicht	389
ee) Kumulierte Datenschutz-Folgenabschätzung	389
d) Vorherige Konsultation der Aufsichtsbehörde	389
3. Informationspflichten	390
a) Informationspflichten bei Direkterhebung	391
aa) Inhalt der Informationspflicht	392
bb) Zeitpunkt der Informationspflicht	395
cc) Weitere Anforderungen an die Informationen	396
dd) Weiterverarbeitung für andere Zwecke	397
ee) Ausnahmen von der Informationspflicht	397
b) Informationspflichten bei Dritterhebung	398
aa) Inhalt der Informationspflicht	399
bb) Zeitpunkt der Informationspflicht	401
cc) Weitere Anforderungen an die Informationen	402
dd) Weiterverarbeitung für andere Zwecke	402
ee) Ausnahmen von der Informationspflicht	402
c) Informationspflichten bei in Verkehr bringen von elektronische Kommunikation erlaubender Software	403
d) Informationspflichten bei öffentlich zugänglichen Verzeichnissen mit Suchfunktion	405
e) Informationspflichten über erkannte Sicherheitsrisiken bei elektronischen Kommunikationsdiensten	406
4. Technische Umsetzung von Löschpflichten bei Providern	406
a) Löschen? Löschen. Löschen!	407
aa) Ausgangssituation, Zielsetzung und Begriffe	407
bb) Erwartungshorizont: Löschen (nur) im Internet?	409
b) Überblick über Vorgaben zum Löschen in der Datenschutz-Grundverordnung	411
aa) Vorgaben zur Regellöschung	411
bb) Technisch-organisatorischer Aufwand	412
cc) Informationspflichten	412
dd) Löschung und Nicht-Löschung im Einzelfall auf Antrag	412
ee) Mitteilungspflichten	413
ff) Dokumentationsanforderungen	413
gg) Überwachung der Löschmaßnahmen	414
hh) Weiterentwicklung des Löschkonzepts	414

Inhaltsverzeichnis

ii) Löschen beim Auftragsverarbeiter	414
c) Rechtliche Vorgaben für das Löschen aus anderen Vorschriften ...	414
d) Rahmenbedingungen für ein Löschkonzept	415
aa) Anforderungen an ein Löschkonzept	415
bb) Löschen bei Providern und bei anderen Verantwortlichen	416
cc) Handlungsoptionen: Löschen, Anonymisieren, Sperren,...	417
dd) Exkurs: Löschen ist technisch (nicht?) möglich	418
ee) Praxistauglichkeit eines Löschkonzepts	419
e) DIN 66398 – ein Vorschlag zum Aufbau und zur Umsetzung von Löschkonzepten	420
aa) Gegenstand und Aufbau der Norm	420
bb) Löschregeln festlegen	422
cc) Steuern der Umsetzung	425
dd) Weitere Aufgabenstellungen aus der Praxis	426
ee) Dokumente und Pflege des Löschkonzepts	428
f) Anwendung der DIN 66398	430
aa) Anpassen auf die Organisation	430
bb) Nutzen durch ein Löschkonzept	432
cc) Projekt „Löschkonzept“	433
g) Technische Aspekte von Löschen und Anonymisieren	433
aa) Identifikation von löschfähigen Datenobjekten	433
bb) Löschfähige Datenobjekte aus dem Verarbeitungskontext lösen	435
cc) Sicheres Löschen	436
dd) „Gutes“ Anonymisieren	439
h) Kontrolle über Inhalte – auch im Internet	441
V. Rechte der Betroffenen	443
1. Auskunftsrecht	443
a) Grundlagen	443
b) Verfahren	444
c) Identifizierung	445
2. Berichtigungsrecht	446
3. Löschungsrecht und „Recht auf Vergessenwerden“	447
a) Löschungsrecht	447
b) „Recht auf Vergessenwerden“	448
c) Ausnahmen des Löschungsrechts	450
4. Recht auf Einschränkung der Verarbeitung	451
5. Mitteilungspflicht und Unterrichtsrecht	452
6. Recht auf Datenübertragbarkeit	453
7. Widerspruchsrecht	456
8. Verbot automatisierter Entscheidungen im Einzelfall einschließlich Profiling	456
9. Einschränkung von Betroffenenrechten	458

