

NomosHANDBUCH

Geminn | Johannes [Hrsg.]

Europäisches Datenrecht

DA | DGA | DS-GVO | DMA | DSA | KI-VO



Helbing
Lichtenhahn



Nomos

NomosHANDBUCH

Dr. Christian L. Geminn
Paul C. Johannes [Hrsg.]

Europäisches Datenrecht

DA | DGA | DS-GVO | DMA | DSA | KI-VO

Praxishandbuch

Dr. André Artelt, Universität Bielefeld | **Dr. Tamer Bile**, LL.M., Kassel | **Fabiola Böning**, Universität Kassel | **Dr. Ernestine Dickhaut**, Universität Kassel | **Prof. Dr. Kai Erenli**, LL.M. (it-law) (Wien), Fachhochschule des BFI Wien | **PD Dr. Christian Geminn**, Mag. iur., Universität Kassel | **RA Dominik Hoidn**, Frankfurt am Main | **Tom Hubert**, Universität Göttingen | **Johannes Jänicke**, Berlin | **RA Paul C. Johannes**, LL.M., Universität Kassel | **Dr. Murat Karaboga**, Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe | **RAin Dr. Johanna M. Kirschnick**, LL.M. (KCL), Berlin | **Marcel Kohpeiß**, LL.M. (Glasgow), Universität Mainz | **Prof. Dr. Steffen Kroschwald**, LL.M., Hochschule Pforzheim | **Dr. Mahei Manhai Li**, Universität Kassel | **Prof. Dr. Jan Marco Leimeister**, Universität Kassel | **Luisa Lorenz**, LL.M., Universität Kassel | **Dr. Yannic Meier**, Universität Duisburg-Essen, Duisburg | **RA Jan-Philipp Muttach**, Frankfurt am Main | **StA Dr. Johannes K. M. Müller**, MLE., Mühlhausen/Thüringen | **Dr. Maxi Nebel**, Ass. iur., Universität Kassel | **Lars Pfeiffer**, LL.M., Universität Kassel | **Philipp Reinhard**, Universität Kassel | **Fabian Schaller**, Datenschutzbeauftragter, Kassel | **Till Schaller**, Universität Kassel | **VorsRiVGi.R. Hans-Hermann Schild**, Universität Kassel | **Dr. Stephan Schindler**, Universität Kassel | **Sabrina Schomberg**, Hessisches Ministerium des Inneren, für Sicherheit und Heimatschutz, Wiesbaden/Kassel | **Philip Schütz**, Datenschutzkoordinator Mercedes-Benz/Universität Göttingen, Stuttgart | **Linda Seyda**, Universität Kassel | **SyndikusRA Benjamin Stach**, LL.M. (KCL), Hamburg | **RA Robert Weinhold**, Düsseldorf | **Dr. Julia Zirfas**, LL.M., Kaden | **Paul Zurawski**, Universität Kassel

 **Helbing
Lichtenhahn**



Nomos

Zitiervorschlag: EU-DatenR-HdB/Autor § ... Rn. ...

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

ISBN 978-3-8487-7404-3 (Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden)

ISBN 978-3-7190-4664-4 (Helbing Lichtenhahn Verlag, Basel)

1. Auflage 2026

© Nomos Verlagsgesellschaft, Baden-Baden 2026. 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 zwanziger Jahre des 21. Jahrhunderts sollen für die Europäische Union ein digitales Jahrzehnt sein, eine Dekade der Daten. Dieses digitale Jahrzehnt und die digitale Zukunft Europas werden durch ein neues Rechtsgebiet gerahmt, das digitale Daten, aber auch digitale Dienste, digitale Märkte und künstliche Intelligenz zum Gegenstand hat – das europäische Datenrecht. Die Benennung des Rechtsgebiets erkennt an, dass die Wertschöpfung aus Daten (personenbezogen wie nicht personenbezogen) letztlich im Zentrum der Digitalisierung steht.

Daten wurden in einer (schiefen) Analogie als Rohstoff der Digitalisierung, als „neues Öl“ bezeichnet – eine Analogie, die wohl einerseits auf der (weitgehenden) Verdrängung von Ölkonzernen von der Spitze der Liste der Unternehmen mit dem höchsten Marktwert durch die heutigen Digitalisierungsgiganten beruht und andererseits auf die gesamtgesellschaftliche Bedeutung von Daten verweist. Die digitale Marktwirtschaft wurde bisher trotz gegenläufiger Bemühungen von außerhalb Europas determiniert – eben durch die genannten Digitalisierungsgiganten und hier allen voran die U.S.-amerikanischen Unternehmen Microsoft, Apple, Amazon, Alphabet und Meta Platforms. Das europäische Datenrecht soll der Grundstein einer Wende sein, im Zuge derer Europa eine „digitale Souveränität“ gewinnt, die bislang schmerzlich vermisst wurde.

Das europäische Datenrecht ist innovativ. Der Verordnungsgeber reguliert Bereiche, in denen anderswo bislang bestenfalls Soft Law besteht oder vereinzelt mitgliedersstaatliche Vorstöße gemacht wurden. Insbesondere mit der KI-Verordnung hat die Europäische Kommission Neuland betreten. Damit kann das Datenrecht letztlich zumindest in Teilen auch als ein legislatives Experiment charakterisiert werden, dessen Ausgang ungewiss bleibt. Offen ist der Ausgang dabei sowohl bezogen auf das Ziel einer Stärkung des Grundfreiheiten- und Grundrechtsschutzes im digitalen Raum als auch bezogen auf die intendierten wirtschaftsfördernden Effekte. Stellt das Datenrecht selbst in einzelnen Bestandteilen aber auch in seiner Gesamtheit eine Innovation dar, so soll es auch digitale Innovationen rund um die Verarbeitung von Daten fördern. Für die Entstehung neuer, innovativer Geschäftsmodelle und für innovativen Grundrechtsschutz soll ein Rahmen gegeben werden, wobei stets auch die Gefahr besteht, dass die Regulierung in das Gegenteil umschlägt und zu Zurückhaltung führt, die Innovationen behindert oder gar nicht erst entstehen lässt.

Das europäische Datenrecht ist allumfassend. Sein Anspruch besteht insgesamt darin, die Verarbeitung von Daten in allen denkbaren Kontexten und über die gesamte „Lebensspanne“ eines Datums zu regulieren. Zudem werden die auf digitale Daten angewiesenen digitalen Dienste und digitalen Märkte reguliert. Regelungen unterworfen wird ferner auch die für eine Datenökonomie und eGovernment erforderliche Infrastruktur.

Das europäische Datenrecht ist hochkomplex und miteinander verwoben. Eine Vielzahl unmittelbar geltender Verordnungen schaffen im Zusammenspiel mit vielen weiteren Rechtsakten ein Dickicht an datenregulatorischen Anforderungen und Compliance-Vorgaben. Damit einher geht ein hohes Maß an Rechtsunsicherheit bei der Auslegung neuer Rechtsbegriffe und der Abgrenzung der Rechtsakte zueinander. Die Regelungen zu Datenzugang, -austausch und -nutzung stehen zudem vielfach quer zu den Vorgaben der Datenschutz-Grundverordnung.

Eine gesetzeskonforme Datennutzung erfordert eine kontinuierliche Überwachung und Überprüfung, um sicherzustellen, dass diese Datennutzung mit den sich ändernden rechtlichen und regulatorischen Anforderungen konform bleibt. Der europäische Rechtsrahmen stärkt die Datensouveränität, enthält aber auch Einschränkungen und bürokratische Anforderungen, die auf den ersten Blick überwältigend wirken können. Diese Einschränkungen sollen den Interessen der Betroffenen, der Datenanbieter und der Dateninhaber gleichermaßen dienen. Dies ist besonders wichtig im Zusammenhang mit der gemeinsamen Nutzung von Daten durch Organisationen. Die gemeinsame Nutzung von Daten kann zwar wirtschaftliche Vorteile

Vorwort der Herausgeber

bringen, birgt aber auch Risiken für den Datenschutz und die Selbstbestimmung. Insofern ist das europäische Datenrecht stets auch eine Gratwanderung.

Dieses Handbuch möchte insbesondere Praktikern, die durch das neue Datenrecht vor große Herausforderungen gestellt werden, helfen, das entstandene Dickicht zu lichten.

Großer Dank gilt selbstverständlich allen Autorinnen und Autoren, dem Verlag sowie ferner den studentischen Hilfskräften Justus Nägele und Alfiya Zhunussova für Ihre tatkräftige Unterstützung bei der Fertigstellung des Handbuchs.

Kassel im Juni 2025

Die Herausgeber

Inhaltsübersicht

Vorwort der Herausgeber	5
Inhaltsverzeichnis	9
Bearbeiterverzeichnis	25
Literaturverzeichnis	27
Abkürzungsverzeichnis	31

Teil 1: Einleitung

§ 1 Das europäische Datenrecht (<i>Geminn</i>)	43
--	----

Teil 2: Grundlagen

§ 2 Daten aus informatischer Sicht (<i>Artelt</i>)	59
§ 3 Daten im Recht (<i>Johannes</i>)	65
§ 4 Datenschutz und Privatheit aus Sicht der (Medien-)Psychologie (<i>Meier</i>)	92
§ 5 Institutionen des Datenrechts: Unabhängigkeit, Durchsetzungsbefugnisse, Grad der Zentralisierung und Agencification (<i>Karaboga/Schütz</i>)	104
§ 6 Grundrechtlicher Rahmen (<i>Geminn</i>)	131
§ 7 Datensouveränität (<i>Schomberg/Muttach</i>)	153

Teil 3: Der Handel mit Daten

§ 8 Einführung in den Datenhandel (<i>Bile</i>)	167
§ 9 Datengetriebene Geschäftsmodelle (<i>Reinhard/Dickhaut/Li/Leimeister</i>)	170
§ 10 Regulierung des Datenhandels (<i>Bile</i>)	196
§ 11 Verträge über Daten (<i>Stach</i>)	211

Teil 4: Macht durch Daten (Digital Markets Act)

§ 12 Das Gesetz über digitale Märkte (<i>Müller</i>)	227
§ 13 Macht und Machtmissbrauch der Torwächter (<i>Müller</i>)	232
§ 14 Torwächterregulierung (<i>Müller</i>)	242

Teil 5: Datendienste und -produkte (Digital Services Act)

§ 15 Einführung und Hintergrund (<i>Erenli</i>)	277
§ 16 Haftungsregelungen für Vermittlungsdienste (<i>Erenli</i>)	285
§ 17 Verantwortung von Vermittlungsdiensten (<i>Erenli</i>)	295
§ 18 Datenverarbeitung in der Cloud (<i>Kroschwald</i>)	306

Teil 6:		
Datensteuerungsrecht (Data Governance Act)		
§ 19	Einführung ins Datensteuerungsrecht (<i>Schomberg/Muttach</i>)	323
§ 20	Weiterverwendung von Informationen des öffentlichen Sektors (<i>Muttach</i>)	336
§ 21	Datenvermittlungsdienste: Gemeinsame Datennutzung (<i>Pfeiffer</i>)	374
§ 22	Dataltruismus (<i>Lorenz</i>)	403
Teil 7:		
Datennutzungsrecht (Data Act)		
§ 23	Der Data Act als Wegbereiter für europäische Industriedatenbörsen (<i>Jänicke</i>)	455
§ 24	Data Act – Anwendungsbereich (<i>Weinhold</i>)	472
§ 25	Bereitstellung von Daten (<i>Weinhold</i>)	492
§ 26	Missbräuchliche Vertragsklauseln (<i>Weinhold</i>)	503
§ 27	Datenverarbeitungsdienste (<i>Weinhold</i>)	507
Teil 8:		
Recht der KI und der digitalen Infrastrukturen		
§ 28	Künstliche Intelligenz – KI-VO und Datenrecht (<i>Böning/Schindler</i>)	515
§ 29	Elektronische Identifizierung (<i>Johannes</i>)	563
§ 30	Elektronische Vertrauensdienste (<i>Johannes</i>)	575
§ 31	Telekommunikation und Netzregulierung (<i>Zirfas</i>)	590
Teil 9:		
Datenschutz und Datensicherheit		
§ 32	Datenschutzrecht (<i>Nebel</i>)	605
§ 33	Datensicherheitsrecht (<i>Schaller/Hubert/Zurawski</i>)	637
Teil 10:		
Sektorübergreifende Betrachtungen		
§ 34	Datenbezogene Herstellerpflichten (<i>Kroschwald</i>)	671
§ 35	Datenrechte (<i>Kohpeiß/Seyda</i>)	687
§ 36	Forschung mit und an Daten (<i>Johannes</i>)	717
§ 37	Datenschutzvorfälle und Meldepflichten (<i>Schaller</i>)	737
§ 38	Internationale Datenflüsse (<i>Kirschnick/Hoidn</i>)	753
Teil 11:		
Rechtsbehelfe und Sanktionen		
§ 39	Rechtsbehelfe und Rechtswege (<i>Schild</i>)	765
§ 40	Sanktionen (<i>Kirschnick</i>)	795
Teil 12:		
Ausblick		
§ 41	Die Zukunft des europäischen Datenrechts (<i>Geminn</i>)	817
	Stichwortverzeichnis	819

Inhaltsverzeichnis

Vorwort der Herausgeber	5
Bearbeiterverzeichnis	25
Literaturverzeichnis	27
Abkürzungsverzeichnis	31

Teil 1: Einleitung

§ 1 Das europäische Datenrecht	43
A. Datenrecht – Was ist das?	43
B. Der lange Weg zum europäischen Datenrecht	46
C. Zentrale (nicht-rechtliche) Definitionen des Datenrechts	49
D. Zu Aufbau und Zielen dieses Handbuchs	53

Teil 2: Grundlagen

§ 2 Daten aus informatischer Sicht	59
A. Begrifflichkeit	60
B. Datenverarbeitung in der Informatik	62
I. Kryptografie – Sichere Datenverarbeitung, Speicherung und Übertragung	62
II. Data Mining – Wissen und Modelle aus Daten generieren	63
§ 3 Daten im Recht	65
A. Daten im Recht – Einleitung	66
B. Datenbegriff(e) des Unionsrechts	67
I. Primärrecht	67
II. Sekundärrecht	68
C. Personenbezogene und nicht personenbezogene Daten	75
I. Personenbezogene Daten	76
II. Nicht personenbezogene Daten	83
D. Akteure im Zusammenhang mit Daten	84
E. Rechte an und über Daten	87
I. Immaterialgüterrechte	88
II. Dateneigentum	89
III. Datenbesitz	90
F. Zusammenfassung und Bewertung	90
§ 4 Datenschutz und Privatheit aus Sicht der (Medien-)Psychologie	92
A. Privatheit	94
B. Privatheit im Internet	95
C. Digitale Privatheitsentscheidungen	96
I. Paradoxon oder Abwägung?	96

II. Missverhältnis zwischen Vor- und Nachteilen	98
D. Hindernisse und Abhilfen für Nutzende	99
I. (K)ein Gespür für Privatheit	99
II. Negative Auswirkungen des Überwachungsbewusstseins	100
III. Datenschutzerklärungen	100
IV. Einwilligung	101
V. Transparenz und Selbstschutz	102
E. Zusammenfassung und Fazit	103
§ 5 Institutionen des Datenrechts: Unabhängigkeit, Durchsetzungsbefugnisse, Grad der Zentralisierung und Agencification	104
A. Einführung	105
B. Datenschutz-Grundverordnung	106
I. Aufstellung und Unabhängigkeit der Aufsichtsbehörden	106
II. Aufgaben und Befugnisse	107
III. Koordinations- und Kooperationsmechanismen sowie supranationale Institutionen	107
C. Digital Markets Act	109
D. Digital Services Act	110
I. Zuständige Behörden	111
II. Koordinations- und Kooperationsmechanismen	112
E. Data Governance Act	113
I. Zuständige Stellen	113
II. Zuständige Behörden	114
III. Der Europäische Dateninnovationsrat	115
F. Data Act	116
I. Zuständige Behörden	117
II. Rolle des Europäischen Dateninnovationsrats	118
G. KI-VO	119
I. Supranationale Ebene	120
II. Nationale Ebene	122
H. Vergleich	124
I. Unabhängigkeit der Institutionen des Datenrechts	124
II. Durchsetzungsbefugnisse der Institutionen des Datenrechts	125
III. Zentralisierungsgrad von Befugnissen im EU-Mehrebenensystem	126
IV. Analyse im Lichte von Agencification	127
I. Abschließende Betrachtungen und Ausblick	128
§ 6 Grundrechtlicher Rahmen	131
A. Einführung	131
B. Würde des Menschen, Art. 1 GRCh	132
C. Achtung des Privat- und Familienlebens	133
D. Schutz personenbezogener Daten, Art. 8 GRCh, Art. 16 AEUV	134
E. Freiheit der Meinungsäußerung und Informationsfreiheit, Art. 11 GRCh	134

