

Compliance Handbuch EU Data Act

Rechtssichere Implementierung des neuen
EU-Datengesetzes in der Praxis

Herausgegeben von

Sebastian Rockstroh

Rechtsanwalt (Syndikusrechtsanwalt), Ingolstadt

Dr. Peter Katko

Rechtsanwalt und Digital Law Leader bei EY Law

Eric Meyer

Senior Associate bei EY Law

Carl Heymanns Verlag 2025

Bibliografische Information der Deutschen Nationalbibliothek

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

ISBN 978-3-452-30432-2

www.wolterskluwer.com

Alle Rechte vorbehalten.

© 2025 Wolters Kluwer Deutschland GmbH, Wolters-Kluwer-Straße 1, 50354 Hürth

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Ausführungen in diesem Buch dienen lediglich als Anregungen und Arbeitshilfen. Die Verantwortung bei Anwendung und Umsetzung des Data Act liegt beim Benutzer. Herausgeber, Autoren und Verlag übernehmen keine Haftung für die Richtigkeit und Vollständigkeit der enthaltenen Ratschläge und Positionen.

Zur erleichterten Lesbarkeit wird im Text auf die gleichzeitige Nennung weiblicher, männlicher und diverser Sprachformen verzichtet und nur die männliche Form verwendet. Sämtliche Nennungen gelten jedoch selbstverständlich gleichermaßen für alle Geschlechtsformen.

Verlag, Herausgeber und Autoren übernehmen keine Haftung für inhaltliche oder drucktechnische Fehler.

Umschlagkonzeption: Martina Busch, Grafikdesign, Homburg-Kirrburg

Satz: Datagroup-Int SRL, Timisoara, Romania

Druck und Weiterverarbeitung: Sowa Sp. z o.o., Piaseczno, Polen

Gedruckt auf säurefreiem, alterungsbeständigem und chlorfreiem Papier.

Vorwort

Willkommen zu unserem Handbuch Data Act.

Von manchen als Meilenstein der europäischen Datenregulierung betrachtet ist zentraler Inhalt des Data Act der Anspruch der Nutzer von vernetzten (IoT) Geräten auf Zugang sowie Bereitstellung der im Rahmen des Betriebs generierten Daten. Die technische Umsetzung bedeutet für die Hersteller jedoch erheblichen Aufwand, weshalb auch viel Kritik am Data Act laut wurde. Tatsächlich stellt sich die Frage, ob so viele brachliegende und gleichzeitig werthaltige Datensilos bei Herstellern und Dateninhabern vorhanden sind, die diese regulatorischen Eingriffe rechtfertigen. Können also mit implementierungsintensiver Regulatorik Geschäftsmodelle befördert werden oder lässt wie schon bei der DSGVO dieser Ansatz Innovation aus der EU abwandern? Andererseits ist der Data Act nun erst einmal bindend Gesetz geworden; als Herausgeber dieses Handbuchs möchten wir die relevanten Stakeholder aufseiten von Herstellern, Dateninhabern und Anbietern bei der Umsetzung des Data Act unterstützen. Dies mit Erfahrung aus der Umsetzungspraxis; und über juristische Interpretation hinaus auch mit Schemata und optischen Darstellungen.

Im Teil 1 geht es um Datenzugang und Datennutzung. Also einerseits die Gestaltung des Datenzugangs (»Access by Design«) und andererseits der Workflow im Hinblick auf die Datenbereitstellung mit dem Fokus auf Authentifizierung, Bestimmung der Daten, Datenschutz sowie Schutz von Geschäftsgeheimnissen. Darüber hinaus werden mögliche Leitplanken für die Gestaltung von Verträgen zwischen einerseits Dateninhabern und andererseits Nutzern und Dritten dargestellt. Die Vielzahl der Themen macht jedoch auch hier augenfällig, dass operative Aufwände für IoT-Hersteller und Betreiber beträchtlich sein werden.

Im Teil 2 geht es dann um die Bereitstellung von Daten der Privatwirtschaft an den öffentlichen Sektor (Business to Government – B2G). Zwar hat die Corona-Pandemie gezeigt, dass in bestimmten Notlagen der öffentliche Sektor mit einer größeren Datengrundlage punktgenauer agieren kann. Aber auch hier stellt sich die Frage, ob nicht sektoral schon ausreichend Berichtspflichten und Zugriffsmöglichkeit bestehen. Die Praxis wird weisen, inwieweit Unternehmen durch die Vorbereitung auf diese Bereitstellungspflichten wie schon bei Access-by-Design erhebliche Kosten entstehen.

Im Teil 3 wird durch Möglichkeiten zum Wechsel des IT-Cloudproviders sowie Interoperabilität versucht, Lock-In-Effekte im IT Betrieb aufzulösen. Kunden von IT-Services soll es erleichtert werden, zu anderen Anbietern zu wechseln. Nachdem das Universum von IT-Dienstleistungen sich immer mehr in die Cloud bewegt, dürfte die Basis für leichteren Anbieterwechsel in der IT geschaffen werden. In der Praxis werden die starke Verzahnung in der Welt des jeweiligen IT-Serviceprovider nebst Migrationsaufwand weiterhin hohe faktische Hürden darstellen. Mit den Transparenzpflichten bei Drittstaatentransfers knüpft der Data Act an Regelungen der DSGVO an – wie schon beim Datenzugang mit der Datenportabilität.

Vorwort

Abschließend möchten wir als Herausgeber betonen, dass uns jedenfalls daran gelegen ist, ein möglichst praxisnahes Werk zum Data Act mit vielen Anwendungshinweisen zu schaffen – unabhängig von der rechtspolitischen Kritik. Insofern gilt unser besonderer Dank den kompetenten Mitautoren sowie Julie Tiltmann und Silvana Redfearn für ihre geduldige Unterstützung.

Wir wünschen viel Spaß beim Lesen.

