bitkom

Umsetzungsleitfaden zum Data Act

Hilfestellungen zur Umsetzung von (EU) 2023/2854 – aus der Praxis für die Praxis

Inhalt

1 Einleitung

David Schönwerth, Bereichsleiter Data Economy, Bitkom e.V.

Mit diesem Praxisleitfaden wollen wir Mitarbeitenden in Unternehmen und anderen Personen das Verständnis und die Umsetzung des Data Acts (**DA**)[1] erleichtern. Da wir uns dabei auf bestimmte Artikel und Kapitel des DA konzentriert haben, ist das vorliegende Dokument nicht umfassend.

Da der Leitfaden nicht nur für juristisch geschulte Personen, sondern eine vielfältige Leserschaft konzipiert ist, nutzen wir juristische Fachsprache nur sparsam.

Der Gesetzestext des DA ist im generischen Maskulinum verfasst, deshalb haben wir im Leitfaden auf die sonst im Bitkom übliche genderneutrale Schreibweise verzichtet, um hohe Konsistenz und keine sprachlichen Missverständnisse zu erzeugen.

Zu Beginn der jeweiligen Abschnitte haben wir wo sinnvoll die jeweiligen Erwägungsgründe (**EG**) zu den Artikeln des DA ergänzt.[2]

Über Feedback, Anregungen und Kritik sind wir sehr dankbar, wenden Sie sich dafür gerne an die Ansprechperson am Ende des Dokuments.

1.1 Regelungsschwerpunkt

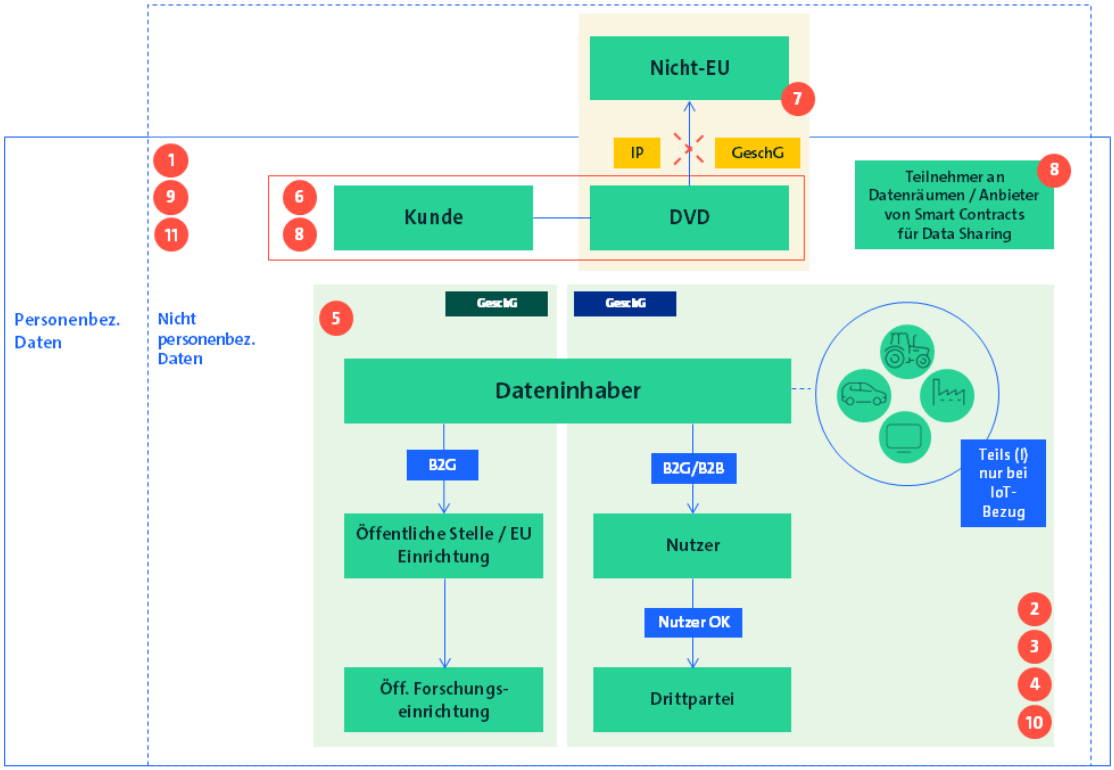
Die Europäische Datenstrategie von 2020 hat zum Ziel, einen europäischen Binnenmarkt für Daten zu schaffen.[3] Bestandteile der Strategie sind u. a. der Data Governance Act,[4] der DA, als auch die Schaffung von sog. Common European Data Spaces[5].