F. Berufsfreiheit, 15 GRCh	135
G. Unternehmerische Freiheit, Art. 16 GRCh	135
H. Eigentumsrecht, Art. 17 GRCh	135
I. Eigentum an Datenträgern	136
II. Eigentum an Daten	137
III. Daten als geistiges Eigentum	137
I. Drittwirkung der Grundrechte der Charta	138
J. Verfassungsrecht der Mitgliedstaaten	138
I. Belgien	139
II. Bulgarien	139
III. Dänemark	139
IV. Deutschland	139
V. Estland	143
VI. Finnland	144
VII. Frankreich	144
VIII. Griechenland	144
IX. Irland	144
X. Italien	145
XI. Kroatien	145
XII. Lettland	145
XIII. Litauen	146
XIV. Luxemburg	146
XV. Malta	146
XVI. Niederlande	146
XVII. Österreich	147
XVIII. Polen	147
XIX. Portugal	147
XX. Rumänien	148
XXI. Schweden	148
XXII. Slowakei	149
XXIII. Slowenien	149
XXIV. Spanien	150
XXV. Tschechien	151
XXVI. Ungarn	151
XXVII. Zypern	151
§ 7 Datensouveränität	153
A. Begriff der Datensouveränität	154
B. Verhältnis zur digitalen Souveränität	155
C. Datensouveränität in der rechtswissenschaftlichen Literatur	157
D. Konflikt mit dem Datenschutz?	160
E. Rechtswahrnehmung	162
F. Regelungsansätze in neuem europäischen Datenrecht?	162

**Teil 3:
Der Handel mit Daten**

§ 8	Einführung in den Datenhandel	167
§ 9	Datengetriebene Geschäftsmodelle	170
	A. Einleitung	171
	I. Digitalisierung und digitale Transformation	171
	II. Von Daten zu Big Data	173
	III. Einsatz von Daten	175
	IV. Plattformeffekte und Entstehung von Gatekeepern	176
	B. Von Daten zu Geschäftsmodellen	180
	I. Wertnetzwerk und Ökosystem	182
	II. Wertarchitektur	184
	III. Wertversprechen	187
	IV. Wertrealisierung	189
	C. Fallbeispiele	190
	I. Google – Plattformökosystem	190
	II. Mitsubishi Electric – Industrie 4.0	192
	D. Diskussion & Fazit	194
§ 10	Regulierung des Datenhandels	196
	I. Möglichkeiten und Restriktion des Datenhandels durch die DS-GVO ...	197
	II. Zugang zu Daten nach dem Data Governance Act	199
	III. Zugang zu und Weiterwendungsmöglichkeiten von Daten durch den Data Act	204
	IV. Fazit	208
§ 11	Verträge über Daten	211
	A. Einleitung	211
	B. Grundlagen der Datenverträge	211
	I. Datenschutz-Grundverordnung (DS-GVO)	212
	II. Data Act (DA)	213
	III. Data Governance Act (DGA)	214
	IV. Digital Markets Act (DMA)	215
	V. Digital Services Act (DSA)	216
	VI. KI-VO	217
	C. Vertragsgestaltung und Compliance	218
	I. Wichtige Aspekte der Vertragsgestaltung	219
	II. Rechtskonforme Vertragsgestaltung	219
	III. Besondere Herausforderungen	221
	D. Fazit	223

Teil 4:
Macht durch Daten (Digital Markets Act)

§ 12	Das Gesetz über digitale Märkte	227
	A. Relevanz von Plattformen und digitalen Diensten	228
	B. Zeitliche Entstehung	230
§ 13	Macht und Machtmissbrauch der Torwächter	232
	A. Ursachen	233
	B. Bestreitbarkeit und Fairness	236
	I. Vertraglicher Missbrauch	237
	II. Technischer Missbrauch	238
	III. Faktischer Missbrauch	239
§ 14	Torwächterregulierung	242
	A. Bisherige Regulierung	242
	I. Europäische Ebene	242
	II. Nationale Ebene	243
	B. Regulierung durch den DMA	244
	I. Der Gegenstand und Anwendungsbereich des DMA	245
	II. Die Erfassung der Torwächter durch den DMA: Art. 2, 3, 4	246
	III. Die „Verpflichtung(en)“ der Torwächter	255
	IV. Sanktionsregime	271
	C. Fazit und Ausblick	274
 Teil 5: Datendienste und -produkte (Digital Services Act)		
§ 15	Einführung und Hintergrund	277
	A. Der Weg zum DSA – Historischer Kontext und Entwicklung	278
	B. Der DSA – Kerninhalte und Ziele	280
	C. Definition und Bedeutung von Vermittlungsdiensten	280
§ 16	Haftungsregelungen für Vermittlungsdienste	285
	A. Haftungsprivilegierung	285
	I. Reine Durchleitung	286
	II. Caching	288
	III. Hosting	290
	B. Überwachungs- und Informationspflichten	292
	C. Zwischenfazit	293
§ 17	Verantwortung von Vermittlungsdiensten	295
	A. Kategorisierung der Vermittlungsdienste im DSA	296
	B. Sorgfaltspflichten	297
	I. Alle Vermittlungsdienste	297
	II. Hostinganbieter einschließlich Online-Plattformen (Abschnitt 2)	298

III. Anbieter von Online-Plattformen (Abschnitt 3)	299
IV. Anbieter von Online-Handelsplattformen (Abschnitt 4)	301
V. VLOPs (Abschnitt 5)	302
C. Fazit	304
§ 18 Datenverarbeitung in der Cloud	306
A. Übersicht	308
B. Datenverarbeitung in der Cloud	309
C. Cloud-Dienste im DSA	310
I. Die Cloud als (privilegierter?) Vermittlungsdienst	310
II. Sorgfaltspflichten für Cloud-Anbieter	311
III. Inhaltsmoderation in der Cloud?	311
D. Cloud-Dienste nach der DS-GVO	312
I. Sachlicher Anwendungsbereich	313
II. Cloud als Auftragsverarbeitung?	313
III. Verantwortlicher Cloud-Anbieter?	314
IV. Rechte betroffener Personen und Datenportabilität	316
V. Grenzüberschreitendes Cloud Computing	316
E. Datenverarbeitung in der Cloud nach dem DA	317
F. Datenverarbeitung in der Cloud nach dem DGA	318
G. Datenverarbeitung in der Cloud im Digital Markets Act	319

Teil 6:

Datensteuerungsrecht (Data Governance Act)

§ 19 Einführung ins Datensteuerungsrecht	323
A. Die Richtlinie über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (RL 2019/1024)	324
I. Genese	324
II. Regelungsziele	325
III. Überblick über die Regelungen	325
B. Das Gesetz für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz – DNG)	326
I. Genese	326
II. Regelungsziele	326
III. Überblick über die Regelungen	327
C. Der Data Governance Act (DGA)	327
I. Genese	327
II. Regelungsziele	328
III. Überblick über die Regelungen im Data Governance Act	328
IV. Abgrenzung zu verwandten Rechtsakten	334
D. Gesetze und Verordnungen mit Bereitstellungsregelungen	334

§ 20	Weiterverwendung von Informationen des öffentlichen Sektors	336
A.	Datenzugangsregelungen	338
I.	Bereitstellungspflicht gem. § 12a EGovG – Open-Data-Regelung des Bundes	338
II.	Bereitstellungsregelungen gem. § 3a PBefG iVm Mobilitätsdatenverordnung (MDV)	340
III.	Datenzugangsansprüche	340
B.	Weiterverwendung offener Daten	341
I.	Richtlinie (EU) 2019/1024 (OD-PSI-RL)	341
II.	Gesetz für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz – DNG)	347
C.	Weiterverwendung geschützter Daten (DGA)	360
I.	Adressaten und Anwendungsbereich	360
II.	Grundsätzliches Verbot von Ausschließlichkeitsvereinbarungen, Art. 4 DGA	365
III.	Weiterverwendung von Daten nach dem DGA – Bedingungen und Grenzen	367
§ 21	Datenvermittlungsdienste: Gemeinsame Datennutzung	374
A.	Hintergrund der Regulierung	377
B.	Der Ordnungsrahmen für Datenvermittlungsdienste im DGA	379
I.	Datenvermittlungsdienste qua Legaldefinition	379
II.	Datenvermittlungsdienste im Anwendungsbereich des Kap. III DGA	383
C.	Pflichten für Anbieter von Datenvermittlungsdiensten	386
I.	Vor Aufnahme der Tätigkeit	387
II.	Während der Erbringung der Tätigkeit	387
III.	Nach Beendigung der Tätigkeit	392
D.	Aufsicht, Durchsetzung und Sanktionen	392
I.	Zuständige Behörden	392
II.	Aufgaben und Befugnisse der zuständigen Behörden	395
III.	Beschwerderecht, Rechtsbehelf und Sanktionen	397
E.	Zusammenspiel mit anderen Rechtsakten und Vorhaben	397
I.	Datenschutz-Grundverordnung	398
II.	Data Act	399
III.	Gemeinsame europäische Datenräume	400
F.	Bewertung und Ausblick	401
§ 22	Datenaltruismus	403
A.	Einführung	405
B.	Datenaltruismus als vielversprechende Form gesetzlicher Datenregulierung	405
C.	Einordnung des DGA in den Rechtsrahmen für datenaltruistische Verarbeitungen	406
I.	Vorbemerkung	406

II. Zusammenwirken von DGA und nationalem Recht, DS-GVO und Data Act	408
D. Das Konzept des „Datenaltruismus“ nach DGA	412
I. Überblick	412
II. „Datenaltruismus“ iSv Art. 2 Nr. 16 DGA	412
III. Abgrenzung zum (Rechts-)Institut der sog. Datenspende	415
IV. Zugrundeliegendes Regulierungskonzept	416
E. Kapitel IV (Art. 16 bis 25) des DGA zum Datenaltruismus im Einzelnen	417
I. Nationale Regelungen für Datenaltruismus (Art. 16 DGA)	417
II. Anerkennung, Tätigkeit und Überwachung datenaltruistischer Organisationen (Art. 17 bis 24 DGA)	419
III. Ergänzendes Regelwerk der Kommission (Art. 22 DGA)	433
IV. Behördliche Zuständigkeit und Organisation (Art. 23 und 26 DGA)	434
V. Behördliche Überwachungsbefugnisse nach Art. 24 DGA	436
VI. Europäisches Einwilligungsformular für Datenaltruismus (Art. 25 DGA)	441
VII. Zwischenfazit	445
F. Ergänzende Regelungen (Art. 27 f., 29 f. und 34 DGA)	445
I. Beschwerderecht (Art. 27 DGA)	445
II. Recht auf einen wirksamen gerichtlichen Rechtsbehelf (Art. 28 DGA) ..	446
III. Mitgliedstaatliche Sanktionsvorschriften (Art. 34 DGA)	447
IV. Europäischer Dateninnovationsrat (Art. 29 f. DGA)	449
G. Gesamtfazit und Ausblick	449

Teil 7:

Datennutzungsrecht (Data Act)

§ 23 Der Data Act als Wegbereiter für europäische Industriedatenbörsen	455
A. Einleitung	456
B. Das Marktdesign für Produktdaten in Kapitel II	457
I. Der anreiz-ineffiziente Status Quo	457
II. Asymmetrische Informationsverteilung über Daten und ihren Wert	457
III. Niedrigere Grenzkosten bei Datenzugang und -verarbeitung	457
IV. Die Möglichkeit Daten in aggregierter Form anzubieten	458
V. Suboptimale Anreizperspektive für Hersteller zum Datenteilen	458
C. Die Limitierung des Kommissionsvorschlags auf primäre Datenmärkte	458
D. Ergebnis der Trilog-Verhandlungen: Aktivierung des Data Acts für Sekundärmärkte	459
I. Änderung 1: Unterscheidung bei vorvertraglichen Pflichten zwischen Kauf eines IoT Produktes einerseits und Abschluss eines Vertrags über verbundene Dienste andererseits	460
II. Änderung 2: Unterscheidung zwischen Produktdaten und verbundenen Dienstdaten	462
III. Änderung 3: Exklusive Vermarktungsrechte an Produktdaten für Nutzer in Art. 4 Abs. 14	463

IV. Änderung 4: Unterscheidung zwischen Produktdaten und verbundenen Dienstdaten	464
E. Die Rolle von Datenvermittlungsdiensten im Kontext von Art. 4 Abs. 14	465
F. Zusammenfassung der Neuerungen in Kapitel II	465
G. Herausforderungen und Überblick – Ein unsicherer Blick auf die Zukunft der Datenökonomie	467
I. Möglichkeit des prospektiven Nutzers, die Datenverwertung zu planen	468
II. Neue Geschäftsmodelle zum Handel mit Rechten auf Datenzugang- und Nutzung	468
III. Herausforderungen bei der Wertbestimmung von Daten	469
IV. Erste Ansätze zur Wertbestimmung/Rolle von Intermediären	469
V. Datenmärkte heute und die Verknüpfung zwischen Data Act und Data Governance Act	470
H. Fazit	470
§ 24 Data Act – Anwendungsbereich	472
A. Gegenstand und Anwendungsbereich des Data Acts	473
I. Gegenstand der Verordnung	473
II. Sachlicher Anwendungsbereich	475
III. Räumlicher und persönlicher Anwendungsbereich	480
IV. Anwendung und Durchsetzung	482
B. Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen	482
I. Pflichten zur Zugänglichmachung von Produktdaten und verbundenen Dienstdaten	482
II. Bereitstellung von Daten	483
III. Weitergabe von Daten	485
IV. Pflichten Dritter, die Daten auf Verlangen des Nutzers erhalten haben ..	487
V. Einschränkung für KMU	489
VI. Obligatorische Nutzerrechte	490
§ 25 Bereitstellung von Daten	492
A. Unrechtmäßiger staatlicher Zugang und Interoperabilität	493
B. Verhältnis zu anderen Vorschriften	493
I. Datenschutz	493
II. Sonstige Vorschriften	494
C. Bedingungen der Datenbereitstellung	494
I. Vereinbarung und FRAND-Bedingungen	494
II. Gegenleistung für die Bereitstellung von Daten	497
III. Streitbeilegung	498
IV. Technische Schutzmaßnahmen	500
V. Umfang der Pflichten von Dateninhabern	500
D. Bereitstellung von Daten für öffentliche Stellen	500

§ 26	Missbräuchliche Vertragsklauseln	503
	A. Anwendungsbereich	503
	B. Einseitiges Auferlegen	504
	C. Klauselkontrolle	505
	I. Klauseln ohne Wertungsmöglichkeit	505
	II. Klauseln mit Wertungsmöglichkeit	505
	III. Generalklausel	506
	D. Rechtsfolgen	506
§ 27	Datenverarbeitungsdienste	507
	A. Begriff Datenverarbeitungsdienst	508
	I. Flächendeckender und auf Abruf verfügbarer Netzzugang	508
	II. Gemeinsam genutzter Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen	508
	III. Zentralisierter, verteilter oder hochgradig verteilter Art	509
	IV. Minimaler Verwaltungsaufwand oder minimale Interaktion des Diensteanbieters zur raschen Bereitstellung und Freigabe	509
	V. Erfasste Dienste	509
	B. Verpflichtete und Begünstigte	510
	C. Wechsel zu gleichartigen Diensten, IKT-Infrastruktur oder bei gleichzeitiger Inanspruchnahme mehrerer Anbieter	510
	D. Anforderungen an Datenverarbeitungsdienste	510
Teil 8:		
Recht der KI und der digitalen Infrastrukturen		
§ 28	Künstliche Intelligenz – KI-VO und Datenrecht	515
	A. Einführung: Die KI-VO	518
	I. Entstehungskontext, Gesetzgebungshistorie und Auslegungsprobleme	519
	II. Zielsetzung	521
	III. Struktur	521
	IV. Geltung der KI-VO	521
	B. Begriff der künstlichen Intelligenz	522
	I. KI-System	522
	II. KI-Systeme und KI-Modelle mit allg. Verwendungszweck	525
	C. Anwendungsbereich der KI-VO	525
	I. Anwendungsbereich gem. Art. 2 Abs. 1 KI-VO	525
	II. Ausnahmen und Einschränkungen	530
	D. Vorgaben der KI-VO	533
	I. KI-Kompetenz	533
	II. Verbotene Praktiken im KI-Bereich	533
	III. Hochrisiko-KI-Systeme	541
	IV. Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme	550