Ihre Herausgeber

Sebastian Rockstroh, Dr. Peter Katko und Eric Meyer

Autorinnen und Autoren

Birnbauer, Daniela, (LL.M.), MA (Wien) Rechtsanwältin, Wien	Abschnitt 1, Kapitel 2, F.
Bürckel, Lorena (LL.M.) Rechtsanwältin (Syndikusrechtsanwältin), Stuttgart	Abschnitt 1, Kapitel 2, H.
Mag. Dannhausen, Estella, Bsc. LL.M. (Uni Wien) Rechtsanwältin, Wien	Abschnitt 1, Kapitel 2, D.
Foerster, Martin Projectmanager Data & AI Porsche AG, Berlin	Abschnitt 1, Kapitel 2, F.
Frison, Laura, LL.M. Eur. (München) Rechtsanwältin (Syndikusrechtsanwältin), Ingolstadt	Abschnitt 1, Kapitel 2, E. Abschnitt 1, Kapitel 2, I.
Dr. Katko, Peter EY Digital Law Leader, München	Abschnitt 1, Kapitel 1 Abschnitt 1, Kapitel 2, A. I Abschnitt 1, Kapitel 2, A. II. 1. Abschnitt 1, Kapitel 2, E.
Krug, Nicole, LL.M. (London) Rechtsanwältin (Syndikusrechtsanwältin), Kassel	Abschnitt 1, Kapitel 2, H.
Leuthner, Christian Rechtsanwalt, Partner, Frankfurt	Abschnitt 1, Kapitel 2, H.
Meyer, Eric Senior Associate EY Law, München	Abschnitt 1, Kapitel 1 Abschnitt 1, Kapitel 2, A. II. 2. Abschnitt 1, Kapitel 2, A. II. 5 Abschnitt 1, Kapitel 2, C. Abschnitt 1, Kapitel 2, F.
Peschel, Christopher Rechtsanwalt (Syndikusrechtsanwalt), Erlangen	Abschnitt 1, Kapitel 2, G. Abschnitt 1, Kapitel 2, I. Abschnitt 1, Kapitel 3
Reich, Lennart Rechtsanwalt, Baker McKenzie, Stadtbergen	Abschnitt 2, Kapitel 4 Abschnitt 2, Kapitel 5 Abschnitt 2, Kapitel 6 Abschnitt 2, Kapitel 7
Rockstroh, Sebastian Rechtsanwalt (Syndikusrechtsanwalt), Ingolstadt	Abschnitt 1, Kapitel 2, D.
Schall, Tobias Rechtsanwalt EY Law, München	Abschnitt 1, Kapitel 2, B. Abschnitt 3, Kapitel 8 Abschnitt 3, Kapitel 9
Schels, Stefan Rechtsanwalt (Syndikusrechtsanwalt), Ingolstadt	Abschnitt 1, Kapitel 2, A. II. 3. Abschnitt 1, Kapitel 2, E. Abschnitt 1, Kapitel 2, G.

Autorinnen und Autoren

Schultz, Marion Rechtsanwältin, Geschäftsführende Gesellschafterin Trenchant Rechtsanwalts-GmbH, Nürnberg	Abschnitt 3, Kapitel 8 Abschnitt 3, Kapitel 9
Dr. iur. Schwinger, Florian Rechtsanwalt (Syndikusrechtsanwalt), Ingolstadt	Abschnitt 1, Kapitel 2, A. II. 4. Abschnitt 1, Kapitel 2, A. II. 6. Abschnitt 1, Kapitel 3
Schwarz, Alexander Rechtsanwalt und Partner Shepherd & Black PartGmbH, Nürnberg	Abschnitt 1, Kapitel 2, A. II. 2. Abschnitt 1, Kapitel 2, C. Abschnitt 1, Kapitel 2, G.
Tannen, Florian Rechtsanwalt, Partner bei Baker McKenzie, München	Abschnitt 2, Kapitel 4 Abschnitt 2, Kapitel 5 Abschnitt 2, Kapitel 6 Abschnitt 2, Kapitel 7
Weiß, Rebekka, LL.M. (Glasgow) Leiterin Regulierungspolitik, Microsoft Deutschland GmbH, Berlin	Abschnitt 3, Kapitel 8 Abschnitt 3, Kapitel 9
Dr. Wiesemann, Hans Peter Rechtsanwalt, München	Abschnitt 1, Kapitel 2, B. Abschnitt 1, Kapitel 3
Zimmermann, Robert Rechtsanwalt (Syndikusrechtsanwalt), Wolfsburg	Abschnitt 1, Kapitel 3

Inhaltsübersicht

Vorwort	V
Autorinnen und Autoren	VII
Inhaltsverzeichnis	XI
Abkürzungsverzeichnis	XXI
Literaturverzeichnis	XXIII
Abschnitt 1 Datenzugang und Datennutzung	1
Kapitel 1 Überblick – Datenzugang und Datennutzung	1
Kapitel 2 Einzelne Rechte und Pflichten	5
Kapitel 3 Datennutzungsverträge und Missbrauchskontrolle	192
Abschnitt 2 Datenzugang des öffentlichen Sektors (Business to Government - B2G)	219
Kapitel 4 Einführung	219
Kapitel 5 Rechtliche Inhalte	221
Kapitel 6 Implementierung	255
Kapitel 7 Praxistipps	256
Abschnitt 3 Wechsel des IT-Cloudproviders - Interoperabilität	259
Kapitel 8 Einführung	259
Kapitel 9 Rechtliche Inhalte	261
Anhang : Der EU Data Act im Wortlaut (Verordnung (EU) 2023/2854) ...	335
Stichwortverzeichnis	445



Inhaltsverzeichnis

Vorwort	V
Autorinnen und Autoren	VII
Inhaltsübersicht	IX
Abkürzungsverzeichnis	XXI
Literaturverzeichnis	XXIII
Abschnitt 1 Datenzugang und Datennutzung	1
Kapitel 1 Überblick – Datenzugang und Datennutzung	1
A. Hintergrund und Ziele des Datenzugangs und der Datenbereitstellung des Data Acts	1
B. Wesentliche Inhalte dieses Abschnittes für den Datenzugang und die Datenbereitstellung	3
Kapitel 2 Einzelne Rechte und Pflichten	5
A. Grundsatz des Datenzugangs	11
I. Einführung	11
II. Rechtliche Inhalte	11
1. Daten	11
2. Vernetztes Produkt & verbundener Dienst	11
3. Produktdaten und verbundene Dienstdaten	12
4. Ohne Weiteres verfügbare Daten	14
5. Nutzer	15
6. Dateninhaber	20
B. Informationspflichten	23
I. Einführung	23
II. Rechtliche Inhalte	23
1. Information	23
2. Ausgestaltung	28
3. Zeitpunkt	30
III. Implementierung	30
IV. Praxistipps	30
C. Access by Design (Art. 3 DA)	31
I. Einführung	31
II. Rechtliche Inhalte – Die einzelnen Elemente und Anforderungen von Art. 3 DA	34
1. Die konkreten Designanforderungen an vernetzte Produkte oder verbundene Dienste aus Art. 3 DA (»Access by Design«)	34
2. Der Hersteller von vernetzten Produkten oder Anbieter verbundener Dienste als Adressaten der »Access by Design«-Anforderungen	53
3. Der Nutzer als Begünstigter	54
4. Transparenzpflichten	54
	XI