[1] Abl. L, 2023/2854, 22.12.2023, S. 1ff.
[2] Ausschnittsweise übernommen und weiter ergänzt auf Grundlage von: Universität Potsdam, Forschungsstelle Geistiges Eigentum – Digitalisierung – Wettbewerb, Die Bestimmungen des Data Act (EU) 2023/2854 und die jeweils zugehörigen Erwägungsgründe, zuletzt abgerufen am 25.08.2025, https://www.uni-potsdam.de/fileadmin/projects/geidigwett/Erw%C3%A4gungsgr%C3%BCnde_zum_Data_Act.pdf.
[3] EU-KOM, A European Strategy for Data, zuletzt abgerufen am 13.08.2025, https://digital-strategy.ec.europa.eu/en/policies/strategy-data.
[4] Für Zusammenfassung vgl. EU-KOM, European Data Governance Act, zuletzt abgerufen am 13.08.2025, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act. Zu den Pflichten für sog. Datenvermittlungsdienste vgl. Bitkom, Pflichten für Datenvermittlungsdienste durch den Data Governance Act, https://www.bitkom.org/Bitkom/Publikationen/Pflichten-Datenvermittlungsdienste-Data-Governance-Act.
[5] EU-KOM, Common European Data Spaces, zuletzt abgerufen am 13.08.2025, https://digital-strategy.ec.europa.eu/en/policies/data-spaces. Für Übersicht zu Cloud- und Data Economy Initiativen in Europa vgl. Bitkom, Data Economy Landscape, Stand April 2024, https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Data-Economy-Landscape.

Der DA hat zum Ziel, die europäische Datenwirtschaft zu entwickeln und zu stärken, indem er EU-weit insbesondere:

- Die Nutzungsrechte an Daten im Kontext von IoT-Geräten regelt (B2B- und B2C-Data-Sharing, Kap. II, III DA)
- Schranken für faire Datenverträge definiert (Klauselkontrolle, Kap IV DA)
- öffentliche Stellen ermächtigt, Daten von Unternehmen unter besonderen Umständen zu erhalten (B2G-Data Sharing, Kap. V DA)
- Anbieter von Cloud- und ähnlichen Diensten zum Abbau von Wechselhürden und zur Gewährleistung von Interoperabilität verpflichtet (Kap VI, VIII DA)
- Anbieter von Cloud- und ähnlichen Diensten verpflichtet, nicht-personenbezogene Daten im internationalen Kontext zu schützen (Kap. VII DA)
- Teilnehmer an Datenräumen Vorgaben zur Dateninteroperabilität macht (Kap. VIII DA)
- Anbietern von Smart Contracts für das Teilen von Daten vertrauensschaffende Vorgaben macht (Kap. VIII DA).