V. KI-Modelle mit allg. Verwendungszweck	552
VI. Maßnahmen zur Innovationsförderung	553
VII. Governance: Behörden und Einrichtungen	553
VIII. Beobachtung, Informationsaustausch, Marktüberwachung und Rechtsbehelfe	554
IX. Verhaltenskodizes, Leitlinien und delegierte Rechtsakte	555
X. Sanktionen und Haftung	556
E. Bezüge zu anderen Gesetzen und Umsetzungsbedarf	557
I. Bisherige Rechtslage in Deutschland und der Union	557
II. Verhältnis der KI-VO zu anderen Vorschriften des Datenrechts	557
III. Umsetzungsbedarf der Mitgliedstaaten	561
F. Fazit und Ausblick	562
§ 29 Elektronische Identifizierung	563
A. Regulierung der Dateninfrastruktur	563
B. Regelungssystematik der eIDAS-VO	564
C. Elektronische Identifizierung in eIDAS	566
I. Harmonisierung von eID-Systemen	566
II. Europäische Brieftasche für die digitale Identität	568
D. eID im Kontext des europäischen Datenrechts	572
E. Schlussbemerkung	574
§ 30 Elektronische Vertrauensdienste	575
A. Regulierung der Dateninfrastruktur	575
B. Regelungssystem der eIDAS-VO	575
C. Vertrauensdienste in eIDAS-VO	577
I. Begriffsbestimmungen	578
II. Allgemeine Regeln für Vertrauensdienste	578
III. Anforderungen an qualifizierte Vertrauensdiensteanbieter	579
IV. Qualifizierte elektronische Signaturen	581
V. Qualifizierte elektronische Siegel	583
VI. Qualifizierte elektronische Zeitstempel	583
VII. Qualifizierte Dienste für die Zustellung elektronischer Einschreiben	583
VIII. Qualifizierte Zertifikate für die Website-Authentifizierung	584
IX. Qualifizierte elektronische Attributsbescheinigung	584
X. Qualifizierte elektronische Archivierungsdienste	585
XI. Qualifizierte elektronische Journale	585
D. Rechtswirkung	586
E. Vertrauensdienste im Kontext des europäischen Datenrechts	588
F. Schlussbemerkung	589
§ 31 Telekommunikation und Netzregulierung	590
A. Einleitung	590

B. Gesetzliche Vorgaben	591
I. Fernmeldegeheimnis	591
II. European Electronic Communications Code und Umsetzung im TKG	591
III. Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz	592
IV. Verfügungen, Rechtsverordnungen und Verwaltungsvorschriften	593
C. Datenverarbeitungen in der Telekommunikation	593
D. Regulierungs- und Complianceanforderungen an TK-Unternehmen	595
I. Recht auf Versorgung/„Universaldienst“	595
II. Netzneutralität	597
III. Öffentliche Sicherheit & Auskunftspflichten	599

**Teil 9:
Datenschutz und Datensicherheit**

§ 32 Datenschutzrecht	605
A. Unionsrechtliche Vorgaben	607
I. Datenschutzrichtlinie 95/46/EG (DSRL)	607
II. Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (EK-DSRL)	608
III. Cookie-Richtlinie 2009/136/EG	609
IV. Datenschutz-Grundverordnung 2016/679/EU (DS-GVO)	610
V. ePrivacy-Verordnung	610
B. Das Verhältnis des neuen Europäischen Datenrechts zur DS-GVO	611
C. Der DMA im Verhältnis zur DS-GVO	612
D. Der DSA im Verhältnis zur DS-GVO	614
I. Gestaltung und Organisation der Online-Schnittstelle	615
II. Werbung auf Online-Plattformen	616
III. Online-Schutz Minderjähriger	617
E. Der DGA im Verhältnis zur DS-GVO	619
I. Verhältnis zu anderen Verordnungen, Art. 1 Abs. 3 DGA	619
II. Weiterverwendung von Daten durch öffentliche Stellen, Art. 3 ff. DGA	620
III. „Bemühen“ um eine Einwilligung, Art. 5 Abs. 6 DGA	621
IV. Zuständige Stelle, Art. 7 DGA	622
V. Verhaltenspflichten der Datenvermittlungsdienste, Art. 12 DGA	623
F. Der DA im Verhältnis zur DS-GVO	624
I. Der Begriff der Daten	625
II. Umfang der Datenzugangsrechte und datenschutzrechtliche Konsequenzen	625
III. Datenübertragbarkeit	626
IV. Rechtsgrundlage bei Drittbezug personenbezogener Daten	626
V. Personenbezug der Daten	628
VI. Profiling	628

G.	Die KI-VO im Verhältnis zur DS-GVO	629
I.	Allgemeines	630
II.	Datenschutzgrundsätze und Betroffenenrechte	631
III.	Rechtsgrundlagen	633
IV.	Automatisierte Entscheidungsfindung	634
V.	Rechtsbehelfe	635
H.	Fazit	635
§ 33	Datensicherheitsrecht	637
A.	Einführung	639
I.	Begriff der Datensicherheit	639
II.	Datensicherheit im europäischen Datenrecht	641
B.	Anforderungen an die Gestaltung der Datensicherheit	651
I.	Datensicherheitsbedarf	652
II.	Angemessenheit der Maßnahmen	656
III.	Einzelne Maßnahmen	657
IV.	Rechtliche Grenzen der Datensicherheitsmaßnahmen	660
C.	Normung, Zertifizierung, Verhaltensregeln, Konformitätserklärungen und Kennzeichnungen	662
I.	Normung	662
II.	Konformitätserklärungen	662
III.	Zertifizierung	663
IV.	Verhaltensregeln	664
V.	Kennzeichnungen	664
D.	Folgen eines Verstoßes gegen die Datensicherheit	665
I.	Melde- und Benachrichtigungspflichten	665
II.	Aufsichts- und Durchsetzungsmaßnahmen	667
III.	Haftung	667

Teil 10:
Sektorübergreifende Betrachtungen

§ 34	Datenbezogene Herstellerpflichten	671
A.	Übersicht: Datenbezogene Herstellerpflichten	672
B.	Herstellerpflichten im Data Act	672
I.	Hintergrund und Anwendungsbereich	672
II.	Data Accessibility by Design	674
III.	Regelungsadressaten	674
IV.	Gestaltungsanforderungen	676
V.	Grenzen des Zugangs nach Art. 3 DA	679
VI.	Folgen eines Verstoßes gegen Art. 3 Abs. 1 DA	682
C.	Herstellerpflichten im weiteren europäischen Datenrecht	683
I.	Datenschutz-Grundverordnung	683
II.	Digital Markets Act	684

III. KI-VO	685
§ 35 Datenrechte	687
A. Datenrechte des europäischen Datenrechts	688
I. Eingrenzung und Definition des Begriffs der Datenrechte	689
II. Dargestellte Rechtsakte und ihre Schutzrichtungen	689
B. Rechte auf Auskunft	691
I. Art. 15 Abs. 1 DS-GVO – Auskunftsrecht der betroffenen Person	691
II. Art. 15 Abs. 2 DS-GVO – Auskunftsrecht der betroffenen Person im Fall von Drittlandsübermittlung	698
C. Rechte auf Zugang zu Daten	698
I. Art. 15 Abs. 3 DS-GVO – Recht auf Kopie personenbezogener Daten	699
II. Art. 20 DS-GVO – Recht auf Datenübertragbarkeit	700
III. Art. 4 und 5 DA – Datenzugangsrechte	701
IV. Art. 6 Abs. 9 DMA – Nutzerzugang	702
V. Art. 12 DGA – Zugang für Betroffene ggü. Datenintermediären	702
D. Einwirkungs- und Gestaltungsrechte	702
I. Art. 16 DS-GVO – Recht auf Berichtigung	703
II. Art. 17 DS-GVO – Recht auf Löschung („Vergessenwerden“)	704
III. Art. 18 DS-GVO – Recht auf Einschränkung der Verarbeitung	705
IV. Art. 21 DS-GVO – Widerspruchsrecht	706
E. Verbote und Compliance-Bestimmungen mit objektiver Schutzrichtung	708
I. Art. 22 DS-GVO – Keine Entscheidung, die ausschließlich auf automatisierter Verarbeitung beruht (inkl. Profiling)	708
II. Art. 86 KI-VO – Recht auf Erläuterung der Einzelentscheidung	710
F. Rechte auf Rechtsbehelfe, Vertretung und Schadensersatz	710
I. Rechtsbehelfe, gerichtliche Zuständigkeiten und Rechtsweg; Vertretung	710
II. Art. 82 DS-GVO – Haftung und Recht auf Schadenersatz	711
III. Art. 54 DSA – Entschädigungen	715
G. Datenrechte von Aufsichtsbehörden und Institutionen	716
§ 36 Forschung mit und an Daten	717
A. Forschung und Daten	717
I. Forschungsarbeit und Scientific Data Life Cycle	717
II. Bedeutung	718
B. Wissenschaft- und Forschungsfreiheit	719
C. Forschung im europäischen Datenrecht	721
I. Datenschutz-Grundverordnung	721
II. Data Act	725
III. Data Governance Act	728
IV. KI-Verordnung	729
V. DMA	732
VI. DSA	732

D.	Anwendungsbereich und dessen Eingrenzung	733
I.	Adressaten	734
II.	Wissenschaftliche Forschung	734
III.	Abgrenzungsmöglichkeiten	735
E.	Zusammenfassung und Ausblick	736
§ 37	Datenschutzvorfälle und Meldepflichten	737
A.	Datenschutzvorfälle	737
I.	Rechtliche Grundlagen	738
II.	Verhältnis der verschiedenen Vorfallsarten zueinander	740
III.	Fazit Vorfälle	740
B.	Meldepflichten an Behörden	741
I.	Rechtliche Grundlagen	741
II.	Zusammenfassung Meldepflicht an Behörden	748
C.	Meldepflichten an Betroffene	748
I.	Rechtliche Grundlagen	748
II.	Zusammenfassung Benachrichtigungspflicht an Betroffene	752
§ 38	Internationale Datenflüsse	753
A.	Übersicht	753
B.	Einzelne Regelungen	754
I.	Datenschutz-Grundverordnung	754
II.	Data Act	755
III.	KI-Verordnung	758
IV.	Digital Services Act	759
V.	Digital Markets Act	760
VI.	Data Governance Act	760
C.	Umsetzungs-/Anpassungsbedarf in Deutschland	762
D.	Fazit	762

**Teil 11:
Rechtsbehelfe und Sanktionen**

§ 39	Rechtsbehelfe und Rechtswege	765
A.	Einführung	765
B.	Rechtsbehelfe gegen Verantwortliche und Auftragsverarbeiter – Zivilrechtlicher Rechtsbehelf nach der DS-GVO	766
I.	Zivilverfahren	767
II.	Arbeitsgerichtliches Verfahren	771
C.	Rechtsbehelfe gegen verantwortliche öffentliche Stellen und die Aufsichtsbehörden – Verwaltungsgerichtlicher Rechtsbehelf nach der DS-GVO	771
I.	Rechtsbehelfe nach Art. 79 DS-GVO	772
II.	Amtsermittlung	774
III.	Gerichtlicher Vergleich	774

Inhaltsverzeichnis

IV. Klagen gegen die Aufsichtsbehörde – Sonderregelungen	775
V. Ermessensüberprüfung bei Entscheidungen der Aufsichtsbehörde	779
VI. Streitwerte	781
VII. Rechtsmittel	781
D. Weitere Rechtsakte	783
I. Data Governance Act (DGA)	783
II. Data Act (DA)	785
III. Gesetz über digitale Märkte (DMA)	787
IV. Gesetz über digitale Dienste (DSA)	790
V. Verordnung über künstliche Intelligenz (KI-VO)	792
§ 40 Sanktionen	795
A. Übersicht	795
B. Einzelne Regelungen	796
I. Datenschutz-Grundverordnung	796
II. Data Act	798
III. Data Governance Act	801
IV. Digital Services Act	804
V. Digital Markets Act	808
VI. KI-Verordnung	810
C. Regelungsbedarf und Empfehlungen	812
Teil 12: Ausblick	
§ 41 Die Zukunft des europäischen Datenrechts	817
Stichwortverzeichnis	819

Bearbeiterverzeichnis

<i>Dr. André Artelt</i> Universität Bielefeld	§ 2
<i>Dr. Tamer Bile, LL.M.</i> Kassel	§§ 8, 10
<i>Fabiola Böning</i> Universität Kassel	§ 28 (mit <i>Schindler</i>)
<i>Dr. Ernestine Dickhaut</i> Universität Kassel	§ 9 (mit <i>Reinhard/Li/Leimeister</i>)
<i>Prof. Dr. Kai Erenli, LL.M. (it-law) (Wien)</i> Fachhochschule des BFI Wien	§§ 15 bis 17
<i>PD Dr. Christian Geminn, Mag. iur.</i> Universität Kassel	§§ 1, 6, 41
<i>RA Dominik Hoidn</i> Frankfurt am Main	§ 38 (mit <i>Kirschnick</i>)
<i>Tom Hubert</i> Universität Göttingen	§ 33 (mit <i>Schaller/Zurawski</i>)
<i>Johannes Jänicke</i> Berlin	§ 23
<i>RA Paul C. Johannes, LL.M.</i> Universität Kassel	§§ 3, 29, 30, 36
<i>Dr. Murat Karaboga</i> Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe	§ 5 (mit <i>Schütz</i>)
<i>RAin Dr. Johanna M. Kirschnick, LL.M. (KCL)</i> Berlin	§ 38 (mit <i>Hoidn</i>) § 40
<i>Marcel Kohpeiß, LL.M. (Glasgow)</i> Universität Mainz	§ 35 (mit <i>Seyda</i>)
<i>Prof. Dr. Steffen Kroschwald, LL.M.</i> Hochschule Pforzheim	§§ 18, 34
<i>Dr. Mabei Manhai Li</i> Universität Kassel	§ 9 (mit <i>Reinhard/Dickhaut/Leimeister</i>)
<i>Prof. Dr. Jan Marco Leimeister</i> Universität Kassel	§ 9 (mit <i>Reinhard/Dickhaut/Li</i>)
<i>Luisa Lorenz, LL.M.</i> Universität Kassel	§ 22

Bearbeiterverzeichnis

<i>Dr. Yannic Meier</i> Universität Duisburg-Essen, Duisburg	§ 4
<i>StA Dr. Johannes K. M. Müller, MLE.</i> Mühlhausen/Thüringen	§§ 12 bis 14
<i>RA Jan-Philipp Muttach</i> Frankfurt am Main	§§ 7, 19 (mit <i>Schomberg</i>) § 20
<i>Dr. Maxi Nebel</i> Universität Kassel	§ 32
<i>Lars Pfeiffer, LL.M.</i> Universität Kassel	§ 21
<i>Philipp Reinhard</i> Universität Kassel	§ 9 (mit <i>Dickhaut/Li/ Leimeister</i>)
<i>Fabian Schaller</i> Datenschutzbeauftragter, Kassel	§ 37
<i>Till Schaller</i> Universität Kassel	§ 33 (mit <i>Hubert/Zurawski</i>)
<i>VorsRiVG a.D. Hans-Hermann Schild</i> Universität Kassel	§ 39
<i>Dr. Stephan Schindler</i> Universität Kassel	§ 28 (mit <i>Böning</i>)
<i>Sabrina Schomberg</i> Hessisches Ministerium des Inneren, für Sicherheit und Heimatschutz, Wiesbaden/Kassel	§§ 7, 19 (mit <i>Muttach</i>)
<i>Philip Schütz</i> Datenschutzkoordinator Mercedes-Benz (Stuttgart); Doktorand Universität Göttingen; Geschäftsführer data revo- lution (Karlsruhe)	§ 5 (mit <i>Karaboga</i>)
<i>Linda Seyda</i> Universität Kassel	§ 35 (mit <i>Kohpeiß</i>)
<i>RA Benjamin Stach, LL.M. (KCL)</i> Hamburg und Berlin	§ 11
<i>RA Robert Weinhold</i> Düsseldorf	§§ 24 bis 27
<i>Dr. Julia Zirfas, LL.M.</i> Kaden	§ 31
<i>Paul Zurawski</i> Universität Kassel	§ 33 (mit <i>Schaller/Hubert</i>)