Inhaltsverzeichnis

III.	Implementierung – Praktische Umsetzung der »Access by Design«-Anforderungen und Transparenzanforderungen	56
1.	Vorgehensweise für Hersteller von vernetzten Produkten und Anbietern von verbundenen Diensten	56
2.	Praxistipps: Checkliste	56
D.	Datenzugang und Pflichten des Nutzers (Art. 4 DA)	58
I.	Einführung	58
II.	Rechte und Pflichten von Nutzern und Dateninhabern nach Art. 4 DA	58
1.	Subsidiarität von Art. 4 Abs. 1 DA ggü. Art. 3 Abs. 1 DA	59
2.	Verpflichteter: »Dateninhaber«	61
3.	Anspruchsinhaber: »Nutzer«	62
4.	Umfang des Anspruchs nach Art. 4 Abs. 1 DA	66
5.	Anforderungen an die Bereitstellung der Daten	72
6.	Geschäftsgeheimnisse	83
7.	Datenschutz	88
8.	Beschränkung der Wahlmöglichkeiten	88
9.	Verträge zwischen Dateninhaber und Nutzer	89
10.	Beschränkungen des Nutzers	89
III.	Implementierung	91
IV.	Praxistipps	91
1.	Übersicht	91
2.	Beschränkung des Nutzers	93
3.	Checkliste	93
E.	Weitergabe an Dritte (Art. 5 DA)	95
I.	Einführung	95
II.	Ohne Weiteres verfügbare Daten	97
III.	Nutzerverlangen und Berechtigungsprüfung	98
1.	Begriff des Nutzers	98
2.	Berechtigtes Interesse an einer Prüfung der Nutzereigenschaft	99
3.	Dritter	100
4.	Datensparsamkeit gem. Art. 5 Abs. 4 DA	100
5.	Praktische Umsetzung	101
6.	Bevollmächtigung	102
7.	Formfreiheit des Verlangens	103
IV.	Dateninhaber	103
1.	Legaldefinition	103
2.	Einschränkung der Pflichten für Kleinunternehmen und Kleinunternehmen gem. Art. 7 DA	104
V.	Bestimmung des Datensets	105
1.	Vertiefung zu »ohne Weiteres verfügbaren Daten«	105
2.	Die für die Auslegung und Nutzung erforderlichen Metadaten	107
3.	Innovationsvorbehalt, Art. 5 Abs. 2 DA	107
VI.	Anforderungen an die Bereitstellung der Daten	108
1.	Bereitstellung der Daten	108
2.	unverzüglich	109
3.	einfach und sicher	109

Inhaltsverzeichnis

4. Unentgeltlich für den Nutzer	110
5. in einem umfassenden, gängigen [strukturierten] und maschinenlesbaren Format	110
6. gleiche Qualität wie für den Dateninhaber	111
7. Kontinuierlich und in Echtzeit	112
8. falls relevant und technisch durchführbar	112
VII. Datenschutz	113
1. Personenbezogene Daten	113
2. Rechtsgrundlage nach DSGVO erforderlich (Art. 5 Abs. 7 DA)	114
3. Gewährleistung von Datenportabilität und anderen Betroffenenrechten nach Art. 15 ff. DSGVO (Art. 5 Abs. 8 DA)	115
VIII. Rechtsbeziehung Dateninhaber – Dritter	115
1. Vertragliche Grundlagen	115
2. Beschränkungen der Parteien	116
IX. Geschäftsgeheimnisse	118
1. Definition Geschäftsgeheimnisse	118
2. Ermitteln der Geschäftsgeheimnisse	119
3. Vereinbarung angemessener technischer und organisatorischer Maßnahmen	119
4. Verweigern bzw. Aussetzen des Bereitstellungs-verlangens nach Art. 5 Abs. 10 DA	120
5. Ablehnen des Bereitstellungs-verlangens (»Handbrake Mechanism« – Art. 5 Abs. 11 DA)	120
6. Rechtsbehelf nach Art. 5 Abs. 12 DA	120
X. Torwächter-Prüfung	121
1. Torwächter	121
2. keine Bereitstellung an Torwächter	122
3. Verbote für Torwächter	122
4. Freiwillige Vereinbarungen mit Torwächtern	123
XI. Praxistipps	123
1. Vorprüfung	123
2. Bestimmung der bereitzustellenden Daten	124
3. Prüfung der Erforderlichkeit der Offenlegung von Geschäftsgeheimnissen	124
4. Bereitstellung (des Datensets)	125
F. Tatsächliche Implementierung	125
I. Einführung	125
II. Organisatorische Umsetzung	126
1. Datenmanagement als Aufgabe der Geschäftsleitung	127
2. Organisatorische Maßnahmen für eine Data Act Compliance, inkl. Datenmanagement	128
III. Projektmanagement für die Implementierung	131
1. Projektorganisation	131
2. Zusammenstellung Projektteam – Notwendige Kompetenzen und Teamgröße	133
3. Projektzeitschiene	135

Inhaltsverzeichnis

IV.	Technische Implementierung	135
1.	Technische Umsetzung/Erfüllung der Anforderungen gemäß Art. 3 DA	135
2.	Datenzugangs- und Datennutzungsanspruch gemäß Art. 4, 5 DA	138
3.	Implementierung Data Management und Data Governance im Rahmen eines eigenständigen Teilprojekts	139
4.	Nutzerinterface und Verfügbarmachung/Bereitstellung von Daten	143
V.	Technische Schutzmaßnahmen	146
1.	Intelligente Verträge (Smart Contracts)	149
2.	Verschlüsselung	150
3.	Technische Zugriffskontrolle	152
G.	Datennutzung durch den Dateninhaber (Art. 4 Abs. 13 & Abs. 14 DA)	153
I.	Einführung	153
II.	Rechtliche Inhalte	153
1.	Abgrenzung des Anwendungsbereichs – nicht personenbezogene Daten vs. personenbezogene Daten	153
2.	Dateninhaber	154
3.	»nutzen«	154
4.	Nutzung nur auf Grundlage eines Vertrags	154
5.	Erfüllung rechtlicher Verpflichtungen vs. Notwendigkeit einer Vertragsgrundlage	157
III.	Implementierung	162
1.	Aus Sicht des Nutzers, der Rechte an Daten erteilt	162
2.	Aus Sicht des Dateninhabers und Datenempfängers	163
IV.	Praxistipps	166
H.	Zusammenspiel DSGVO, TDDDG und Data Act	167
I.	Einführung	167
II.	Verhältnis DSGVO und TDDDG zum Data Act	167
1.	DSGVO	167
2.	TDDDG, speziell § 25 TDDDG	168
3.	Informationspflichten	169
4.	Datenschutzgrundsätze Art. 5, 25 DSGVO vs. Art. 3 DA	170
5.	Betroffenenrechte Art. 15, 20 DSGVO vs. Art. 4, 5 DA	170
III.	Implementierung	171
1.	Rechtsgrundlagen	171
2.	Datenschutz als Mittel zur Einschränkung?	176
3.	Infizierung des Datensatzes mit personenbezogenen Daten	177
4.	Vorhalten von Daten	177
5.	Datenzugangs- und -weitergabeanspruch	179
6.	Nutzung von Daten	180
7.	Auftragsverarbeitung	180
I.	Wettbewerbsrecht und Data Act	181
I.	Einführung	181
II.	Rechtliche Inhalte	182
1.	Essential Facility (»wesentliche Einrichtung«) Doctrine	182
2.	Informationsaustausch zwischen Wettbewerbern	184