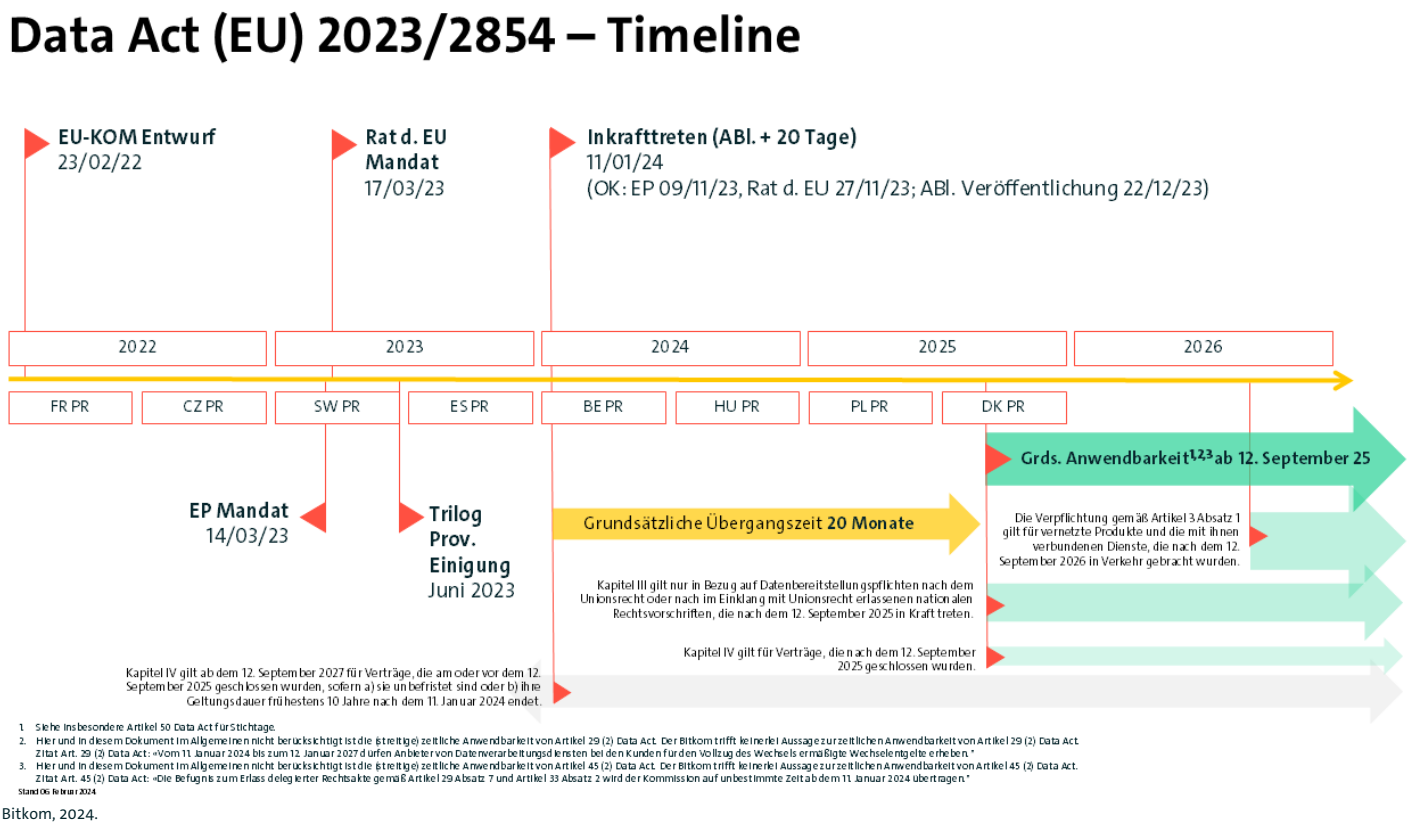
Stark vereinfachte Abbildung.



Bitkom, 2022.

1.2 Der Gesetzgebungsprozess

Der formale Gesetzgebungsprozess zum DA startete am 23.02.2023 mit der Veröffentlichung des Impact Assessments sowie des Verordnungsentwurfs durch die EU-KOM, der eine öffentliche Konsultation voranging.[6] Im März 2023 beschlossen das EU-Parlament sowie der Rat der EU ihre jeweiligen Positionen zum Verordnungsentwurf.[7] Die anschließenden Trilogverhandlungen zwischen Rat der EU, EU-Parlament und EU-KOM kamen am 27.06.2023 zu einem Ergebnis.[8] Nach formaler Annahme des Rechtsakts durch den Rat der EU sowie EU-Parlament trat der DA am 11.01.2024 in Kraft und ist zum 12.09.2025 grundsätzlich anwendbar.[9]



Bitkom, 2024.

[6] EU-KOM, Have Your Say Data Act & amended rules on the legal protection of databases, zuletzt abgerufen am 13.08.2025, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases_en.
[7] EU-Parlament, Legislative Train Data Act Q3/2021, zuletzt abgerufen am 13.08.2025, https://www.europarl.europa.eu/legislative-train/carriage/data-act/report?sid=9301.
[8] Rat der EU, Press Release: Data Act: Council adopts new law on fair access to and use of data, Stand 27.11.2023, zuletzt abgerufen am 13.08.2025, https://www.consilium.europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/.
[9] Art. 50 DA.