Teil 1: Einleitung

§ 1 Das europäische Datenrecht

Literatur: *Dettling/Krüger*, Erste Schritte im Recht der Künstlichen Intelligenz, MMR 2019, 211; *Ebers/Steinrötter* (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021; *Fleisch/Mattern* (Hrsg.), Das Internet der Dinge, 2005; *Floridi/Taddeo*, What is data ethics?, Philosophical Transactions of the Royal Society A 2083/2016; *Geminn/Roßnagel*, „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts – ein Überblick, JZ 2015, 703; *Geminn*, Deus ex machina? – Grundrechte und Digitalisierung, 2023; *Gettler*, Is Justified True Belief Knowledge?, Analysis 1963, 121; *Hennemann*, Datenrecht, 2025; *Kühling/Sackmann*, Irrweg „Dateneigentum“, ZD 2020, 24; *Reinermann/von Lucke*, Speyerer Definition von Electronic Government, 2000; *Roßnagel*, Kein „Verbotsprinzip“ und kein „Verbot mit Erlaubnisvorbehalt“ im Datenschutzrecht, NJW 2019, 1; *Roßnagel/Geminn*, Vertrauen in Anonymisierung, ZD 2021, 487; *Steinrötter*, Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts, RD 2021, 480; *von Lucke/Reinermann*, Speyerer Definition von Electronic Government, 2000; *Zuboff*, A Digital Declaration, in: FAZ, 15.09.2014; *Zuboff*, The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power, 2019.

A. Datenrecht – Was ist das?	1	C. Zentrale (nicht-rechtliche) Definitionen des Datenrechts	19
B. Der lange Weg zum europäischen Datenrecht	10	D. Zu Aufbau und Zielen dieses Handbuchs ..	50

A. Datenrecht – Was ist das?

Der Begriff des Datenrechts hat sich in der rechtswissenschaftlichen Diskussion etabliert. Dies wird ua durch die Institutionalisierung seiner Beforschung belegt; ein Beispiel ist hier die Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech) e.V. Die Neue Juristische Wochenschrift hat sich bereits 2022 in einer Sonderausgabe dem „Neuen Digital- und Datenrecht“ gewidmet. Erste juristische Lehrbücher,¹ Sammelbände² und Buchreihen³ tragen den Begriff des Datenrechts im Titel. Aber was steckt eigentlich hinter dem Begriff? Welche Bereiche umfasst das Datenrecht? Und wie ordnet es sich in die Rechtsordnung ein? Hier gehen die Meinungen durchaus auseinander. Das Datenrecht kann eng oder weit verstanden werden. So kann es beispielsweise als Ergänzung des *Datenschutzrechts* gesehen werden oder als ein Überbegriff, der weit mehr erfasst als die Verarbeitung personenbezogener Daten, diese aber miteinschließt.

Klar zum Datenrecht gehörig sind jene Verordnungen, die die Europäische Kommission in der Folge des Geltungsbeginns der Datenschutz-Grundverordnung (DS-GVO)⁴ auf den Weg gebracht hat und die den Begriff Daten bereits im Kurztitel tragen: die Datenverordnung (Data Act, DA)⁵ und der Daten-Governance-Rechtsakt (Data Governance Act, DGA).⁶ Sie sind wiederum Teil eines Pakets von Verordnungen, dem auch das Gesetz über digitale Märkte (Digital Markets Act, DMA),⁷ das Gesetz über digitale Dienste (Data Services Act, DSA)⁸ und die Verordnung über künstliche Intelligenz (KI-Verordnung, KI-VO)⁹ angehören und die ebenfalls als dem Datenrecht zugehörig angesehen werden können. Die Inklusion von DMA, DSA und KI-Verordnung mag dabei vielleicht zunächst verwundern. Bei näherer Betrachtung finden sich jedoch in den drei Verordnungen zahlreiche Vorschriften, die sich klar dem Umgang mit Daten

1 ZB Hennemann, Datenrecht, 2025.

2 S. beispielhaft Specht-Riemenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2019.

3 So etwa die Reihe Datenrecht und neue Technologien im Nomos Verlag, deren erster Band 2021 erschien: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021.

4 VO (EU) 2016/679.

5 VO (EU) 2023/2854.

6 VO (EU) 2022/868.

7 VO (EU) 2022/1925.

8 VO (EU) 2022/2065.

9 VO (EU) 2024/1689.

1 § 1 Das europäische Datenrecht

zurechnen lassen – so etwa Art. 40 DSA, der mit „Datenzugang und Kontrolle“ überschrieben ist. Der DMA wiederum spricht vom Zugang zu großen Datenmengen als zentralem Faktor für wirtschaftliche Macht¹⁰ und von Daten als einem in der digitalen Wirtschaft entscheidendem Input.¹¹ Bezogen auf die KI-Verordnung spricht bereits der Kommissionsentwurf in seiner Begründung davon, dass Künstliche Intelligenz „häufig auf großen und vielfältigen Datensätzen“ beruhe und hebt die Bedeutung von hoher Datenqualität für KI-Anwendungen hervor.¹² Die für Hochrisiko-KI-Systeme geltenden Anforderungen sollen sich ausdrücklich auch auf Daten beziehen.¹³ Mit Art. 10 KI-VO ist eine eigene Vorschrift ganz Daten und Daten-Governance gewidmet. Die genannten Verordnungen sind somit sowohl direkt als auch indirekt im Kontext des Datenrechts relevant und dürfen als **Teilregelungen des Datenrechts** gelten, wenngleich sie (mitunter sogar schwerpunktmäßig) auch anderen Regulierungsbereichen zugehörig sind – etwa dem Verbraucherrecht, dem Produktsicherheitsrecht oder dem Wettbewerbsrecht.

- 3 Mit diesen fünf Rechtsakten versucht die Kommission, Korrekturen an der digitalen Marktwirtschaft vorzunehmen, aber auch klare Regeln zur Datennutzung in vielen Bereichen, wie etwa der Forschung, zu setzen. Klarer wird der Bezug, wenn man die digitale Marktwirtschaft als **Datenkapitalismus** begriff.
- 4 Das Datenrecht wird zutreffend als „**Querschnittsmaterie**“ charakterisiert, „dessen einendes Element das Regelungsobjekt Daten ist“.¹⁴ Andere verwenden mit Blick auf Data Act, Data Governance Act, Digital Markets Act, Digital Services Act und KI-Verordnung den Begriff des (Europäischen bzw. EU-)Datenwirtschaftsrechts. Dieses wird zB definiert als ein Teilrechtsgebiet, das sich auf „digitalisierte Informationen“ beziehe und neben dem Datenschutzrecht stehe.¹⁵ Damit wäre das Datenwirtschaftsrecht ein Teil des Datenrechts.¹⁶ Die Nomos Textsammlung Digitalrecht etwa trennt zwischen Datenrecht und Datenschutzrecht und fasst beide unter diesem Überbegriff zusammen.
- 5 Viel spricht für einen weiten und zugleich engen **Begriff des Datenrechts**, der explizit das Datenschutzrecht mit einbezieht, gleichzeitig aber auf die Modalitäten der Nutzung von Daten aller Art fokussiert bleibt. Dieser Begriff liegt diesem Werk zugrunde. In der Folge ist eine differenzierte Betrachtung erforderlich: Das Gesetz über digitale Märkte lässt sich – wie dargestellt – nicht in seiner Gesamtheit dem Datenrecht zurechnen; es enthält aber einzelne Regelungen, die zum Kernbestand des Datenrechts gehören. Aber auch bei dieser vermeintlich klaren Konkretisierung des Begriffs des Datenrechts bleiben an den Rändern Unschärfen und Überlappungen, so wie sie etwa auch zwischen dem Datenschutz und der Datensicherheit bestehen, die indes beide unter dem Dach des Datenrechts gefasst werden können und wohl auch sollten. Neben den genannten Verordnungen umfasst das Datenrecht jedenfalls auch weiteres Unionsrecht sowie viele mitgliedstaatliche Regelungen,¹⁷ die vielfach Rechtsakte der EU umsetzen, aber auch eigene Regelungsansätze enthalten. Beispiele unter vielen sind die Richtlinie über offene Daten,¹⁸ die Verordnung über den europäischen Gesundheitsdatenraum,¹⁹

10 S. ErwG 3 S. 2 sowie 59 S. 1 DMA. Zur Bedeutung von personenbezogenen Daten s. ErwG 36 DMA.

11 ErwG 3 S. 4 DMA.

12 COM(2021) 206 final, Begründung, 2.2 und 2.3. S. insbes. auch ErwG 44 KI-VO-KOM-E sowie ErwG 67 KI-VO.

13 COM(2021) 206 final, Begründung, 3.3.

14 Vorwort, in: Specht-Riemenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 5.

15 So Steinrötter RDt 2021, 480.

16 S. auch Gloy/Loschelder/Danckwerts WettbR-HdB/Becker § 64 Rn. 6: „Datenrecht setzt sich als Rechtsgebiet aus dem Schutz personenbezogener und dem (noch jungen) Schutz nicht-personenbezogener Daten zusammen. Da Daten vermehrt in wirtschaftlichem Zusammenhang relevant sind, ist seit wenigen Jahren auch vom Zweig des ‚Datenwirtschaftsrechts‘ die Rede.“

17 Wie etwa das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG; BGBl. I S. 1982; 2022 I S. 1045.

18 RL (EU) 2019/1024.

19 VO (EU) 2024/2847.

die NIS-2-Richtlinie²⁰ und weitere Rechtsakte aus dem Bereich Cyber-/IT/Datensicherheit. Sie sind so zahlreich, dass in diesem Handbuch nur ein nicht abschließender Überblick gegeben werden kann. DA, DGA, DS-GVO, DMA, DSA und KI-VO stellen dabei ohne Zweifel einen zentralen Kernbereich des Datenrechts dar – sie sind eine Art „Nukleus“ des Datenrechts. Ihnen ist dieses Handbuch deshalb schwerpunktmäßig gewidmet.

Durch die Regulierungsoffensive der Kommission bezogen auf den Umgang mit Daten im digitalen Binnenmarkt und darüber hinaus ist ein Dickicht entstanden, das nur schwer zu entwirren ist. Ein harmonisches Nebeneinander der zahlreichen Rechtsakte ist längst nicht immer gewährleistet. Ganz im Gegenteil stellen sich **Abgrenzungsfragen**, die nicht zuletzt auch gegenläufigen Zielsetzungen geschuldet sind. So stehen bereits die Grundsätze Datenminimierung und Speicherbegrenzung in einem natürlichen Konfliktverhältnis mit dem Ziel der Förderung von Datennutzung, das sich – wenn überhaupt – nur schwer auflösen lässt.

Bei einer Gegenüberstellung der Begriffe Datenrecht und Datenschutzrecht könnte unterstellt werden, dass die Verkürzung um den Begriffsteil „schutz“ nicht (nur) vor dem Hintergrund einer Erweiterung des Regelungsgegenstandes erfolgt ist, sondern gerade auch einen **Paradigmenwechsel** weg vom Schutz und hin zu einer umfassenden Nutzbarmachung von Daten einläuten soll. In der Folge würde das Datenschutzrecht von dem Stoppschild, als das es zumindest in der Praxis häufig wahrgenommen wird, zu einem vermeintlich gleichberechtigten Bestandteil unter dem Dach des Datenrechts; der Datenschutz erführe also eine Relativierung. Bei näherer Betrachtung ist das Datenschutzrecht aber ein Ermöglicher der Verarbeitung personenbezogener Daten, nicht sein Verhinderer: „Das Datenschutzrecht wird dadurch geprägt, dass es die Datenverarbeitung unter bestimmten, in den datenschutzrechtlichen Erlaubnistatbeständen genannten Bedingungen erlaubt.“²¹ Dementsprechend kann nicht von einem Paradigmenwechsel gesprochen werden, sondern ganz im Gegenteil von einer konsequenten Linie, die vom Datenschutzrecht zum Datenrecht führt und keine Relativierung des Datenschutzrechts zum Ziel hat, sondern seine Stärkung. Dennoch wird ein solcher Paradigmenwechsel in der im Rahmen der Diskussion um das Datenrecht verwendeten Rhetorik immer wieder behauptet – in den einzelnen Rechtsakten des Datenrechts und ihrem Zusammenwirken spiegelt er sich nicht wider. Im Datenrecht stehen sich somit gerade nicht Datenschutzrecht und ein „Datennutzungsrecht“ gegenüber. Der Begriff des Datenrechts darf ferner nicht verstanden werden als Ausdruck eines „Rechts an Daten“ im Sinne eines Ausschließlichkeitsrechts.²² Das Datenrecht ist das „Recht über Daten“ und nicht ein „Recht an Daten“.

Das Datenrecht schließt einerseits Lücken, die durch die ausschließliche Geltung des Datenschutzrechts für die Verarbeitung personenbezogener Daten entstanden sind; andererseits erweitert es aber auch die Regelungen des Datenschutzrechts um unterschiedlichste weitere zu beachtende Modalitäten. Ein zentraler Missstand ist allerdings nach wie vor nicht beseitigt: Es fehlt weiterhin an abstrakten und allgemeingültigen Regeln für den Umgang mit nicht personenbezogenen Daten.²³

Zusammenfassend muss festgestellt werden, dass eine Verkürzung des Datenrechts auf ein Datenwirtschaftsrecht zu kurz greift. Trotz der Fragmentierung des Datenrechts sollten die Rechtssetzungsaktivitäten der jüngeren Zeit als Chance genutzt werden, mit dem Datenrecht ein neues Rechtsgebiet fest zu etablieren, das einer gesamtheitlichen Behandlung des Umgangs mit jeder Form von Daten gewidmet ist.