Inhaltsverzeichnis

3. Verbot der Entwicklung von konkurrierenden Produkten unter Einsatz der Daten/Erkenntnisse	186
III. Implementierung	188
1. »FRAND«	188
2. Vorkahrungen beim Informationsaustausch	189
Kapitel 3 Datennutzungsverträge und Missbrauchskontrolle	191
A. Einführung	191
I. Data is the new IP	191
II. Datennutzungsverträge allgemein	192
B. Rechtliche Inhalte	193
I. Datennutzungsverträge unter dem EU Data Act	193
1. Datennutzungsverträge zwischen dem Nutzer und dem Dateninhaber	193
2. Datennutzungsverträge zwischen dem Dateninhaber und dem Datenempfänger	197
3. Datennutzungsverträge zwischen dem Nutzer und dem Datenempfänger	199
II. Missbrauchskontrolle nach dem EU Data Act	199
1. Gesetzgeberischer Hintergrund	199
2. Missbrauchskontrolle im Einzelnen	200
3. Vergleich mit deutschem AGB-Recht	203
4. Prüfungsschema	204
III. Mustervertragsbedingungen nach Art. 43 DA	204
C. Implementierung	212
D. Praxistipps	217
Abschnitt 2 Datenzugang des öffentlichen Sektors (Business to Government - B2G)	219
Kapitel 4 Einführung	219
A. Hintergrund des Kapitel V des Data Act	219
B. Inhalte des Kapitel V des Data Act	220
Kapitel 5 Rechtliche Inhalte	221
A. Systematik des Kapitel V des Data Act	222
B. Umfang der Pflichten aus Art. 14 und 15 DA zur Datenbereitstellung an Public Bodies wegen außergewöhnlicher Notwendigkeit	224
I. Berechtigte Antragssteller	224
1. Öffentliche Stellen	225
2. Kommission	228
3. Europäische Zentralbank	228
4. Einrichtung der Union	228
II. Richtiger Antragsgegner	231

Inhaltsverzeichnis

III.	Erbringung des Nachweises der außergewöhnlichen Notwendigkeit der Nutzung bestimmter Daten	232
1.	Begriff der außergewöhnlichen Notwendigkeit	232
2.	Maßstab der außergewöhnlichen Notwendigkeit	232
3.	Auslegung der außergewöhnlichen Notwendigkeit	233
IV.	Notwendigkeit der Nutzung der Daten zur Erfüllung der rechtlichen Aufgaben des Antragsstellers, die im öffentlichen Interesse liegen	234
V.	Bereitzustellende Daten	235
C.	Pflichten der Public Bodies gemäß Art. 17 (1), (2) und (6) DA bei Datenbereitstellungsvorgängen	236
I.	Überblick	236
II.	Aufbau	236
III.	Anforderungen an Gegenstand, Inhalt und Form des Datenbereitstellungsvorgangs	237
1.	Anforderungen an den Gegenstand des Datenbereitstellungsvorgangs	237
2.	Inhaltliche Anforderungen	237
3.	Formelle Anforderungen	238
D.	Pflichten und Rechte der Dateninhaber gemäß Art. 17 (5) und Art. 18 DA bei Geltendmachung eines Anspruchs nach Art. 14 und 15 DA durch einen Public Body	239
I.	Überblick	239
II.	Aufbau	240
III.	Datenbereitstellungspflicht	240
1.	Zeitpunkt der Datenbereitstellung	240
2.	Erforderliche technische, organisatorische und rechtliche Maßnahmen	242
3.	Ablehnung und Beantragung einer Änderung eines Datenverlangens	242
4.	Beschwerderecht des Dateninhabers aus Art. 17 (5) DA	244
E.	Rechte und Pflichten der Public Bodies hinsichtlich der aufgrund eines Datenherausgabeverlangens erhaltenen Daten, Pflicht der Empfänger bei Weitergabe solcher Daten und das Beschwerderecht des Dateninhabers gegen eine Datenweitergabe gemäß Art. 17 (3) und (4) sowie Art. 19 und 21 DA	244
I.	Überblick	245
II.	Aufbau	245
III.	Umgang der Public Bodies mit erhaltenen Daten	245
1.	Pflichten der Public Bodies beim Umgang mit erhaltenen Daten	245
2.	Rechte der Public Bodies beim Umgang mit erhaltenen Daten	247
3.	Verantwortlichkeit der Public Bodies für erhaltene Daten	248
IV.	Umgang der Drittempfänger mit erhaltenen Daten	248
V.	Beschwerderecht des Dateninhabers gegen eine Datenweitergabe	249
F.	Vergütungs- und Kompensationsansprüche gemäß Art. 20 DA	249
I.	Überblick	249
II.	Aufbau	249
III.	Vergütungs- und Kompensationsansprüche	249
G.	Amtshilfe und grenzüberschreitende Zusammenarbeit gemäß Art. 22 DA	251
I.	Überblick	251
II.	Aufbau	251

Inhaltsverzeichnis

III. Rechtsfragen der Amtshilfe und grenzüberschreitenden Zusammenarbeit	252
Kapitel 6 Implementierung	255
Kapitel 7 Praxistipps	256
Abschnitt 3 Wechsel des IT-Cloudproviders - Interoperabilität	259
Kapitel 8 Einführung	259
Kapitel 9 Rechtliche Inhalte	261
A. Definition der Datenverarbeitungsdienste	263
I. Legaldefinition Datenverarbeitungsdienste	263
1. Rechenressourcen	264
2. Attribute der adressierten Rechenressourcen	265
3. Bereichsausnahmen	266
II. Gleiche Dienstart und Unterkategorien	267
1. Gleiche Dienstart	267
2. Unterkategorien	268
3. Einwände der Stakeholder	270
B. Wechselmöglichkeit und Anforderungen	278
I. Kontext und Zweck der Wechselmöglichkeit	278
II. Hindernisbeseitigung für den Wechsel	279
1. dieselbe Dienstart	279
2. Abbau von Wechselhindernissen	280
III. Vertragliche Anforderungen	283
1. Form	283
2. Vertragliche Mindestregelungen	283
3. Wechselfrist und Kündigung	284
4. Pflichten während des Wechselprozesses	286
5. Informationspflichten	286
6. Wechselverlangen	289
7. Treu und Glauben nach Art. 27	290
8. Wechselentgelte und weitere Entgeltregelungen nach Art. 29	290
C. Migrationssupport – Technische Aspekte	293
I. Technische und rechtliche Entwicklungen	293
1. Technische und rechtliche Entwicklungen	293
II. Technische Aspekte – Grundlagen	297
1. Abgrenzung Portabilität von Interoperabilität	297
2. Die Ausgangssituation beim Kunden	298
3. Grundsatz der Verhältnismäßigkeit – Treu und Glauben	298
4. Begrifflichkeiten: »Exportierbaren Daten«, »Metadaten«, »Semantik«, »Informationen«	299