1.3 Abgrenzung zu anderen EU-Rechtsakten

Bernd Daamen, Prokurist, BusinessCode GmbH

1.3.1 KI-Verordnung (KI-VO)

1.3.1.1 Regelungsinhalt der KI-VO

Die Verordnung[10] legt Regeln für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der EU fest. Ihr Ziel ist es, das Vertrauen in KI zu stärken, die Sicherheit von KI-Systemen zu gewährleisten und Innovation zu fördern[11] sowie gleichzeitig ein hohes Schutzniveau für Gesundheit, Sicherheit und Grundrechte zu gewährleisten[12].

1.3.1.2 Abgrenzung zum DA

Der DA konzentriert sich auf die Schaffung von Vorschriften für einen fairen Zugang zu Daten und deren Nutzung. Die Regelungen des DA beziehen sich insbesondere auf Daten, die durch die Nutzung vernetzter Produkte oder verbundener Dienste generiert werden.[13] Die KI-VO etabliert dahingegen einen risikobasierten Ansatz, der spezifische Anforderungen an Hochrisiko-KI-Systeme stellt, bestimmte KI-Praktiken verbietet und Transparenzregeln für KI-Systeme mit spezifischen Risiken sowie für KI-Modelle mit allgemeinem Verwendungszweck festlegt.[14]

Der DA schafft somit eine Grundlage für die Verfügbarkeit von Daten, die unter anderem für das Training von KI-Modellen relevant sein können,[15] während die KI-Verordnung die spezifischen Sicherheits-, Transparenz- und Konformitätsanforderungen für die KI-Systeme und -modelle selbst definiert, auch wenn diese als Komponenten in andere Produkte integriert sind[16].

1.3.2 Data Governance Act (DGA)

1.3.2.1 Regelungsinhalt des DGA

Der Data Governance Act (**DGA**)[17] verfolgt zwei Hauptziele. Erstens soll das Teilen und Spenden von Daten unter Privatpersonen, Unternehmen und anderen Teilnehmern der Datenwirtschaft sowie deren Nutzung gefördert werden. Zu diesem Zweck schafft der

[10] Abl. L., 2024/1689, 13.7.2024, S. 1ff.
[11] Bitkom, Umsetzungsleitfaden zur KI-Verordnung (EU) 2024/1689, Stand 29.10.2024, S. 11., https://www.bitkom.org/Bitkom/Publikationen/Umsetzungsleitfaden-zur-KI-Verordnung-EU-2024-1689.
[12] Art. 1 Abs. 1 KI-VO, DA; EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, https://ec.europa.eu/newsroom/dae/redirection/document/108144.
[13] Art. 1 Abs. 1 DA.
[14] Art. 1 Abs. 2 KI-VO; EG 26 KI-VO.
[15] Vbw (Vereinigung der Bayerischen Wirtschaft), »Data Act Leitfaden«, Stand 09/2024, S. 12, https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2024/Downloads/vbw-Leitfaden-Data-Act-September-2024.pdf.
[16] Art. 6 Abs. 1 KI-VO; EG 46 KI-VO.
[17] ABl. L 152, 2022/868, 3.6.2022, S. 1ff.

DGA einen Rechtsrahmen für Datenvermittlungsdienste und datenaltruistische Organisationen, um Vertrauen zu stärken und datenschutzkonformes Teilen zu ermöglichen. Zweitens sollen öffentliche Stellen geschützte Daten, wie personenbezogene Informationen, Geschäftsgeheimnisse oder geistiges Eigentum, unter klar definierten Bedingungen zur Weiterverwendung bereitstellen können. [18]

1.3.2.2 Abgrenzung zum DA

Der DGA schafft primär organisatorische und institutionelle Rahmenbedingungen für den freiwilligen Datenaustausch und begründet weder eine allgemeine Pflicht zur Datenfreigabe noch erweiterte Zugangsrechte zu geschützten Daten des öffentlichen Sektors.[19] Im Gegensatz dazu etabliert der DA verbindliche Rechte und Pflichten für den Datenzugang und die Datennutzung, insbesondere im Kontext vernetzter Produkte und Dienstleistungen.

Ein weiteres Abgrenzungskriterium ist der Fokus auf bestimmte Datenkategorien. So regelt der DGA die weitere Verwendung bestimmter geschützter Daten im Besitz öffentlicher Stellen sowie den Datenaltruismus. Der DA konzentriert sich hingegen auf Produktdaten und verbundene Dienstdaten aus vernetzten Produkten und erleichtert den Wechsel zwischen Datenverarbeitungsdiensten.