VI. Rechtsschutz für Betroffene	458
1. Recht auf Beschwerde bei der Aufsichtsbehörde	459
a) Geltendmachung des Beschwerderechts	460
aa) Adressat der Beschwerde	460
bb) Beschwerdebefugnis	462
cc) Form und Frist	463
dd) Inhaltliche Anforderungen	463
b) Pflichten der Aufsichtsbehörden	465
aa) Pflicht zur Befassung mit der Beschwerde	466
bb) Pflicht zur Unterrichtung des Beschwerdeführers	468
cc) Pflicht zur Belehrung des Beschwerdeführers	468
dd) Weitere Pflichten der Aufsichtsbehörden	469
c) Zusammenfassung	469
2. Haftung und Recht auf Schadensersatz	470
a) Anspruchsberechtigte	471
b) Anspruchsgegner und Haftung	471
c) Verstoß	472
d) Schaden	473
e) Haftungsbefreiung	474
f) Zusammenfassung	475
3. Gerichtliche Durchsetzbarkeit	475
a) Gerichtlicher Rechtsbehelf gegen eine Aufsichtsbehörde	476
aa) Gerichtlicher Rechtsbehelf des Betroffenen gegen Beschlüsse einer Aufsichtsbehörde	477
bb) Gerichtlicher Rechtsbehelf bei Nichtbefassung oder bei Verletzung der Informationspflicht	479
b) Gerichtlicher Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	480
c) Parallele Verfahren	482
d) Die Rolle des Europäischen Gerichtshofs	484
aa) Nichtigerklärung eines Beschlusses des Ausschusses	484
bb) Vorabentscheidung	485
e) Zusammenfassung	486
4. Vertretung von betroffenen Personen, Verbandsbeschwerde und Verbandsklage	486
5. Rechtsschutz nach der Datenschutz-Grundverordnung	488
VII. Sanktionen	489
1. Verwaltungsrechtliche Sanktionen und Anordnungen	490
a) Aufgaben der Aufsichtsbehörden	490
b) Untersuchungsbefugnisse der Aufsichtsbehörden	490
c) Zuständigkeit der Aufsichtsbehörden	492
aa) Sachliche Zuständigkeit	492
bb) Örtliche Zuständigkeit	493

Inhaltsverzeichnis

2. Verwaltungsrechtliche Sanktionen und Anordnungen	495
a) Anordnungsbefugnisse	495
aa) Warnung und Verwarnung	495
bb) Anweisung	497
cc) Untersagung	498
b) Rechtsschutz	499
3. Ordnungswidrigkeitsrechtliche Sanktionen	500
a) Bußgeldtatbestände	501
aa) Hoher Bußgeldrahmen	501
bb) Mittlerer Bußgeldrahmen	502
cc) Niedriger Bußgeldrahmen	503
b) Bußgeldverfahren	503
aa) Unternehmensbegriff	503
bb) Verhalten von Mitarbeitern und Externen	505
cc) Kriterien für die Verhängung von Bußgeldern	506
dd) Bußgeldhöhe	507
c) Rechtsschutz	507
4. Strafrechtliche Sanktionen	508
5. Wettbewerbsrechtliche Sanktionen	509
6. Verbraucherschutzrechtliche Verbandsklage	509
Stichwortverzeichnis	511

Verzeichnis der Autoren

Dr. Jens Ambrock	Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
Dr. Ubbo Aßmus	Rechtsanwalt für Datenschutz- und IT-Recht bei Heuking Kühn Lüer Wojtek, Frankfurt aM, Lehrbeauftragter an der Hochschule RheinMain
Dr. Christian L. Geminn	Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel
Dr. Volker Hammer	Consultant bei der Secorvo Security GmbH, Karlsruhe
Prof. Dr. Felix Hermonies	Mag. rer. publ. LL.M. (R.L.), Professor für Datenschutz- und Medienrecht an der Hochschule Darmstadt
Dr. habil. Silke Jandt	Referatsteileiterin bei der Landesbeauftragten für den Datenschutz Niedersachsen, Privatdozentin an der Universität Kassel
Dr. Moritz Karg	Referent und Projektleiter, Digitale Agenda und zentrales IT Management, Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung des Landes Schleswig-Holstein
Till Karsten, LL.M.	Syndikus-Rechtsanwalt bei der infoscore Consumer Data GmbH, part of Arvato Financial Solutions
Henry Krasemann	Referatsleiter beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, Jurafunk, Dozent an FH, WAK, Universität Kiel
Dr. Philipp Richter	Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Annika Selzer	Senior Researcher und Datenschutzrechtlerin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Dr. Roland Steidle	Fachanwalt für Informationstechnologierecht und Partner bei SWM Rechtsanwälte in Frankfurt am Main
Prof. Dr. Thomas Wilmer	Professor für Informationsrecht an der Hochschule Darmstadt