Inhaltsverzeichnis

5. Art und Weise der Bereitstellung von Informationen, die nicht exportierbare Daten sind	301
6. Schnittstellen und Protokolle	301
7. Verantwortlichkeiten innerhalb der Abstraktionsebenen	301
III. Ausgewählte Anforderungen an den bisherigen Anbieter	302
1. Unterstützung der Ausstiegsstrategie des Kunden	302
2. Vermeidung von Ausfallzeiten (Erwgr. 78)	306
IV. Ergänzende rechtliche Aspekte zum Migrationssupport	307
1. Vorgehen im Falle einer außerordentlichen Kündigung	307
2. Beendigung	308
3. Aufrechterhaltung einer Minimal-Lizenz aus Compliance-Gründen	308
4. Haftung	308
D. Drittlandstransfer/Schutz im internationalen Verkehr	309
I. Überblick	309
II. Anforderungen an Herausgabe oder Zugangsgewährung	310
1. internationale Übereinkunft	310
2. keine internationale Übereinkunft	311
3. Auslegung des Herausgabe- oder Zugangsverlangens	313
4. Information des Kunden	313
III. Anforderungen an technische, rechtliche, organisatorische und vertragliche Maßnahmen	313
IV. Umsetzung unter Heranziehung von Transfer Impact Assessment Logiken	315
1. Maßnahmen und Bausteine im Überblick	316
2. Transparenz und Offenlegung	317
3. verbindliche vertragliche Regelungen zur Reaktion auf Zugangsanfragen und Zugriffe	318
4. verbindliche vertragliche Prüfungspflichten des Anbieters bei Zugriffsanfragen	318
5. verbindliche vertragliche Pflicht des Anbieters zur Einlegung von Rechtsmitteln	319
6. verbindliche vertragliche Unterstützungspflicht des Anbieters bei der Durchsetzung der Rechte des Kunden	319
7. verbindliche vertragliche Maßnahmen und Prozesse im Umgang mit behördlichen Anfragen	320
8. Warrant-Canary-Verfahren	320
9. technische Maßnahme – Verschlüsselung	320
10. technische Maßnahme – TTE	321
V. Offenlegung der Maßnahmen	322
E. Interoperabilität	322
I. Interoperabilität in und von Datenräumen	323
1. Wesentliche Interoperabilitätsanforderungen	323
2. Weitergehende Spezifizierungs- und Standardisierungsmechanismen	325

Inhaltsverzeichnis

II.	Interoperabilität von Datenverarbeitungsdiensten	327
1.	Interoperabilität zu Zwecken der parallelen Nutzung von Datenverarbeitungsdiensten	328
2.	Spezifizierung und Standardisierung der Interoperabilität von Datenverarbeitungsdiensten	329
III.	Anforderungen an intelligente Verträge.	332
1.	Wesentliche Anforderungen an intelligente Verträge.	332
2.	Konformitätsbewertung und -erklärung	333
3.	Weitergehende Spezifizierungs- und Standardisierungs- mechanismen	333
IV.	Beobachtung und Implementierung von Interoperabilitätsanforderungen . . .	334
	Anhang	335
	Stichwortverzeichnis.	445



sollten unternehmensintern Prozesse definiert werden, um die in der Datenbank enthaltenen Informationen aktuell zu halten.

Im **Online-Handel** sollten die **Produktbeschreibungen** frühzeitig um die entsprechenden Informationen **ergänzt** werden. 129

Im **Offline-Handel** sollten – soweit möglich – **Produktverpackungen** um die entsprechenden Informationen bzw. eine **Link** oder einen **QR-Code** auf diese Informationen ergänzt werden. Falls dies nicht möglich ist, sollten frühzeitig die entsprechenden **Aufsteller** oder **Aufkleber** bereitgehalten werden. 130

C. Access by Design (Art. 3 DA)

I. Einführung

Der Data Act etabliert in Art. 3 Abs. 1 die Verpflichtung für Hersteller von **vernetzten Produkten** und Anbietern von **verbundenen Diensten**, Nutzern standardmäßig Zugang zu ihren **Produktdaten** und **verbundenen Dienstdaten** zu verschaffen. Diese Verpflichtung stellt dabei keinen Anspruch des Nutzers gegenüber dem Hersteller oder Anbieter dar, sondern ist eine *ex lege* Verpflichtung, die der Hersteller oder Anbieter bei der Entwicklung seiner vernetzten Produkte oder verbundenen Dienste berücksichtigen muss. Sie gilt für derartige Produkte und Dienste, die nach dem 12. September 2026 in Verkehr gebracht werden (vgl. Art. 50 UAbs. 3 DA). Im Ergebnis etabliert der Gesetzgeber hier eine »Access by Design«-Anforderung an derartige Produkte und Dienste. 131

Insbesondere die Design-Anforderung der direkten Zugriffsmöglichkeit auf Produktdaten hat naturgemäß weitreichende Konsequenzen für die technischen wie organisatorischen Gegebenheiten und Prozesse beim Hersteller. Denn anders als die **ohne Weiteres verfügbaren Daten**, welche nach Art. 4 bzw. Art. 5 DA bereitzustellen sind (im Detail hierzu unter Rdn. 44 ff.; sowie Abschnitt 1, Kapitel 2, Titel D. und E.), bezieht sich Art. 3 auf alle Produktdaten bzw. verbundenen Dienstdaten, die das vernetzte Produkt bzw. der verbundene Dienst bei seiner Nutzung generiert und die zur Ausleitung konzipiert sind. Diese Datenkategorien müssen daher nicht bereits beim Dateninhaber/Hersteller in dessen Servern/Backends vorliegen, um vom Anwendungsbereich des DA umfasst zu sein. 132

So schlussfolgert auch *Bomhard* richtigerweise, dass »[a]ngesichts der sehr weiten Datendefinition in Art. 2 Abs. 1 DA als auch der Tatsache, dass personenbezogene Daten und nicht-personenbezogene Daten aufgeführt werden, [...] jedes denkbare Datum von Art. 1 Abs. 2 DA und damit vom Data Act umfasst sein [dürfte]«⁴⁶, was auch die Produkt- und verbundenen Dienstdaten nach Art. 2 Nr. 15 und 16 DA praktisch sehr umfassend macht. 133

⁴⁶ *Bomhard*, »Der Anwendungsbereich des Data Act – Offene Fragen rund um Art. 1 DA«, MMR-Beil. 01/2024, S. 72.