1.3.3 Digital Markets Act (DMA)

1.3.3.1 Regelungsinhalt des DMA

Das Ziel des Digital Markets Act (**DMA**)[20] ist die Regulierung der Marktmacht sehr großer Plattformen, die auch als »Gatekeeper« bezeichnet werden. Er soll Transparenz und einen fairen Wettbewerb im digitalen Sektor gewährleisten, indem unfaire Praktiken der »Gatekeeper« untersagt und ihnen eine Reihe von Verhaltenspflichten auferlegt werden.[21]

1.3.3.2 Abgrenzung zum DA

Der DA und der DMA lassen sich anhand folgender Kriterien voneinander abgrenzen: der DA schafft einen horizontalen und sektorübergreifenden Rechtsrahmen für den Zugang zu und die Nutzung von Daten aus vernetzten Produkten und verbundenen Diensten und legt Rechte und Pflichten für Dateninhaber, Nutzer und Dritte fest, um eine faire Wertschöpfung und Innovationsförderung zu ermöglichen.[22]

[18] Fraunhofer CINES, »Implikationen der europäischen Datenstrategie und -regulierung für die Energiewirtschaft«, Stand 02/2025, S. 11, https://www.cines.fraunhofer.de/content/dam/zv/cines/dokumente/publikationen/digitalisierung/2024-Whitepaper_DataAct_final.pdf.
[19] Art. 1 Abs. 2 DGA; Der Bayerische Landesbeauftragte für den Datenschutz, »Daten-Governance Rechtsakt - Auf dem Weg zu einem europäischen Binnenmarkt für Daten - Orientierungshilfe«, Stand 01.05.2024, S. 11 Rn. 16, https://www.datenschutz-bayern.de/infothek/OH_DGA.pdf.
[20] ABl. L. 265, 2022/1925, 14.9.2022, S. 1ff.
[21] Art 1 Abs. 1 DMA; Verbraucherzentrale, »Digitale Dienste: Was regelt der Digital Markets Act?«, Stand 10.4.2025, S. 5.5, https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste/digitale-dienste-was-regelt-der-digital-markets-act-93970.
[22] EG 1, 5, 15 DA; Data Act; EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 2, https://ec.europa.eu/newsroom/dae/redirection/document/108144.

Der DMA hingegen richtet sich ausschließlich an Gatekeeper Plattformen und verpflichtet diese zu spezifischen Verhaltensregeln, um ihre marktübergreifende Macht zu begrenzen, Wettbewerbsverzerrungen zu verhindern und Innovation zu fördern.[23]

Während also der DA den allgemeinen Datenzugang und die Datennutzung branchenübergreifend regelt, konzentriert sich der DMA auf die Regulierung großer Gatekeeper-Plattformen und deren Verhalten im Marktgeschehen.

1.3.4 Digital Services Act (DSA)

1.3.4.1 Regelungsinhalt des DSA

Mit dem Digital Services Act (**DSA**)[24] soll ein sicheres, transparentes und verantwortungsvolles Online-Umfeld geschaffen werden.[25] Dazu legt der DSA harmonisierte Sorgfaltspflichten für Anbieter von Vermittlungsdiensten, insbesondere für Online-Plattformen, fest. Dies umfasst Maßnahmen gegen rechtswidrige Inhalte,[26] Desinformation und manipulative Praktiken, um Grundrechte zu schützen und die Funktionsweise des Binnenmarktes zu verbessern.[27] Die Regulierung ist abgestuft und richtet sich nach Art, Größe und Reichweite der Dienstanbieter.[28]

1.3.4.2 Abgrenzung zum DA

Der DA und der DSA lassen sich anhand mehrerer Kriterien voneinander abgrenzen.