20 RL (EU) 2022/2555.

21 S. Roßnagel NJW 2019, 1.

22 S. hierzu Kühling/Sackmann ZD 2020, 24.

23 S. Roßnagel/Geminn ZD 2021, 487.

B. Der lange Weg zum europäischen Datenrecht

- 10 Die Wurzeln des Datenrechts reichen zurück bis zu den ersten Regelungen zum Umgang mit Daten. Seine Anfänge können in den ersten Überlegungen zu den Wechselwirkungen zwischen moderner (Computer-)Technik und Recht in den 1950er Jahren gesehen werden, die wiederum mit der beginnenden Verbreitung von Großrechenanlagen einhergehen. Hervorzuheben ist ferner der Abschlussbericht der **Bangemann-Gruppe**, einer vom FPD-Politiker und Kommissar für Industriepolitik, Informationstechnik und Telekommunikation Martin Bangemann geleiteten Expertengruppe, aus dem Jahr 1994. Hier hieß es noch: „Die Schaffung der Informationsgesellschaft sollte dem privaten Sektor und den Marktkräften überlassen werden.“²⁴ Das Vertrauen in die Marktkräfte ist indes längst Vergangenheit; die hierin zum Ausdruck kommende Grundhaltung steht in einem klaren Gegensatz zu weiten Teilen des neuen Datenrechts.
- 11 Ein erster wichtiger Meilenstein für die Entwicklung des heutigen europäischen Datenrechts war die 2010 veröffentlichte **Digitale Agenda**.²⁵ Ihre eigenen Wurzeln reichen zurück zum Aktionsplan eEurope 2002 aus dem Jahr 2000.²⁶ Bereits vor der Vorstellung der Digitalen Agenda hatten die Arbeiten an der Datenschutz-Grundverordnung begonnen, die im Bereich des Datenschutzrechts eine unionsweite Harmonisierung erreichen wollte, die ihre Vorgängerin, die Datenschutzrichtlinie 95/46/EG, trotz entsprechender Bemühungen nicht bewirkt hatte. Ein wichtiger Trittstein auf dem Weg zur Datenschutz-Grundverordnung war die Mitteilung der Kommission zum Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert.²⁷ Hier steckte die Kommission öffentlichkeitswirksam den Rahmen der angestrebten Reform des EU-Datenrechts ab.
- 12 2014 veröffentlichte die Europäische Kommission dann die Mitteilung „Für eine florierende datengesteuerte Wirtschaft“²⁸ Darin griff sie Schlussfolgerungen des Europäischen Rats aus dem Oktober 2013 auf, in denen dieser „Rahmenbedingungen für einen Binnenmarkt für Big Data und Cloud-Computing“ forderte.²⁹ 2015 folgte die Strategie für einen digitalen Binnenmarkt für Europa;³⁰ 2017 die Mitteilung „Aufbau einer Europäischen Datenwirtschaft“³¹ Weitere wichtige Meilensteine waren ua:
- „Gestaltung der digitalen Zukunft Europas“;³²
 - „Conclusions on the Future of a highly digitised Europe beyond 2020“;³³ sowie die
 - „Berlin Declaration on Digital Society and Value-Based Digital Government“³⁴
- 13 Ein Jahrzehnt nach der Digitalen Agenda folgte schließlich die 2020 vorgestellte **Europäische Datenstrategie**.³⁵ Sie ruht auf vier Säulen: 1. Einem sektorübergreifenden Governance-Rahmen für Datenzugang und Datennutzung; 2. Investitionen in Daten und in die Stärkung der europäischen Kapazitäten und Infrastrukturen für das Hosting, die Verarbeitung und die Nutzung von Daten sowie der Interoperabilität; 3. der Stärkung der Handlungskompetenz des Einzelnen, Investitionen in Kompetenzen und in KMU; 4. gemeinsamen europäischen

24 Bangemann u.a., Europa und die globale Informationsgesellschaft, Empfehlungen für den Europäischen Rat v. 26.5.1994, S. 35; s. auch S. 30.

25 Eine Digitale Agenda für Europa, KOM(2010) 245 endg.

26 eEurope 2002, Eine Informationsgesellschaft für alle, Entwurf eines Aktionsplans, KOM(2000) 330 endg.

27 COM(2012) 9.

28 COM(2014) 442 final.

29 EUCO 169/13, S. 2.

30 COM(2015) 192 final. S. auch „Ein vernetzter digitaler Binnenmarkt für alle“, COM(2017) 228 final.

31 COM(2017) 9 final. S. auch das Begleitdokument SWD(2017) 2 final.

32 COM(2020) 67 final.

33 Ratsdok. 10102/19 v. 7.6.2019.

34 Erklärung v. 8.12.2020. In Anknüpfung an die „Tallinn Declaration“ (Ministerial Declaration on eGovernment) v. 6.10.2017.

Datenräumen in strategischen Sektoren und Bereichen von öffentlichem Interesse.³⁶ Zur Motivation führte die Kommission aus: „Digitale Technik hat in den letzten Jahren die Wirtschaft und Gesellschaft verändert und wirkt sich auf alle Tätigkeitsbereiche und das tägliche Leben aller Europäerinnen und Europäer aus. Daten stehen im Mittelpunkt dieses Wandels, und dies ist erst der Anfang. Die von Daten vorangetriebene Innovation wird den Bürgerinnen und Bürgern enorme Vorteile bringen, beispielsweise durch eine verbesserte personalisierte Medizin, durch eine neue Mobilität und durch ihren Beitrag zum europäischen Grünen Deal. In einer Gesellschaft, in der jeder Einzelne immer größere Datenmengen erzeugt, muss die Art und Weise, wie Daten gesammelt und verwendet werden, zuallererst den Interessen des Einzelnen entsprechen – ganz im Einklang mit den europäischen Werten, Grundrechten und Vorschriften. Die Bürgerinnen und Bürger werden sich nur dann auf datengetriebene Innovationen einlassen und ihnen Vertrauen entgegenbringen, wenn sie zuversichtlich sind, dass bei jeder Weitergabe personenbezogener Daten in der EU die strengen EU-Datenschutzvorschriften strikt eingehalten werden. Zugleich entsteht mit der zunehmenden Menge nicht personenbezogener industrieller und öffentlicher Daten in Europa in Verbindung mit den technologischen Veränderungen bei der Speicherung und Verarbeitung der Daten eine potenzielle Quelle für Wachstum und Innovation, die unbedingt genutzt werden sollte.“³⁷ Zielsetzung ist somit letztendlich nicht weniger als ein Ausgleich zwischen ökonomischen Interessen und durch Datenverarbeitung betroffenen Grundrechten sowie einfachgesetzlichen Schutzrechten. Wirtschaftspolitisches Ziel ist es dabei, dass bis zum Jahr 2030 „der Anteil der EU an der Datenwirtschaft (dh die in Europa gespeicherten, verarbeiteten wertschöpfend genutzten Daten) mindestens ihrem wirtschaftlichen Gewicht entspricht“.³⁸ Grundlage dafür soll „die Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarktes für Daten,“ sein, „der für Daten aus aller Welt offensteht, in dem sowohl personenbezogene als auch nicht personenbezogene Daten, darunter auch sensible Geschäftsdaten, sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten.“³⁹ Datenräume werden dabei auch sektorspezifisch geschaffen, so zB in den Bereichen Gesundheit und Mobilität.

Entsprechende gesetzgeberische Bemühungen sieht die Kommission in einer Linie mit der **Datenschutz-Grundverordnung**, die sie trotz deutlich älterer Regulierungsbemühungen selbst **als Ausgangspunkt** benennt.⁴⁰ Zudem benennt die Kommission die Verordnung über den freien Verkehr nicht personenbezogener Daten,⁴¹ den Rechtsakt zur Cybersicherheit⁴² und die Richtlinie über offene Daten⁴³ sowie bereichsspezifische Regelungen. 14

Daneben und ergänzend steht die Diskussion um die Regulierung von Künstlicher Intelligenz. **Meilensteine** sind hier ua:⁴⁴ 15

- Mitteilung der Europäischen Kommission, Künstliche Intelligenz für Europa, COM(2018) 237 final;

35 COM(2020) 66 final.

36 COM(2020) 66 final, 13 ff.

37 COM(2020) 66 final, 1.

38 COM(2020) 66 final, 5.

39 COM(2020) 66 final, 5.

40 COM(2020) 66 final, 4. Dabei wird das Datum 2014 genannt (und damit das Jahr der Verabschiedung der Verordnung durch das Europäische Parlament), wengleich die Entwicklungsgeschichte der Datenschutz-Grundverordnung bereits im Jahr 2010 beginnt (mit der Vorstellung des Gesamtkonzepts für den Datenschutz in der Europäischen Union, KOM(2010) 609 endg.).

41 VO (EU) 2018/1807.

42 VO (EU) 2019/881.

43 RL (EU) 2019/1024.

44 Für einen umfassenden Überblick über die Aktivitäten der Europäischen Union im Bereich Künstliche Intelligenz s. COM(2021) 205 final, Appendix 1.

1 § 1 Das europäische Datenrecht

- Koordinierter Plan für künstliche Intelligenz, COM(2018) 795 final;⁴⁵
- OECD Recommendation on Artificial Intelligence⁴⁶ mit ihren fünf „Principles for Responsible Stewardship of Trustworthy AI“ aus dem Mai 2019;⁴⁷
- G20 AI Principles;⁴⁸
- 2019–2020: Veröffentlichung der Deliverables der Hochrangigen Expertengruppe für künstliche Intelligenz (1. Ethics guidelines for trustworthy AI; 2. Policy and investment recommendations for trustworthy Artificial Intelligence; 3. Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment; 4. Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI);
- Ad Hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study, CAHAI(2020)23;⁴⁹
- Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final
- UNESCO Recommendation on the ethics of artificial intelligence, SHS/BIO/REC-AI-ETHICS/2;
- Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law als erstes verbindliches internationales Vertragswerk zum Thema KI.⁵⁰

Grundrechtliche Überlegungen stellen die Schlussfolgerungen zur Charta der Grundrechte im Zusammenhang mit künstlicher Intelligenz und dem digitalen Wandel aus dem Oktober 2020 an⁵¹ sowie bereits zuvor die Studie des Europarates „Algorithms and Human Rights“;⁵² Ebenfalls aus dem Oktober 2020 stammt eine Entschließung des Europäischen Parlaments zu „ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien“.⁵³ Das Parlament forderte hier eine Verordnung über ethische Grundsätze für die Entwicklung, den Einsatz und die Nutzung der genannten Technologien. Hier wurde bereits eine „erschöpfende und kumulative Liste von Bereichen sowie Verwendungen mit hohem Risiko, die das Risiko der Verletzung von Grundrechten und Sicherheitsvorschriften in sich bergen“, formuliert.⁵⁴

- 16 Zu den Bemühungen um die Regulierung von Künstlicher Intelligenz treten zahlreiche weitere **bereichsspezifische Aktivitäten** mit Relevanz für das Datenrecht, so zB:
- Europäische Cloud-Initiative;⁵⁵
 - Strategie für ein digitales Finanzwesen in der EU;⁵⁶
 - Die Cybersicherheitsstrategie der EU für die digitale Dekade;⁵⁷

45 Ein Review des Plans wurde 2021 zeitgleich mit dem Entwurf eines Artificial Intelligence Act vorgestellt; COM(2021) 205 final.

46 Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

47 Eine Aktualisierung erfolgte schließlich im Mai 2024. Die Definition von KI-Systemen in Art. 3 Nr. 1 KI-VO ist sehr eng an die hier vorgestellte Definition angelehnt.

48 G20 Ministerial Statement on Trade and Digital Economy v. 16. Juli 2019, Annex, S. 11.

49 Diese identifiziert die folgenden „key values, rights and principles“ als essenziell: Human dignity; Prevention of harm to human rights, democracy and the rule of law; Human Freedom and Human Autonomy; Non-Discrimination, Gender Equality, Fairness and Diversity; Principle of Transparency and Explainability of AI systems; Data protection and the right to privacy (ebd., S. 27 ff.).

50 CM(2024)52-final v. 17.05.2024. Zur Kritik an der Convention s. beispielhaft die Pressemitteilung des Europäischen Datenschutbeauftragten v. 11.05.2024. Insbesondere sei die Convention vornehmlich deklarativer Natur.

51 Ratsdok. 11481/20 v. 21. Oktober 2020.

52 Council of Europe study, DGI(2017) 12.

53 Legislative Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien (2020/2012(INL)).

54 S. den Anhang zum Verordnungsentwurf.

55 COM(2016) 178 final.

56 COM(2020) 591 final.

- Eine digitale Dekade für Kinder und Jugendliche: die neue europäische Strategie für ein besseres Internet für Kinder (BIK+);⁵⁸
- Strategische Vorausschau 2022 – Verzahnung des grünen und des digitalen Wandels im neuen geopolitischen Kontext⁵⁹ sowie die
- EU-Initiative für das Web 4.0 und virtuelle Welten: mit Vorsprung in den nächsten technologischen Wandel.⁶⁰

Vor allem aber hat die Kommission die 2020er Jahre im „2030 Digital Compass“ zum „**digitalen Jahrzehnt**“ erklärt und Ziele formuliert, die einen „europäischen Weg“ durch dieses Jahrzehnt weisen sollen.⁶¹ 2022 folgte die hier bereits angekündigte „Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade“.⁶² Dieses digitale Jahrzehnt ist auch das Jahrzehnt des europäischen Datenrechts. 17

Die **Motive** für das Tätigwerden des Gesetzgebers waren und sind dabei so vielfältig wie die 18 einzelnen (sich zudem noch überlappenden und verwobenen) Teilbereiche und -aspekte des Datenrechts. Sie reichen vom technischen Fortschritt und marktwirtschaftlichen oder gesellschaftlichen Dynamiken – ausgedrückt zB im Aufkommen neuer digitaler Dienstleistungen oder sozialer Phänomene (oft auch nur als Neufassung bekannter Phänomene) – bis hin zu weltpolitischen Ereignissen wie Krieg, Pandemie oder Wahlbeeinflussung. Zentrale Motive sind jedoch ohne Zweifel digitale Souveränität und Datensouveränität in Europa zu gewährleisten, einen europäischen und dritten Weg (neben den USA und der VR China) zu beschreiten und den Schutz der europäischen Grundrechte und -freiheiten zu gewährleisten. Um diese Ziele zu erreichen, muss vor allem Vertrauen durch effektive Rechtsetzung geschaffen werden. Daran muss sich das Datenrecht messen lassen.

C. Zentrale (nicht-rechtliche) Definitionen des Datenrechts

Jenseits der unzähligen Begriffsdefinitionen, die sich in den einzelnen Rechtsakten des Datenrechts finden und in den nachfolgenden Kapiteln ausführlich behandelt werden, werden in der Diskussion auch Begriffe verwendet, die entweder ohne rechtliche Definition bleiben oder deren rechtlichen Definitionen andere Definitionen zur Seite gestellt werden (oder diesen vorausgingen). Einige ausgewählte Definitionen ohne rechtliche Bindungswirkung sind im Folgenden aufgeführt. 19

Big Data – „consists of extensive datasets – primarily in the characteristics of volume, velocity, variety, and/or variability – that require a scalable architecture for efficient storage, manipulation, and analysis.“⁶³ 20

Blockchain – „ein verteiltes Register, in dem digitale Datensätze, Ereignisse oder Transaktionen in chronologischer Reihenfolge für alle Teilnehmer nachvollziehbar in Datenblöcken gespeichert („Block“) und unveränderbar miteinander verkettet („Chain“) werden.“⁶⁴ 21

Corporate Digital Responsibility – „freiwillige unternehmerische Aktivitäten, die über das heute gesetzlich vorgeschriebene hinausgehen und die digitale Welt aktiv zum Vorteil der Gesellschaft mitgestalten“.⁶⁵ 22

57 JOIN(2020) 18 final.

58 COM(2022) 212 final.

59 COM(2022) 289 final.

60 COM(2023) 442 final.

61 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final.