- 134 So fallen beispielsweise bei einem modernen Fahrzeug mit rund 20.000 Datenpunkten, die sich in Zeitabständen von Zehntelsekunden bis Sekunden aktualisieren und potenziell ausleitbar sind, Datenmengen an, die rasch in die Terabyte gehen.⁴⁷ Von diesen Daten wird aktuell nur ein Bruchteil tatsächlich aus dem Fahrzeug ausgeleitet, da jedes übertragene Kilobyte mit **Kosten** verbunden ist, etwa für den Datentransport (d.h., Kosten des Mobilfunkanbieters), das Speichern (d.h., Kosten für die Server) und die Verarbeitung durch Mensch und Computer. Die Kosten einer jeden Datenausleitung sind daher gegen den wirtschaftlichen Vorteil des Nutzbarmachens dieser Daten abzuwägen. Davon abgesehen ist eine kontinuierliche **Echtzeit-Übertragung** von den anfallenden Datenmengen mit der derzeit verfügbaren LTE/5G-Technologie technisch unmöglich. Die häufig beschworenen Datenmonopole sind in der Automobil-Branchen vor diesem Hintergrund daher bloß beschränkt vorhanden, da Hersteller auf die im Fahrzeug generierten Daten zwar theoretisch zugreifen könnten, dies aus Kostengründen jedoch nur sehr eingeschränkt tun bzw. die technischen Möglichkeiten eine umfassende Ausleitung derzeit auch gar nicht erlauben. So werden von den Automobilherstellern selbst nur selektiv und in vorab definierten Umfängen bestimmte Daten aus zuvor festgelegten Fahrzeugen im Rahmen der rechtlichen Zulässigkeit für einen vorab determinierten Zeitraum ausgeleitet. Die so erhobenen Daten unterscheiden sich somit von Fall zu Fall und stellen in keiner Weise eine kontinuierliche und in Echtzeit nutzbare Zugriffsmöglichkeit dar. Vielmehr dürfte es sich bei derart ausgeleiteten Daten, die der Hersteller zu eigenen konkreten Zwecken nutzt, um ohne Weiteres verfügbare Daten handeln, die Nutzer vom Hersteller als Dateninhaber nach Art. 4 DA verlangen können.
- 135 Die Verpflichtung des Art. 3 Abs. 1 DA stellt Hersteller daher vor unerwarteten technischen, organisatorischen und letztlich auch finanziellen Herausforderungen. Dabei hat der Gesetzgeber es leider verpasst, die unterschiedliche Komplexität von vernetzten Produkten zu berücksichtigen und für eine entsprechende praktische **Verhältnismäßigkeit** der verschiedenen Hersteller zu sorgen. Denn praktisch dürften Hersteller von etwa Smartwatches, Fitness-IoT Geräten oder etwa »smarten« Staubsaugern vor weniger komplexen Herausforderungen nach Art. 3 DA stehen, wie Automobilhersteller oder Herstellern großer, komplexer IoT-Produktionsanlagen. Hersteller der vorherigen Produktkategorien haben bereits heute etablierte Zugriffsmöglichkeiten der Nutzer auf die Gerätedaten, sei es am dem jeweiligen Produkt selbst oder mittelbar über damit verbundene Applikationen, wie »Health Apps«. Viel entscheidender dürfte aber der Fakt sein, dass eine Smartwatch eine viel geringere Datenmenge bei der Nutzung produziert als etwa das moderne Fahrzeug.
- 136 Unabhängig von dieser Verhältnismäßigkeitsdiskussion, sind im Ergebnis Entwickler und Hersteller von vernetzten Produkten angehalten, ihre **Entwicklungsprozesse**

47 »Connected cars are forecast to make up 95% of all vehicles on the road by 2030, with each one generating an estimated 25 gigabytes of data per hour, which is the same amount of data as it would take someone to stream 578 hours of music.« **Quelle:** <https://www.zdnet.com/article/connected-cars-powered-by-ai-will-make-up-95-of-all-vehicles-on-the-road-by-2030/>; <https://www.comparitech.com/blog/information-security/how-much-data-does-your-car-log/>.

um die Anforderung »Access by Design« zu erweitern. Dies kann mit mal mehr, mal weniger Aufwand einhergehen und ist abhängig von der Komplexität des herzustellenden vernetzten Produkts.

Um bei dem Beispiel der Automobilindustrie zu bleiben, so muss das vernetzte Produkt »Fahrzeug« so konzipiert und hergestellt werden, dass auch dem Nutzer Produktdaten zugänglich sind. Wie dieser Zugang im Detail erfolgen muss, ob er etwa direkt oder »mittelbar direkt« erfolgen kann (sprich direkt im Fahrzeug mittels Schnittstelle oder via remote Server-Lösung), bleibt bis zur abschließenden Klärung durch den EuGH abzuwarten. Es spricht einiges dafür, dass Hersteller von vernetzten Produkten hier eine **Abwägung** treffen können, wie sie die Anforderung aus Art. 3 DA erfüllen möchten. Die **EU Kommission** spricht sogar von einem **Wahlrecht**, ob der Zugriff direkt oder indirekt (nach Art. 4 Abs. 1 DA) erfolgen soll (ausführlich dazu unten im Abschnitt II.).⁴⁸ In jedem Fall muss der Zugang für den Nutzer zu seinen Produktdaten aber *einfach, sicher und unentgeltlich* sein. Dies stellt die Automobilhersteller wie die gesamte Branche mit ihren produktbedingten langen Entwicklungszyklen, die eher als Jahrzehnt als Jahre gedacht werden vor erhebliche Hürden, gesetzliche Anforderungen mit fundamentalen Auswirkungen auf die fahrzeuginterne Dateninfrastruktur bei relativ kurzen Umsetzungsfristen zur erfüllen. Eine solche Schnittstelle kann daher realistisch erst in zukünftigen Fahrzeuggenerationen vernünftig eingeplant, entwickelt und umgesetzt werden. Bis dahin stehen Fahrzeughersteller vor der Herausforderung, eine Beurteilung für jene Modelle vorzunehmen, die noch lange nach dem Geltungsbeginn des Art. 3 Abs. 1 DA am 12.09.2026 vom Fertigungsband laufen werden, ob eine Anpassung für eine direkte Schnittstelle im Fahrzeug relevant und technisch durchführbar ist. Über diese direkte oder indirekte Schnittstelle müssen in weiterer Folge Datenmengen zugänglich gemacht werden, die in dem nach dem DA geforderten Ausmaß bislang nicht vorgesehen waren. Entsprechend gering fallen die aktuellen (und für kommende Fahrzeuggenerationen bereits geplanten) Kapazitäten aus.

Dabei darf nicht außer Acht gelassen werden, dass der DA gleichzeitig verhindern soll, dass Anreize für Investitionen in vernetzte Produkte, von denen die Daten erlangt werden, verloren gehen.⁴⁹ In diesem Sinne sieht Art. 9 DA vor, dass Dateninhaber von Dritten, denen sie die Daten bereitstellen, eine **angemessene Gegenleistung** fordern können, um unverhältnismäßige Belastungen bei Datenzugang und Datennutzung zu vermei-

⁴⁸ EU Kommission, »Frequently Asked Questions« (v. 1.2), S. 17 (abrufbar unter: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act> [letzter Abruf: 3. Februar 2025]) (Hervorhebung durch den Autor): »By the date of entry into application of the Data Act (12 September 2025), products already on the market and new products (when placed on the market) must allow for data to be accessed by the user. **By this date, manufacturers have to decide whether such access will be made directly or indirectly (cf. Article 4[1]). Companies will find practical ways to incentivize the use of the solution that works best for them. Sectoral legislation can be more specific.**«.

⁴⁹ Vgl. Erwgr. 32 DA.

den. Andernfalls wäre die Datenweitergabe wirtschaftlich nicht mehr tragfähig.⁵⁰ Eine solche Entschädigung soll insbesondere jene Kosten umfassen, die mit der Bereitstellung der Daten verbunden sind, wie beispielsweise Kosten, die für die Wiedergabe, die elektronische Verbreitung, die Speicherung und die Formatierung der Daten anfallen.⁵¹

- 139 Der europäische Gesetzgeber hat damit im Kontext des Art. 5 DA klargestellt, dass jede Datenbereitstellung mit entsprechenden Kosten verbunden ist. Nichts anderes kann für die Datenzugangsansprüche des Nutzers gelten. Zwar hat sich der europäische Gesetzgeber in dieser Konstellation dazu entschieden, dem **Nutzer ein kostenfreies Zugangsrecht** einzuräumen. Dennoch darf die grundsätzliche **Interessensabwägung** auch hier nicht außer Acht gelassen werden: eine unverhältnismäßige Belastung der Normadressaten (Hersteller und Anbieter) muss verhindert werden, andernfalls kein Anreiz mehr besteht, überhaupt noch Daten zu generieren und zu erheben.
- 140 Neben der Schaffung eines Zugangs für Nutzer durch die Hersteller und Anbieter, treffen die Verkäufer, Vermieter oder Leasinggeber von diesen vernetzten Produkten oder verbundenen Diensten – bei dem es sich auch um den Hersteller oder Anbieter handeln kann – **Transparenzanforderungen** gegenüber dem Nutzer.⁵² Der Gesetzgeber möchte damit den Nutzer als »Herr seiner Daten« etablieren, und die Information nach Art. 3 Abs. 2 und 3 DA ist dabei die Voraussetzung, den Nutzer über die Datenfähigkeiten der vernetzten Produkts als auch über die entsprechenden Datenempfänger, als mögliche Adressaten seiner Datenbereitstellungsansprüche nach Art. 4 und 5 DA, bestmöglich und umfanglich in Kenntnis zu setzen.

II. Rechtliche Inhalte – Die einzelnen Elemente und Anforderungen von Art. 3 DA

1. Die konkreten Designanforderungen an vernetzte Produkte oder verbundene Dienste aus Art. 3 Abs. 1 DA (»Access by Design«)

- 141 Nach der Vorstellung des EU Gesetzgebers herrscht »in vielen Sektoren« eine Situation, nach der *»die Hersteller, da sie die Kontrolle über die technische Konzeption der vernetzten Produkte oder verbundener Dienste haben, bestimmen, welche Daten generiert werden und wie darauf zugegriffen werden kann, obwohl sie keinen Rechtsanspruch auf diese Daten haben. Daher muss sichergestellt werden, dass vernetzte Produkte so konzipiert und hergestellt sowie damit verbundene Dienste so konzipiert und erbracht werden, dass die Produktdaten und die verbundenen Dienstdaten, einschließlich der entsprechenden Metadaten, die zur Auslegung und Nutzung dieser Daten erforderlich sind, und zwar auch, um die Daten abrufen, nutzen oder weitergeben zu können, für einen Nutzer stets leicht und sicher zugänglich sind, und dies kostenlos, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format«⁵³.*

⁵⁰ Vgl. Erwgr. 46 DA.

⁵¹ Vgl. Erwgr. 47 DA.

⁵² Vgl. Art. 3 Abs. 2 und 3 DA.

⁵³ Vgl. Erwägungsgrund 20 S. 3 ff. DA.

Deshalb verlangt Art. 3 Abs. 1 DA, dass vernetzte Produkte und verbundene Dienste 142
so konzipiert bzw. erbracht werden, dass »die Produktdaten und verbundenen Dienst-
daten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen
relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in
einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit
relevant und technisch durchführbar, direkt zugänglich sind.«⁵⁴

Ausgangspunkt ist damit das vernetzte Produkt bzw. der verbundene Dienst. Diese 143
müssen so konzipiert bzw. erbracht werden, dass Nutzer Zugang zu den von ihnen mit
diesen Produkten bzw. Diensten erzeugten Produktdaten und verbundenen Dienst-
daten haben. Wenngleich der Gesetzgeber es unterlassen hat, den konkreten Adres-
saten in Art. 3 Abs. 1 DA zu nennen, so ist denklogisch nur richtig, dass sich die
Anforderungen aus Art. 3 Abs. 1 DA zur Konzeptionierung und Herstellung bzw.
Erbringung an den jeweiligen Hersteller eines vernetzten Produkts bzw. den Anbieter
eines verbundenen Dienstes richten. Sie sind es, die das Produkt bzw. Dienst »kon-
zipieren und herstellen/erbringen«.

Wie in der Einführung beschrieben, etabliert der Gesetzgeber damit eine *ex lege* Ver- 144
pflichtung für Hersteller und Anbieter in Form von »Access by Design«.

Der »Access by Design« nach Art. 3 Abs. 1 DA verlangt dabei nicht die »Bereitstellung« 145
der Daten, sondern lediglich deren **Zugänglichmachung**. Begrifflich ist die Bereit-
stellung ein mehr gegenüber der Zugänglichmachung aus operativer Aufwandssicht.
Die Bereitstellung setzt generell eine aktive Komponente des Dateninhabers voraus,
indem die Daten dem Nutzer derart verfügbar gemacht werden müssen, dass diese
vom Speichermedium extrahiert und in einem gängigen Format so zur Verfügung
gestellt werden, dass der Nutzer die bereitstehenden Daten abrufen kann, ohne auf den
Speicherort selbst zugreifen zu müssen, um die Daten zu extrahieren. Die Zugänglich-
machung hingegen setzt allein die Ermöglichung eines Zugangs des Nutzers auf den
Speicherort mit den dort gespeicherten Daten voraus, sodass der Nutzer die Daten
ohne weiteres Zutun des Herstellers selbst extrahieren kann – beispielsweise mittels
eines Kabels. Ob der Datenzugang tatsächlich realisiert wird, liegt in der Entschei-
dung des Nutzers, den insoweit die Aktionslast trifft.⁵⁵

Beim Zugang wird also der Nutzer selbst aktiv und greift auf den Datenspeicher 146
mit den Daten zu, wohingegen bei der Bereitstellung dem Nutzer die Daten als
bereits durch den Dateninhaber extrahiert zur Abrufung zur Verfügung stehen. In
Erwägungsgrund 24 DA wird entsprechend differenziert zwischen der Information
des Nutzers darüber, wie die Daten durch den Nutzer »abgerufen« oder »wie auf sie
zugegriffen werden kann«.