62 COM(2022) 28 final.

63 NIST Big Data Interoperability Framework: Volume 1, Definitions, NIST Special Publication 1500-1r2, Version 3, S. 10.

64 Bundesnetzagentur, Die Blockchain-Technologie – Grundlagen, Potenziale und Herausforderungen, 2021, S. 5.

65 BMJV, CDR-Initiative, S. 3.

1 § 1 Das europäische Datenrecht

- 23 **Data asset/Datenbestand** – „A data asset is any collection of data, any data set or any information that is somehow linked, e.g. by common codes or metadata, which has been created by the Commission, collected from Member States or other stakeholders, or acquired from third parties in the context of projects, policy or administrative processes. Data assets may be structured or unstructured, static or dynamic, raw or curated. Data assets are in digital formats.“⁶⁶
- 24 **Data policies/Datenrichtlinien** – „Data policies are a set of broad, high level principles which form the guiding framework in which data assets [...] can be managed. More specifically, data policies govern data management, data interoperability and standards, data quality, data protection and information security.“⁶⁷
- 25 **Daten** – „Der Begriff ‚Daten‘ versammelt eine immense Diversität von Erscheinungsformen unter einem Begriffsdach. So lassen sich Daten etwa anhand des Datentyps (zB binäre, nominale, ordinale, metrische und textuelle Daten), des datengenerierenden Prozesses (zB Umfragedaten, Sensordaten), des Erhebungsbereichs (zB Finanzdaten, Wetterdaten) oder ihrer Funktion in einem digitalen System (zB Log-in-Daten, Trainingsdaten) einteilen. Eine weitere Einteilung setzt am Grad der Verarbeitung (Veredelung) an: Ohne eine weitere Verarbeitung spricht man auch von ‚Rohdaten‘; je nach dem Grad der Strukturierung (Normalisierung) von ‚strukturierten‘ oder ‚unstrukturierten‘ Daten. Daten können der Input in ein System sein oder auch der Output, der wiederum der Input in das nächste System sein mag. Daten können zugleich digitale Vermögensgüter (digital assets) repräsentieren, wie multimediale Inhalte oder Einheiten von Kryptowährungen.“⁶⁸
- 26 **Datenethik** – „branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions (e.g. right conducts or right values)“⁶⁹
- 27 **Datengovernance** – „A set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority and management and decision making parameters related to the data produced or managed by the enterprise.“⁷⁰; „Data governance entails defining, implementing and monitoring strategies, policies and shared decision-making over the management and use of data assets.“⁷¹
- 28 **Datenraum** – „Eine föderierte, offene Infrastruktur für souveränen Datenaustausch, die auf gemeinsamen Vereinbarungen, Regeln und Standards beruht.“⁷²
- 29 **Datenschutz** – „Datenschutz ist die Gesamtheit von Regeln, Institutionen und Maßnahmen, um die informationelle Selbstbestimmung der Bürger zu schützen. Er schützt nicht die Daten (des Datenverarbeiters), sondern die Grundrechte der von einer Datenverarbeitung ‚betroffenen Person‘ (gegen den Datenverarbeiter).“⁷³

66 European Commission, Data governance and data policies at the European Commission, Juni 2020, S. 7.

67 European Commission, Data governance and data policies at the European Commission, Juni 2020, S. 6.

68 Gutachten der Datenethikkommission, 2019, S. 52.

69 Floridi/Taddeo, *Philosophical Transactions of the Royal Society A*, 374(2083), 2016, S. 3.

70 Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, S. 41 unter Verweis auf NSA/CSS Policy II-1.

71 European Commission, Data governance and data policies at the European Commission, Juni 2020, S. 6.

72 Reiberg/Niebel/Kraemer, Was ist ein Datenraum? – Definition des Konzeptes Datenraum, Gaia-X Hub Germany, White Paper 1/2022.

73 Roßnagel, Datenschutz, in: Andersen/Gobumil/Marschall/Woyke (Hrsg.), *Handwörterbuch des politischen Systems der Bundesrepublik Deutschland*, S. 172–177 (172).

- Datensicherheit** – „Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist ‚Informationssicherheit‘.“⁷⁴ 30
- Datenwirtschaft** – „The Data Economy measures the overall impacts of the data market on the economy as a whole. It involves the generation, collection, storage, processing, distribution, analysis elaboration, delivery, and exploitation of data enabled by digital technologies. The data economy also includes the direct, indirect, and induced effects of the data market on the economy.“⁷⁵ 31
- Desinformation** – „all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit“⁷⁶ 32
- Digital Single Market/digitaler Binnenmarkt** – „A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. Achieving a Digital Single Market will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally.“⁷⁷ 33
- Digitalisierung** – „Unter dem Begriff der Digitalisierung werden unterschiedliche Phänomene zusammengefasst, die zumeist aus technologischen Entwicklungen im Umfeld von Computern und Datennetzen resultieren. Grundlegend wird dabei von der Umwandlung analoger Informationen in verschiedene digitale Formate ausgegangen, wobei nicht allein die kommunikative Dimension („digitale Medien“) relevant ist, sondern zunehmend auch Produktion und Distribution immaterieller Güter, die Prozessierung großer Datenmengen sowie die Entwicklung und der Einsatz von Algorithmen eingeschlossen werden.“⁷⁸ 34
- E-Government** – „Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien“⁷⁹ 35
- Fake News** – „absichtlich falsche Nachrichten, die eigens zum Zweck der viralen Verbreitung über das Internet und soziale Netzwerke produziert wurden“ mit dem Ziel „die Öffentlichkeit für bestimmte politische und/oder kommerzielle Zwecke zu manipulieren“⁸⁰ Der Begriff wird jedoch vielfach abgelehnt;⁸¹ stattdessen findet der Begriff der Desinformation Verwendung.⁸² 36
- Hate Speech** – „The term encompasses a wide array of hateful messages, ranging from offensive, derogatory, abusive and negative stereotyping remarks and comments, to intimidating, inflammatory speech inciting violence against specific individuals and groups. Only the most egregious forms of hate speech, namely those constituting incitement to discrimination, hostility and violence, are generally considered unlawful.“⁸³ 37

74 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, 2023, Glossar, S. 2.

75 European Data Market, SMART 2013/0063, 2017, S. 123.

76 A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation, März 2018, S. 3.

77 A Digital Single Market Strategy for Europe, COM(2015) 192 final.

78 Bieber, Digitalisierung, in: Andersen/Gobumil/Marschall/Woyke (Hrsg.), Handwörterbuch des politischen Systems der Bundesrepublik Deutschland, S. 234–240 (234).

79 Von Lucke/Reinermann, Speyerer Definition von Electronic Government, 2000, S. 1.

80 Fake News, Definition und Rechtslage, WD 10 – 3000 – 003/17, 6.

81 S. beispielhaft House of Commons, Digital, Culture, Media and Sport Committee, Disinformation and „fake news“, S. 2. S. auch HC 1791 v. 18.2.2019.

82 S. beispielhaft A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation, März 2018, S. 3 sowie COM(2018) 236 final.

83 Report of the Special Rapporteur on minority issues, A/HRC/28/64, UN Human Rights Council.

1 § 1 Das europäische Datenrecht

- 38 **Industrie 4.0** – „bezeichnet die sog. vierte industrielle Revolution auf der Basis cyber-physischer Systeme (intelligente technische Systeme aus der Elektronik, Softwaretechnologie, Informationssysteme, Mechatronik). Demgegenüber fußt die erste industrielle Revolution auf der Nutzung von Dampfmaschinen und der Einführung mechanischer Produktionsanlagen am Ende des 18. Jahrhunderts, die zweite industrielle Revolution ua auf dem Einsatz elektrischer Energie, die Massenproduktion erlaubte. Die dritte industrielle Revolution wird durch den umfangreichen Einsatz von Elektronik und Informationstechnologie (IT) zur weitreichenden Automatisierung charakterisiert.“⁸⁴
- 39 **Information** – „Information ist Wissen in Aktion und Kontext.“⁸⁵ (informationswissenschaftliche Definition)
- 40 **Informations- und Kommunikationstechnologie (IKT)** – „Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).“⁸⁶
- 41 **Internet of Things** – „Vision einer Welt smarterer Alltagsgegenstände, welche mit digitaler Logik, Sensorik und der Möglichkeit zur Vernetzung ausgestattet ein ‚Internet der Dinge‘ bilden, in dem der Computer als eigenständiges Gerät verschwindet und in den Objekten der physischen Welt aufgeht“⁸⁷
- 42 **Kleine und mittlere Unternehmen** – „Die Größenklasse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.“⁸⁸
- 43 **Künstliche Intelligenz** – „Systeme mit einem ‚intelligenten‘ Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen“⁸⁹
- 44 **Metaverse** – „The term ‚Metaverse‘ stems from Neal Stephenson’s 1992 novel Snow Crash, and describes a collective virtual shared space that’s created by the convergence of virtually enhanced physical reality and persistent virtual space. In its fullest form, the Metaverse experience would span most, if not all virtual worlds, be foundational to real-world AR experiences and interactions, and would serve as an equivalent ‚digital‘ reality where all ‚physical‘ humans would simultaneously co-exist. It is an evolution of the Internet. More commonly, the Metaverse is understood to resemble the world describe by Ernest Cline’s Ready Player One.“⁹⁰
- 45 **Smart Contract** – „a computerized transaction protocol that executes the terms of a contract“⁹¹
- 46 **Suchmaschine** – „Online-Index von Dokumenten und Bildern, die auf mit dem weltweiten Internet verbundenen Computern veröffentlicht und gespeichert sind. Diese Suchindizes werden

84 Deutscher Bundestag, Wissenschaftliche Dienste, Aktueller Begriff Nr. 23/16 (26.9.2016), S. 1.

85 Kühlen, Information – Informationswissenschaft, in: Kühlen/Semar/Strauch (Hrsg.): Grundlagen der praktischen Information und Dokumentation, S. 1 (4).

86 Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, S. 62 unter Verweis auf DoDI 5200.44.

87 Fleisch/Mattern, Vorwort, in: Fleisch/Mattern (Hrsg.), Das Internet der Dinge, 2005.

88 Empfehlung der Kommission vom 6.5.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, Art. 2 Abs. 1.

89 Hochrangige Expertengruppe für Künstliche Intelligenz, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete, S. 1 unter Bezugnahme auf COM(2018) 237 final; zur Kritik an der gewählten Definition s. beispielhaft Dettling/Krüger MMR 2019, 211 (211 f.).

90 Ball, Fortnite Is the Future, but Probably Not for the Reasons You Think, Blogbeitrag v. 5.2.2019 (matthewball.vc).

91 Szabo, Smart Contracts, 1994.

Stichwortverzeichnis

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

- Abgrenzung zu Inhalten **24** 25
Abhilfe **18** 14
Abrechnungsinformationen **3** 44
Abschlusszeugnis **30** 55
Abwägung **33** 77, **35** 38 f.
Abwehrrecht **36** 16
Acces by Design **23** 17, **33** 97
Accessibility
– by Default **34** 7
– by Design **34** 7
Achtung des Privat- und Familienlebens **6** 6
Adressat **16** 7
AGB **17** 18, **22** 78, **40** 20
– Transparenzpflichten **17** 10
Agencification **5** 2 ff.
Agentur der Europäischen Union für Cybersicherheit (ENISA) **27** 12
Aggregierte Daten **23** 32
AI Act **5** 52 ff., **28** 1 ff.
AI literacy **28** 57
Akkreditierung **33** 107
Akteure **5** 2 ff.
Akzeptanz **22** 58 ff.
Algorithmen **35** 91 ff.
All-Gefahren-Ansatz **33** 65
Allgemeine Bereitstellungsregelung **19** 41
Allgemeines Persönlichkeitsrecht **35** 38 f.
Allgemeine Versicherungsbedingungen (AVB) **33** 121
Allgemeininteresse **20** 138
Allgemeinverfügung **39** 158 f.
Altersverifikation, Datenminimierung **32** 39 ff.
Amtsermittlung **39** 52
Amtsgericht **39** 12 f.
Analysedienst **21** 24
Anbieter **24** 41, **34** 51
Anbieterkennzeichnung **22** 41
Anerkennung **29** 14, **30** 34, 55
– Anerkennungspflicht **29** 33 ff.
– Freiwilligkeit **22** 29
Anfechtungsklage **21** 77
– Einspruchsverfahren **39** 49
Angemessenheit von Datensicherheitsmaßnahmen **33** 74 ff.
Anmeldeverfahren **21** 39 ff.
– DGA **10** 30
Anonyme Daten **3** 78 ff.
Anonymisierung **3** 68 ff., 81 ff., **10** 19, **19** 39, **21** 85, **36** 22
Anonymität **29** 43, **30** 70
Anreize **21** 89
– zum Datenteilen **23** 40
Ansprechpartner, Datenschutzbeauftragter **22** 41
Anspruch, subjektiver **20** 88 f.
Anspruchsgrundlage **20** 93 f., 98, 106
Anspruchsverpflichteter **20** 112
Antrag **20** 33, 166 f.
Antragserfordernis **22** 41
Antragsverfahren **24** 61
An- und Abmeldeverfahren **21** 68 ff.
Anwaltsprozess, Prozessvertretung **39** 20
Anwendungsbereich **21** 8, 25 ff.
– persönlicher **20** 48, **21** 26 ff., **24** 40
– räumlicher **15** 13, **21** 36, **24** 40
– sachlicher **15** 14, **20** 53, **21** 26 ff.
– zeitlicher **21** 37
Anwendungsprogrammierschnittstellen (API) **20** 98
Anwendungsvorrang **21** 81
Anzeigepflicht **21** 39
Arbeitsgericht **39** 31 ff.
– Beschlussverfahren **39** 35
– Gebühren **39** 33
– Güteverfahren **39** 34
Arbeitskollektivrecht **35** 37
Arbeitsrecht **33** 101
Archivierung **30** 14
Archivierungsdienste **30** 57 ff.
Artificial Intelligence Act
– CSA-Zertifizierung **33** 56
– technische Lösungen **33** 54 ff.
Attribute **29** 23, **30** 27
Attributsbescheinigung **29** 22, **30** 54 ff., 65, 74
Attributsdaten **30** 56
Aufbewahrung **30** 57
– Bußgeldbewehrung **14** 124 f.
Auffinden, Selbstbevorzugungsverbot **14** 82 f.

Stichwortverzeichnis

- Aufgaben 21 67 ff.
Aufgabenerfüllung 20 58
Aufsichtsbehörde 22 62, 32 104, 35 120 ff.
– Benehmen 39 131
– Beteiligtenfähigkeit 39 70 f.
– Bundesnetzagentur 39 110
– Data Act 39 129
– eIDAS 30 8
– Einvernehmen 39 131
– Ermessensentscheidung 39 87 ff.
– loyale Zusammenarbeit 39 130
– Schutzniveau 39 93
Aufsichtskooperation 30 36
Aufsichtsmaßnahme 33 118
Aufsichtsmechanismus 21 57 ff.
Aufsichtsrecht 35 120 ff.
Auftragsverarbeitung 11 5
– Cloud Computing 18 18
– Weisungs- und Kontrollrecht 18 18
– Zertifikat 18 20
Auftragsverarbeitungsvertrag 11 8
Aufzeichnungspflicht, Transparenz 22 44
Augenscheinsbeweis 30 63
Auschluss 35 53
Auskunftsexzess 35 28 ff.
Auskunftsform 35 24 f.
Auskunftsmodalitäten 35 22 ff.
Auskunftsrecht 35 16 ff.
Auskunftsrechtsbeschränkung 35 34 ff.
Auskunftsverpflichtungen 31 45
Auskunftsverweigerung 22 68, 35 28 ff.
Auslegung 22 60
Ausnahme 20 59, 113 ff.
Ausschließlichkeitsvereinbarung 20 36, 74 ff., 131, 135, 137 f., 142
Ausschlussstatbestand 20 30
Ausschuss für digitale Dienste 5 24 f.
Außergewöhnliche Notwendigkeit 25 55 f.
Aussteller 29 25
Ausstellung 30 10 f.
Authentifizierung 29 13
Authentische Quelle 30 65
Automatisierte Entscheidungsfindung 35 21 f., 91 ff.
– Konflikt mit KI-VO 32 98
Automatisiertes Auskunftsverfahren 31 48 ff.
Automatisiertes Verfahren 35 52
Automatisierte Verarbeitung 35 91 ff.
B2B-Data Sharing 23 28
Backup 33 70, 85, 87 ff.
Bangemann-Gruppe 110, 15 5
BDI 211
Beantwortungsfristen 35 26 f.
Bedingung 20 121
Bedingungslosigkeit 20 35
Befugnisse 5 1 ff.
– behördliche 21 71 ff.
Behörde 35 120 ff.
– Behördenauskunfts 35 120 ff.
– Behördenkooperation 21 66, 73
– Behördenpersonal 21 62
– Behördenprinzip 39 74
– Behördenstruktur, Kompetenzkonflikt 22 61 ff.
Beihilferecht 20 161
Beiladung 39 82 ff.
– Beschluss 39 84 f.
– einfache 39 81
– notwendige 39 81, 83
Belgien 6 27 f.
Benachrichtigungspflicht 33 110 ff.
– Anweisung durch die Behörde 37 70
– Auftragsverarbeiter 37 65
– Folgen 37 72
– Form 37 67, 69
– Frist 37 66
– Inhalt 37 69
– Meldung an Behörde 37 63
– öffentliche Bekanntmachung 37 62, 68
– Verantwortlicher 37 64
– Verstoß 37 73
– Voraussetzung 37 59 ff.
Benennung
– Aussetzung 14 60
– Befreiung 14 60
– Benannte Torwächter 14 46
– Benennungsbeschluss 14 43
– Billigkeit 14 56
– Einfang- oder Allgemeinklausel 14 38
– Erreichen von Schwellenwerten 14 40
– Marktuntersuchung 14 49 ff.
– Mitteilungsinhalte 14 39
– Widerlegung 14 45, 56
– Zuständigkeit 14 35
Benennungsbeschluss
– Folgen 14 55
– Inhalt 14 55
Benutzerschnittstelle 34 20
Bereisung von Datensätzen 23 44