Diese Ansicht wird insbesondere weiter durch den Gedanken in Art. 3 Abs. 2 lit. 147
d) DA untermauert, der verlangt, dass der Verkäufer, Vermieter oder Leasinggeber –
wobei es sich auch um den Hersteller handeln kann – den Nutzer über die »techni-

⁵⁴ Art. 3 Abs. 1 DA.

⁵⁵ Vgl. *Specht-Riemenschneider*: Der Entwurf des Data Act, MMR 2022, 809 (815).

«*schon Mittel*» informiert, die für den Zugriff bzw. den Abruf der Daten notwendig sind (ausführlicher hierzu im Abschnitt 1, Kapitel 2, Titel B.).

- 148 Die Differenzierung wird besonders in der in Art. 4 Abs. 1 DA angelegten Abgrenzung zu Art. 3 Abs. 1 DA deutlich: »*soweit der Nutzer nicht direkt vom vernetzten Produkt oder verbundenen Dienst aus auf die Daten zugreifen kann, stellen die Dateninhaber dem Nutzer ohne Weiteres verfügbare Daten [...] bereit.*«⁵⁶
- 149 Ein Abrufen von Daten scheint also mit der Bereitstellung von Daten und ein Zugreifen auf Daten mit einer Zugänglichmachung von Daten zu korrespondieren.

► Hinweis

- 150 In ihren veröffentlichten »*Frequently Asked Questions*«⁵⁷ geht die EU Kommission bei Frage 22 davon aus, dass der direkte Zugang erfüllt ist, wenn der Nutzer ohne Eingreifen einer anderen Partei, insbesondere des Dateninhabers, auf etwa die Produktdaten zugreifen kann (Hervorhebungen durch den Autor):

»*Data are ›directly accessible‹ when:*

- *The user is able to access the data without the intervention of any other party, notably the data holder (this is an alternative to making requests under Articles 4 and 5, which do require data holder intervention).*
- *The user has the technical means to stream or download the data as a result of the design of the connected product[.] Recital 22 explains that the location where the data are stored is irrelevant: data can be ›directly accessible‹ from a storage point on the device itself or from a remote server under the control of the manufacturer or a data holder.*

Put simply, for data to be ›directly accessible‹, the user must therefore be able to access it without the involvement of the data holder, regardless of where the data are stored. Even if there is direct access and a remote server, the data holder is obliged to provide the means (i.e. appropriate interfaces, such as an API) to allow the user to easily access the relevant data (cf. recital 35, which compares Article 3[1] of the Data Act with Article 20 of the GDPR).«⁵⁸

- 151 Im Ergebnis reicht es für den »Access by Design« nach Art. 3 Abs. 1 DA aus, wenn der Hersteller oder Anbieter dem Nutzer den Zugang zu den Daten gewährt. Eine aktive Bereitstellung bedarf es durch sie nicht, sondern der Nutzer muss selbst aktiv den Zugang nutzen.

56 So beispielsweise auch Erwägungsgrund 40 DA: »[...] *Dritte, denen Daten auf Verlangen des Nutzers bereitgestellt werden* [...]«; in Art. 5 Abs. 1 DA geht es ebenso um bereitstellen und nicht zugänglich machen von Daten.

57 Abrufbar unter: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act> (letzter Abruf: 3. Februar 2025).

58 Ibid., S. 16 f.

a) *Das vernetzte Produkt und der verbundene Dienst*

Ein **vernetztes Produkt** ist im Sinne des Data Acts ein (physischer⁵⁹) Gegenstand, der Daten über seine Nutzung oder Umgebung mittels seiner Komponenten oder seines Betriebssystems erlangt, generiert oder erhebt und nach außen übermitteln kann, wobei dessen Hauptfunktion nicht in der Speicherung, Verarbeitung oder Übermittlung von Daten im Auftrag Dritter besteht.⁶⁰ Erfasst sein sollen damit insbesondere solche Produkte, die auch als »**Internet der Dinge**« bezeichnet werden, mit Ausnahme von Prototypen.⁶¹ 152

Als Beispiele für **elektronischen Kommunikationsdienste** zählt der Gesetzgeber in Erwägungsgrund 14 insbesondere »*terrestrische Telefonnetze, Fernseekabelnetze, Satellitennetze und Nahfeldkommunikationsnetze*« auf. 153

Der Gesetzgeber hat ebenfalls erkannt, dass **vernetzte Produkte** (engl. »Connected Product«) 154

*»in allen Bereichen der Wirtschaft und Gesellschaft vor[kommen], einschließlich in privaten, zivilen oder gewerblichen Infrastrukturen, Fahrzeugen, medizinischer Ausrüstung, Lifestyle-Ausrüstung, Schiffen, Luftfahrzeugen, Haushaltsgeräten und Konsumgütern, Medizin- und Gesundheitsprodukten oder landwirtschaftlichen und industriellen Maschinen und Anlagen.«*⁶² 155

Bei dem **verbundenen Dienst** (engl. »Related Service«) handelt es sich um 156

*»einen digitalen Dienst, bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt, – einschließlich Software –, der zum Zeitpunkt des Kaufs, der Miete oder des Leasings so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen.«*⁶³ 157

Als verbundener Dienst bzw. »**virtueller Assistent**« gilt zum Beispiel die Software »Alexa« nach Art. 1 Abs. 4 DA, die auf der gleichnamigen Sprachbox (= vernetztes Produkt) von Amazon läuft bzw. mit dieser verbunden ist. Ebenso können etwa zusätzliche Dienste, etwa Stau- und zusätzliche Ladeinfrastrukturelemente in Navigationsangeboten von Fahrzeugen, die nachträglich durch den Nutzer gebucht werden können, als verbundene Dienste gelten. 158

b) *Die Produktdaten und verbundene Dienstdaten*

Der Nutzer soll bei diesen vernetzten Produkten und verbundenen Diensten Zugang zu seinen generierten Produktdaten bzw. verbundenen Dienstdaten erhalten. 159

59 Vgl. Erwgr. 14 DA erster Satz.

60 Vgl. Art. 2 Abs. 5; Erwgr. 14, 15 DA.

61 Vgl. Erwgr. 14.

62 Vgl. Erwgr. 14.

63 Vgl. Art. 2 Nr. 6 DA.