- Beratung 5 59 f.
Berechtigtes Interesse 7 12, 16, 32 71, 35 82
Bereichsspezifische Bereitstellungspflicht 19 42
Bereitstellung 20 38
– Ansprüche 25 28
– Modalitäten 20 94
– öffentliche 20 57
Bereitstellungspflicht 20 53 ff., 24 58
– allgemeine 20 56
– gesetzliche 20 55
Bereitstellung von Daten 19 40, 20 93, 25 30
– Produktdaten, Dienstdaten, öffentliche Stellen 24 5
Berichtigung 35 62 ff.
Berichtspflicht 22 42 ff.
Berufsfreiheit 6 12
Berufsstatus 30 54
Beschäftigtenexzess 40 7
Beschränkung der Verarbeitung 35 77
Beschränkungen 35 34 ff.
– für Dateninhaber 24 69
– Recht auf Kopie 35 47
Beschwerderecht 19 34, 21 76, 22 81 ff.
Bestandsdaten 31 20
Best-Effort-Prinzip 31 39
Bestreitbarkeit, Definition 13 19
Bestreitbarkeit und Fairness 14 17
Beteiligtenfähigkeit 39 70 ff.
Betriebsdaten 3 33
Betriebs- und Geschäftsgeheimnis 34 36
Betroffenenrechte 21 32, 53, 80, 34 34 f.
– Konflikt mit KI-VO 32 88 ff.
Betroffene Person 3 85, 21 12, 35 18 f., 63
– Cloud Computing 18 22 ff.
– KI-VO 32 99
– Rechte 11 6 f.
Bewahrung 30 10, 14
Bewahrungsdienst 30 46
Beweislast 39 23 ff.
Beweismittel 30 19, 63
Beweisvermutung 30 67 ff.
Bezahlen mit Daten 9 64
Bias 3 32
Big Data 1 20, 7 3
– Anwendungen 7 12 f., 19
Big Five 9 22
Big-Tech
– Brechung der Dominanz 12 3
– eigenes Ökosystem 12 2
– Selbstbevorzugung 13 9 ff.
Bildung, digitale 7 16
Bildungseinrichtung 20 115
Billigkeit, Prüfung 14 57
Binnenmarkt, digitaler 1 33
Binnenmarktintegration 30 34
Biometrie
– Transparenz 28 125, 128
– Verbote 28 72 ff.
Biometrische Daten 3 24
Blockchain 1 21
BNetzA 31 18
– Marktüberwachungsbehörde 28 141
Branchenverband 33 108
Brieftasche 29 6, 18 ff., 30 6
Broad Consent 7 13
Broad Network Access 18 5
Browser 30 53
Browser-Plug-In 21 24
BSI-Gesetz 40 52
Bulgarien 6 29 f.
Bundeskartellamt 39 137
– Beschwerde 39 138
Bundesnetzagentur 5 26 f., 22 8, 39 110, 156
– DSA 39 153
– Marktüberwachungsbehörde 39 168
Bundeszentrale für Kinder- und Jugendmedienschutz 39 155
Büro für Künstliche Intelligenz 5 55 f.
Bürokratie 22 60
Bußgeld 22 66, 85 f.
– Adressat 40 6 f.
– Berechnung 40 5
– DS-GVO 40 4 ff.
– Höhe 40 4 ff.
– öffentliche Stelle 40 8
– Perspektive 14 145
– Spürbarkeit 14 144
Buy-out-Vertrag 23 28
By Design 34 17
– Datenzugang 34 5 ff.
Caching 15 16, 18 7 ff.
– Privilegierung 16 14 f.
Charta der Grundrechte der Europäischen Union 6 1 ff.
ChatGPT/Chatbot 9 10, 28 6, 25, 126
Chilling Effects 4 18
Clearview AI 28 72
Cloud 9 7

- Cloud Computing 27 4
 - Auftragsverarbeitung 18 18
 - Bereitstellungsmodell 18 5 ff.
 - Bestands- und Nutzungsdaten 18 21
 - Betroffenenrechte 18 25
 - Betroffene Person 18 22 ff.
 - Data Act 18 28 ff., 34 19
 - Datenportabilität 18 25
 - Datenschutzrecht 18 16 ff.
 - Datenverarbeitung 18 6
 - Definition 18 6
 - DGA 18 33
 - DMA 18 34 ff.
 - Drittlandtransfer 18 26 ff.
 - DSA 18 8 ff.
 - gemeinsame Verantwortliche 18 21 ff.
 - Geschäftsmodelle 18 5 ff.
 - Haushaltsausnahme 18 22 ff.
 - Hosting 18 8 ff.
 - Inhaltsdaten 18 22 ff.
 - Mittelstand 18 1
 - Nutzungsvertrag 18 23
 - Outsourcing 18 18
 - Paradigma 18 1
 - Quasi-Auftragsverarbeiter 18 24 f.
 - Rechtsfragen 18 2
 - Rollen 18 18
 - Server 18 6
 - Service Model 18 6
 - Verantwortlicher 18 21 ff.
 - Vermittlungsdienst 18 8 ff.
 - Weisungs- und Kontrollrecht 18 18
 - Zertifikate 18 20
- Cloud-Diensteanbieter 27 2
- Cloud-Speicher 21 24
- Cloud Switching 18 30, 27 1
- Cloud-Technologie 9 45
- Code, Software 15 3
- Compliance 11 44 ff.
- Compliance-Einrichtung
 - Ansiedelung 14 130
 - Aufgaben 14 131
 - Ausstattung und Zugang 14 128
 - Bekanntgabe 14 132
 - Bußgeldbewehrung 14 133
 - Schutz 14 130
 - unabhängige Führungskraft 14 129
 - Unabhängigkeit von operativen Funktionen 14 127
- Computer Security Incident Response Team (CSIRT) 33 117
- Cookie-Richtlinie 32 12
- Co-Regulierung 33 102 ff.
- Corporate Digital Responsibility 1 22
- Crawling, Selbstbevorzugungsverbot 14 82 f.
- Creative Commons 20 67
 - BY 4.0 20 45
 - Public Domain Dedication 20 45
- Cybersicherheit 33 7
 - Anforderungen 30 20
 - Begriff 33 7
- Cyber-Versicherung 33 121
- Dänemark 6 31
- Dark Pattern 17 20, 24 64, 32 33 f., 103
 - Einwilligung 32 34
 - Verhältnis zur DS-GVO 32 34
- Daseinsvorsorge 19 4, 9
- Data Access by Design 24 30
- Data Accessibility 34 5
 - by Design 24 50
- Data Act (DA) 7 33, 10 4 ff., 11 10 ff., 21 2, 83 ff., 22 12, 35 3, 39 107, 121 ff.
 - Abgrenzung 40 23 ff.
 - Anwendungsbereich 40 16
 - Aufsicht 40 17
 - Aufsichtsbehörde 39 129
 - berechtigte Interessen 32 71
 - besondere Kategorien personenbezogener Daten 32 72
 - Betroffenenbeschwerde 39 132
 - bisherige Rechtslage 40 20 ff.
 - Cloud Computing 18 28 ff.
 - Datenflüsse 38 9
 - Dateninhaber 39 122
 - Datenschutzaufsichtsbehörde 39 125, 40 17
 - Datenübertragbarkeit 32 67
 - Datenzugangsansprüche 32 67
 - DS-GVO 40 18, 23 ff.
 - Durchsetzung 40 14 ff.
 - Erfüllung einer rechtlichen Verpflichtung 32 70
 - Europäischer Datenschutzbeauftragter 40 19
 - Informationspflichten 32 64
 - Intelligente Verträge 33 27
 - Konfliktfall 32 63
 - Löschen 40 26

- nationaler Regelungsauftrag 40 14 ff.
- Personenbezug 32 74 ff.
- private enforcement 40 27
- Profiling 32 77 ff.
- Rechtsgrundlagen 32 68 ff.
- Rechtsunsicherheit 40 25 f.
- rechtsverbindliche Entscheidung 39 126
- Regelungsauftrag 40 15
- Sanktion 40 14 ff.
- Sanktionierung 40 13 ff.
- unfaire Vertragsklauseln 11 16
- Unterrichtung 39 133
- Verhältnis zur DS-GVO 32 62 ff., 33 23, 40 24 ff.
- Verwaltungsrechtsweg 39 124
- Vorverfahren 39 128
- Widerspruchsverfahren 39 127
- Zugangsrecht 32 65 f.
- Data Act-Durchführungsgesetz-Entwurf 40 14
- Database-as-a-Service 27 11
- Data Governance Act (DGA) 7 31, 10 4 ff., 11 18 ff., 19 1 ff., 16 ff., 20 1 ff., 23 48, 25 49, 32 44 ff., 35 3, 39 107 ff.
- Aufgabe im öffentlichen Interesse 32 50
- Bußgeldberechnung 40 31
- Cloud Computing 18 33
- DS-GVO 40 35
- Einwilligung 32 54 f.
- Erleichterung des Datenaustauschs 32 59
- Formatänderung bereitgestellter Daten 32 58
- Informationspflichten 32 60
- Konfliktfall 32 45
- Rechtsbehelfe 39 108
- Rechtsgrundlage 32 46
- Rechtspflicht 32 51
- Rechtsschutz 39 119
- rechtsverbindliche Entscheidung 39 111
- Rechtsweg 39 114
- Regelungsauftrag 40 29, 36
- Sanktionierung 40 28 ff.
- sichere Verarbeitungsumgebung 33 34
- unparteiische Stelle 39 115
- Verbesserung der Interoperabilität 32 58
- Verhältnis zur DS-GVO 32 44 ff., 58, 60
- Weiterverwendung von Daten durch öffentliche Stellen 32 47 ff.
- zuständige Stelle 32 56
- Zweckänderung 32 49
- Data Governance Act-Sanktion 40 28 ff.
- Data Mining 2 13 ff.
- Dateisystem 3 17
- Daten 1 25, 20 53, 109 ff., 114 ff., 118, 123
 - Akteure 3 84 ff.
 - als Produkt 9 49
 - analoge 3 13
 - anonyme 3 68, 36 20, 22
 - aus informatischer Sicht 2 1 ff.
 - Authentizität 16 19
 - Begriffsbestimmung 3 11 ff.
 - besondere Kategorien 3 18, 36 29
 - Big Data 9 6 ff.
 - biometrische 3 24, 27
 - Data Act 32 64
 - Datennutzer 3 89
 - Definition 32 64
 - deliktischer Schutz 3 96
 - Dienstdaten 34 18
 - digitale 3 13
 - DS-GVO 32 64
 - dynamisch, hochwertig 20 91
 - Eigentum 3 106
 - Eingabedaten 3 30
 - Endkunden 3 45
 - Energie 3 43
 - Format 34 23
 - Forschung 36 1 ff.
 - geistiges Eigentum 6 21
 - genetische 3 25, 36 8
 - Geodaten 3 42
 - geschützt, offen 19 2
 - geschützte 20 108
 - Innovation 34 2
 - Integrität 3 96
 - maschinelle 3 100
 - Metadaten 3 14, 34 18
 - Muster 36 2
 - neue 36 1
 - nicht personenbezogene 3 77 ff., 11 2 ff., 21 48 ff., 88
 - Nutzer 3 86
 - Nutzung 20 62 ff.
 - objektbezogene 3 80
 - offene 20 18
 - ohne Weiteres verfügbare Daten 24 60
 - personenbezogene 3 15, 47 ff., 11 2 ff., 21 31, 80 ff., 88
 - Produktdaten 3 14, 34 18
 - Pseudonym 3 63

Stichwortverzeichnis

- Rechte an 3 95 ff.
- Sachdaten 3 80
- Sammlung 16 20
- sensible operative 3 28
- Speicherung 2 4
- Standortdaten 3 41
- Straftaten 3 22
- Testdaten 3 31
- Trainingsdaten 3 31
- Trends 36 2
- Treuhand 34 38
- Überlassungsvertrag 3 98
- Urheberrecht 3 100
- Validierungsdaten 3 31
- Verkehrsdaten 3 40
- Vermittlungsdienst 3 90
- Verurteilungen 3 22
- Wertschöpfung 34 2
- Zahlungsdaten 3 39
- Zugang 34 2 ff.
- Zugriff 34 2 ff.
- Datenaggregation 23 7
- Datenakkumulation
 - eigene Dienste 13 40
 - Prädiktion 13 40
- Datenaltruismus 7 16, 31, 19 20 ff., 20 138, 21 23, 22 1 ff.
 - Legaldefinition 22 15 ff.
- Datenaltruismus-Organisationen 11 19
- Datenaltruistische Organisation 5 32 ff., 19 28, 39 109
 - Benachrichtigungspflicht 33 111
- Datenaltruistische Person 19 39
- Datenaltruistische Tätigkeit 22 36
- Datenanalyse 9 38
- Datenarten 24 8
- Datenaufbereitung 23 3
- Datenaustausch 11 18 ff.
 - grenzüberschreitender 11 56 f.
- Datenbank 3 102 ff.
- Datenbankhersteller 20 61
- Datenbankschutzrecht 25 15
- Datenbefähiger 9 35
- Datenbegriff 24 11, 35 57
- Datenbereinigung 9 38
- Datenbereitsteller 19 13, 20 48 ff., 81, 89, 91 ff., 96
- Datenbereitstellung durch Hersteller 24 24
- Datenbereitstellungsverlangen 25 57
- Datenbesitz 3 107
- Datenbestand 1 23, 19 18
- Datenbezogene Infrastrukturlösungen 9 51
- Datenbörsen 23 51
- Datenbroker 21 20
- Daten des Privatsektors 24 14
- Dateneigentum 3 106, 7 15, 23 26, 34 3
- Datenempfänger 3 88, 5 45 ff., 24 41, 44, 25 25, 27
 - Bereitstellung 25 26
 - Pflichten 11 11
- Datenerhebung 9 38
- Datenethik 1 26
- Datenflüsse
 - Data Act 38 9
 - DS-GVO 38 5
 - KI-VO 38 23
- Datengenerierung 34 15 ff.
- Datengenossenschaft 7 16, 19 23, 21 33
- Datengetriebene Services 9 50
- Datengetriebenes Geschäftsmodell 19 18, 23 19
 - bezahlen mit Daten 22 3
- Datengovernance 1 27, 19 17, 21 5, 34 53
 - KI-VO 28 96 ff.
- Daten-Governance-Gesetz (DGG) 22 7 ff.
 - Gesetzgebungsverfahren 22 90
- Datenhandel 8 1 ff., 10 1 ff., 23 43
- Datenhandelsunternehmen 10 2
- Datenherrprinzip 7 9
- Dateninfrastruktur 9 45, 23 42, 29 1, 30 1
- Dateninhaber 3 86 f., 5 32 ff., 45 ff., 21 12, 22 14, 23 16, 21, 24 41, 43, 25 27
 - Bereitstellung 25 26
 - Einrichtung des öffentlichen Rechts 25 53
 - Forschungseinrichtung 25 53
 - öffentliche Stelle 25 53
 - öffentliches Unternehmen 25 53
 - Rechte 11 11
- Dateninnovationsrat 40 14
- Datenintegrität 16 10
- Datenintermediäre 23 33, 47, 35 59
- Datenkategorie 20 109 ff.
 - Definition 11 45
- Datenkoordinator 5 46 ff.
- Datenkultur 10 3
- Datenlieferanten 9 35
- Datenlizenzvertrag 22 77
- Datenlöschung 35 68 ff.

- Datenmacht 22 3
 - europäischer 11 62
- Datenmärkte 23 8 f., 31, 49
- Datenmarktplatz 9 6, 21 14, 30
- Datenminimierung 7 12, 20 ff., 25 10
 - Altersverifikation 32 39 ff.
 - DSA 32 31
 - Konflikt mit KI-VO 32 90
- Daten mit Drittbezug, Rechtsgrundlagen 32 68 ff.
- Datenmonetarisierung 9 53, 23 1, 12
- Datennutzer/Datennutzung 3 89, 5 32 ff., 45 ff., 7 13, 26, 9 35, 19 1, 14, 16 ff., 20 62 ff., 68, 81, 88 f., 21 12, 86 ff., 22 14, 33 76
- Datennutzungsgesetz (DNG) 19 1, 9 ff., 20 1 ff., 10 ff., 15 ff., 46 ff., 53 ff., 60 ff.
 - Anwendbarkeit 20 59 ff.
- Datennutzungsgesetz 40 33
- Datennutzungsrechte 23 13
- Datennutzungsrichtlinien 11 50
- Datenökonomie 8 1, 9 6, 23 4
- Datenportabilität 11 25, 32 28, 34 3, 35 42 ff.
 - Antrag 14 88
 - by Design 35 56
 - Cloud Computing 18 25
- Datenprodukt 23 7, 35, 44, 51
- Datenproduzentenrecht 23 26
- Datenqualität 9 8
- Datenquellen 34 19 f.
- Datenraum 1 28, 5 32, 19 18, 36 80
 - persönlicher 21 32
- Datenrecht 11 ff., 3 1 ff., 35 1 ff.
 - Begriff 1 5
 - Benachrichtigungspflichten 37 75
 - Benachrichtigungspflichten an Betroffene 37 77
 - europäisches 11 1 ff.
 - Meldepflichten 37 56 f.
 - weitere Meldepflichten 37 54
- Datenregulierung im europäischen Gesundheitsdatenraum 22 3
- Datenrichtigkeit 35 76
- Datenrichtlinie 1 24
- Datensatz 2 2, 32 84
 - Fehlerfreiheit 32 89
 - hochwertiger 20 38
- Datenschutz 1 29, 7 26, 33 95
 - Begriff 33 6
 - durch Technikgestaltung 7 15, 25 10
 - Herstellerpflichten 34 44 ff.
 - Technikgestaltung 34 44 ff.
- Datenschutzaufsichtsbehörde 5 3 ff.
- Datenschutzbehörde 22 62
- Datenschutzerklärung 4 19
- Datenschutz-Folgenabschätzung 11 51
- Datenschutzfreundliche Voreinstellungen 25 10
- Datenschutzgrundsätze, Konflikt mit KI-VO 32 88 ff.
- Datenschutzgrundverordnung (DS-GVO) 5 3 ff., 11 3 ff., 20 119, 21 12, 31 f., 80 ff., 90, 23 39, 25 3, 32 13 ff., 35 3, 16 ff.
 - Anwendungsbereich 37 4
 - Art 25 15 4
 - Benachrichtigungspflicht 37 20
 - Beschäftigtenexzess 40 7
 - Bußgeld 40 4 ff.
 - Bußgeldadressat 40 6 f.
 - Bußgeldbemessung 40 7
 - Bußgeldberechnung 40 5
 - Bußgeldhöhe 40 5
 - Cloud Computing 18 16 ff.
 - Datenschutzvorfälle 37 1, 3
 - Datentransfers 38 5
 - Datenübermittlungen 38 5
 - Durchsetzung 40 12
 - Einwilligung 32 55, 69
 - EU-Verfahrensverordnungsentwurf 40 12
 - Inkrafttreten 32 13
 - internationale Datenflüsse 38 5
 - Konfliktfall 32 45
 - Konkretisierung unbestimmter Rechtsbegriffe 32 16
 - Meldepflicht 37 20 f., 58
 - Regelungsspielräume 32 16
 - Sanktion 40 3 ff., 10
 - Umsetzung 32 15 f.
 - Unternehmensbegriff 40 5
 - Verhaltenszurechnung 40 7
 - Vorrangverhältnis 22 10 ff.
 - Ziel 32 14
 - Zurechnung 40 7
- Datenschutzrecht 19 38, 32 1 ff.
 - Bezüge zur KI-VO 28 159 ff.
 - Cloud Computing 18 16 ff.
 - Datenschutzrichtlinie für elektronische Kommunikation 32 8 ff.
 - Entwicklung 32 1 ff.
 - Grundsätze der Datenverarbeitung 32 4
 - Künstliche Intelligenz 28 159

Stichwortverzeichnis

- safe harbor 32 5 f.
- unionsrechtliche Vorgaben 32 2 ff.
- Datenschutzrichtlinie 11 50, 32 3 ff.
- Datenschutzrichtlinie für elektronische Kommunikation 32 8 ff.
- Dienste mit Zusatznutzen 32 10
- Direktwerbung 32 10
- Fernmeldegeheimnis 32 9
- Umsetzung 32 11
- Vertraulichkeit der Kommunikation 32 9
- Datenschutzvorfall
- Benachrichtigungspflichten 37 10
- Datenpanne 37 1
- geschützte personenbezogene Daten 37 6
- Meldepflicht 37 10, 19
- Rechtliche Grundlagen 37 2
- Sicherheitsmaßnahmen 37 9
- Verarbeitung 37 7
- Verhältnis zu anderen Vorfällen 37 17
- Verletzung 37 3, 8
- Verletzungshandlung 37 5
- weitere Rechtsquellen 37 16
- Datensicherheit 1 30, 11 45, 33 1 ff.
- Anforderungen/Ziele 33 60 ff.
- BDSG 33 16
- Bedarf 33 63 ff.
- Begriff 33 2 ff.
- Data Act 33 22 ff.
- Definition 33 5
- DGA 33 31 ff.
- DMA 33 38 ff.
- DSA 33 43 ff.
- Grenzen 33 94 ff.
- KI-VO 33 51 ff.
- Maßnahmen/Ziele 33 68 ff.
- MaßnahmenVorschriftenVorgaben 33 78
- Niveau 33 69 ff.
- Schutzziele 33 3
- Sicherheit nicht personenbezogener Daten 33 17 f.
- Sicherheit personenbezogener Daten 33 10 ff.
- Datensicherheitsanforderungen 33 60
- Datensicherheitsbedarf 33 63 ff.
- Datensicherheitsmaßnahmen 33 68 ff., 78 ff.
- Datensicherheitsniveau 33 69 ff., 77
- Datensicherheitsrecht 33 1 ff.
- Datensicherheitsrichtlinie 33 61
- Datensicherheitsvorgaben 33 78
- Datensicherheitsziele 33 60, 68 ff.
- Datensicherung 33 87 ff.
- Datensilo 10 3
- Datensouveränität 7 2 ff., 8 ff.
- Datensparsamkeit, Data Act 32 67
- Datenspeicherung 9 38
- Datenspende 19 25, 22 15, 21
- Datenspende-App 22 21
- Datensteuerungsrecht 19 1
- Datenstrategie 1 13, 7 3, 21 83
- Datenaustauschvorgänge 7 26
- Datenteilung 22 3, 23 13
- Datenteilungshemmnis 21 5, 82, 90
- Datenteilungskonzepte 21 7
- Datenteilungskultur 22 88
- Datenträger 3 4, 96
- Datentransaktionen 23 11, 44, 47
- Datentransfer, internationaler 21 52
- Datentreuhänder 7 26, 29
- Datentypen
- Metadaten 24 17
- nicht personenbezogene Daten 24 17
- ohne Weiteres verfügbare Daten 24 17
- personenbezogene Daten 24 17
- Produktdaten 24 17
- verbundene Dienstdaten 24 17
- Datenüberlassung 3 98
- Datenübermittlung 20 153 ff.
- Datenübertragbarkeit 24 78, 32 67
- Datenübertragung 35 49
- Datenverarbeitung
- Begriff 32 85
- Dritte 22 48
- in der Informatik 2 6 ff.
- Rechtmäßigkeit 11 4 f.
- Datenverarbeitungsdienst 5 45 ff., 24 15, 45, 27 1, 3, 5, 7
- Datenvermittlungsdienst 3 90, 5 32 ff., 7 31, 10 11 ff., 27 f., 11 19, 19 20 ff., 39, 21 4 ff., 8 ff., 25 ff., 22 23, 23 12, 33, 48
- DGA 10 26 ff.
- Verhaltenspflichten 32 57 ff.
- Datenvermittlungszweck 21 13, 16, 20, 22, 45
- Datenverträge, Grundlagen 11 2 ff.
- Datenverwendung 7 19
- Datenverwertung 9 38
- Datenvorteile
- personenbezogene Daten 13 39

- Prädiktion 13 7 f.
- Datenweitergabe 35 56
- Datenwert 23 2
- Datenwirtschaft 1 31, 21 1 ff., 5 ff., 83 ff.
- Datenzugang 19 1, 16 ff., 20 53, 21 84, 24 3, 33 96 f., 35 45, 57, 36 22
 - DGA 10 11 ff.
 - für Dritte 11 26
- Datenzugangsanspruch 19 39 f.
- Datenzugangsrecht 21 51, 23 30, 24 33, 35 42 ff.
 - Daten mit Drittbezug 32 68 ff.
 - Rechtsgrundlagen 32 68 ff.
- Datenzugsregelung 20 2
- Dauer 21 14
- Deckungsvorsorge 30 28
- Deepfakes 28 129
- De-facto-Ausschließlichkeit 20 72
- Definitionen 1 19 ff.
- Delegierter Rechtsakt 19 35
- Design Obligation 34 7
- Desinformation 1 32, 29 44
- Deutsche Wohnen-Urteil 40 7
- Deutschland 6 32 ff.
 - GWB 14 7 ff.
 - UWG 14 7 ff.
- Dezisionale Unabhängigkeit 5 5 ff.
- Dienst, verbundener 21 84
- Dienstdaten 34 7, 18 ff.
- Dienste der Informationsgesellschaft 35 89
- Dienste mit Zusatznutzen 32 10
- Dienstleistung der Informationsgesellschaft 18 7 ff.
- Digital Business 9 2
- Digital Compass 11 7
- Digitale Agenda 1 11
 - Ziele 15 7
- Digitale Bildung 7 16
- Digitale Binnenmarktstrategie 15 8
- Digitale Dekade, level playing field 15 2
- Digitale-Dienste-Gesetz (DDG) 39 153 ff., 40 48
- Digitale Güter 9 13 f.
- Digitaler Binnenmarkt 19 5
- Digitaler Markt 7 32
- Digitaler Zwilling 9 46
- Digitale Signature 30 9
- Digitale Souveränität 7 5 ff., 29 18
- Digitale Transformation 9 1 ff.
- Digitale Vermögenswerte 24 21
- Digitalisierung 1 34, 9 1 ff.
 - Maßnahmen 15 9
 - von Kulturbeständen 20 79
- Digitalization 9 1
- Digital Markets Act (DMA) 5 15 ff., 7 32, 11 24 ff., 21 2, 32 23 ff., 35 3, 39 107, 134 ff.
 - Abgrenzung 40 73
 - Anwendungsbereich 14 21 f.
 - Aufbau 14 18
 - Bestreitbarkeit und Fairness 14 5
 - Bußgeldberechnung 40 72
 - Bußgeldfestsetzung 40 66
 - Bußgeldhöhe 40 65
 - Cloud Computing 18 34 ff.
 - Datenportabilität 32 28
 - datenschutzrechtliche Ziele 32 29
 - Doppelbestrafung 32 27
 - Einwilligung 32 25 ff.
 - Ende-zu-Ende-Verschlüsselung 33 41
 - Entstehung 12 13 ff.
 - Ergänzung 14 16
 - Gatekeeper 39 136
 - Gegenstand 14 19 f.
 - Herstellerpflichten 34 49
 - Historie 12 13 ff.
 - „Hochrangige Gruppe“ 40 61
 - interne Compliance-Funktion 40 68
 - Kommission 39 139
 - Meldung 40 62
 - ne bis in idem 40 74
 - Nichteinhaltungsbeschluss 39 140, 40 63
 - Sanktionierung 40 60
 - Überschneidungen nationales Recht 14 11
 - Unternehmensbegriff 40 67
 - Verbot der Weiterverarbeitung, Zusammenführung und Weitergabe von personenbezogenen Daten 32 25 ff.
 - Verhältnis zum nationalen Recht 14 22
 - Verhältnis zur DS-GVO 32 23 ff.
 - Verjährung 40 64
 - Vermutung 14 12 ff.
 - vorläufige Beurteilung 39 142
 - Wettbewerbsbehörde 40 70
 - Wettbewerbsrecht 39 136, 40 71
 - Widerspruchsfreiheit 14 23
 - Ziel 12 12
 - Zielrichtung 14 12 ff.
 - Zwangsgeld 39 144, 40 69

Stichwortverzeichnis

- Digital Services Act (DSA) 5 20, 7 34, 11 30 ff., 32 30 ff., 35 3, 39 107, 152 ff., 40 57
- Anfechtungsklage 39 157
- Aufsicht 40 41
- außergerichtliche Streitbeilegung 39 163
- Benachrichtigungspflicht 37 76
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 39 153
- Bundesnetzagentur 39 153
- Bundeszentrale für Kinder- und Jugendmedienschutz 39 153
- Bußgeldrahmen 40 43
- Cloud Computing 18 8 ff.
- Dark Pattern 32 33 f.
- Datenminimierung 32 31
- Defizite 40 56 ff.
- Europäisches Gremium für digitale Dienste 40 59
- große Online-Plattformen 39 160
- „großes“ Bußgeld 40 43
- Haftungsfreistellung 16 13
- „kleines“ Bußgeld 40 44
- Marktortprinzip 40 55
- Meldepflicht 37 55
- Online-Schnittstelle 32 33 f.
- Profiling 32 31
- rechtswidrige Inhalte 32 31
- Sanktion 40 40 ff.
- Sanktionierung 40 40 ff.
- Sanktionsadressat 40 47
- Verhältnis zur DS-GVO 32 30 ff., 36 f.
- Vermittlungsdienste 32 30
- Vorverfahren 39 154
- Werbung auf Online-Plattformen 32 35 ff.
- Widerspruch 39 157
- Zwangsgeld 40 46
- Digital Single Market 19 16
- Digitization 9 1
- Direktwerbung 32 10, 35 86
- Discovery-Anspruch 35 45
- Diskriminierung 3 32, 35 58
- Diskriminierungsfreier Zugang 35 58
- Diskriminierungsverbot 25 24
- Dokument 20 26 ff., 30
- elektronisches 30 63
- Dokumentationspflicht 22 42 ff.
- Doppelbestrafung 32 27
- Doppelrollenproblematik 13 30
- Cloud-Services 13 44
- Konkurrenz 13 42
- Ungleichbehandlung 13 31
- Werbedienste 13 43
- Doppeltürenmodell 31 50
- DPIA 11 51
- Drittanfechtung 20 105
- Dritte 20 129
- als Empfänger 24 71
- Dritterhebung 35 19 f.
- Drittland 19 28 f.
- Drittlandsübermittlung 22 50, 33 86, 89, 100, 35 41
- Cloud Computing 18 26 ff.
- Drittstaat 20 153 ff.
- Drittwiderrspruch 20 171
- Durchleitung 18 7 ff.
- reine 16 6
- Durchleitungsdienste, reine 15 15
- Durchsetzungsbehörde, Kommission 39 134
- Durchsetzungsmaßnahmen 33 118
- Durchsetzungsmechanismus 21 57 ff.
- Dynamische Daten 19 14, 20 98, 100
- Echtzeitzugang 35 57
- E-Commerce 15 6
- Richtlinie 40 49
- Edge Computing 9 46
- EDIP *siehe* European Data Innovation Board (EDIB)
- EDSA *siehe* Europäischer Datenschutzausschuss (EDSA)
- EDSB 5 64 f.
- EECC 31 31
- E-Evidence-Verordnung 31 57
- EGDD 5 29 ff.
- E-Government 1 35
- E-Government-Gesetz (EGovG) 19 41, 20 3 ff., 40 30
- eIDAS 30 2
- Sanktionen 30 18
- eIDAS 2.0 29 6, 17, 30 6
- eIDAS-Knoten 29 16
- Eigenbevorzugung, Machtmissbrauch 13 9 ff.
- Eigentum 6 15
- Daten 6 20
- Datenträger 6 19
- Eigenverantwortlichkeit 7 30
- Eingabedaten 3 30
- Ein-Personen-Unternehmen 21 34