Der DA regelt den Zugang zu und die Nutzung von Daten, insbesondere von durch vernetzte Produkte und verbundene Dienste generierten Daten,[29] während der DSA die Anbieter von Online-Vermittlungsdiensten und deren Umgang mit von Nutzern bereitgestellten oder verbreiteten Inhalten reguliert.[30]

Der DA konzentriert sich insbesondere auf Produktdaten und Daten aus verbundenen Diensten, die oft im Kontext des Internets der Dinge (IoT) anfallen. Der DSA adressiert hingegen rechtswidrige und schädliche Inhalte, also Informationen, Produkte, Dienstleistungen oder Tätigkeiten, die nicht im Einklang mit dem Unionsrecht oder nationalem Recht stehen.[31]

Schließlich richtet sich der DA an Hersteller, Nutzer, Dateninhaber und Datenempfänger im Ökosystem vernetzter Produkte,[32] der DSA hingegen an Anbieter von Vermittlungsdiensten wie Hosting-Anbieter, Online-Plattformen und Suchmaschinen.

[23] Art. 3 DMA.
[24] ABl. L 271, 2022/2065, 19.10.2022, S. 1ff.
[25] RA Plutte, »Großer Guide zum Digital Services Act (DSA)«, zuletzt abgerufen am 12.08.2025, https://www.ra-plutte.de/dsa/#was-ist-dsa.
[26] Art. 1 DSA.
[27] EG 3ff. DSA.
[28] Kapitel III DSA.
[29] Art. 1 Abs. 1 DA.
[30] Art. 2 Abs. 1 DSA.
[31] Art. 3 lit. h DSA.
[32] Art. 1 Abs. 3 DA.

1.3.5 Digitale-Inhalte-Richtlinie (DIR)

1.3.5.1 Regelungsinhalt der Digitale-Inhalte-RL

Die Digitale Inhalte Richtlinie (**DIR**)[33] harmonisiert unionsweit die vertragsrechtlichen Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen zwischen Unternehmen und Verbrauchern. Insbesondere werden Anforderungen an die Vertragsmäßigkeit, Abhilfen bei Vertragswidrigkeit oder Nichtbereitstellung sowie Regelungen zur Änderung digitaler Inhalte oder Dienstleistungen festgelegt.[34]

1.3.5.2 Abgrenzung zum DA

Die DIR regelt ausschließlich die vertragsrechtlichen Beziehungen zwischen Unternehmen und Verbrauchern bei der Bereitstellung digitaler Inhalte oder Dienstleistungen und legt dabei insbesondere Rechte und Pflichten hinsichtlich Vertragsmäßigkeit, Gewährleistung und Rechtsbehelfe fest. Sie dient also primär dem Verbraucherschutz.[35] Der DA verfolgt hingegen das Ziel, den Zugang zu und die Nutzung von personenbezogenen und nicht personenbezogenen Daten wirtschaftsweit zu regeln. Der Fokus liegt auf der Datenökonomie und nicht auf dem Vertragsrecht (obwohl der DA auch dazu Regeln enthält). Der Ansatz ist technologie- und akteurübergreifend gestaltet. Darüber hinaus betrifft der DA die Nutzung, Zugangsrechte und Weitergabe von Daten unabhängig von einem konkreten Verbrauchervertrag und ist auch auf B2B- und B2G-Konstellationen anwendbar.

1.3.6 Plattform-to-Business-Verordnung (P2B-VO)

1.3.6.1 Regelungsinhalt der Plattform-to-Business-VO

Die Plattform-to-Business-Verordnung (**P2B-VO**)[36] verpflichtet Anbieter von Online-Vermittlungsdiensten und Suchmaschinen zu mehr Transparenz gegenüber gewerblichen Nutzern. Dazu zählen klare Geschäftsbedingungen, nachvollziehbare Rankingkriterien und ein faires Beschwerdemanagement. Das Ziel besteht in der Förderung eines vertrauensvollen und innovationsfreundlichen, digitalen Binnenmarkts.[37]

1.3.6.2 Abgrenzung zum DA

Während sich die P2B-VO auf die Beziehung zwischen Plattformbetreibern und gewerblichen Nutzern konzentriert, stehen beim DA die Zugänglichkeit und Nutzung von Daten im Vordergrund. Die P2B-VO behandelt keine Datennutzung durch Dritte, sondern strukturiert Vertragsverhältnisse und Informationspflichten digitaler

[33] ABl. L. 136, 2019/770, 20.5.2019, S. 1ff.
[34] Art. 1 DIR, EG 11 DIR.
[35] Art. 1, 3, 6ff. DIR.
[36] ABl. L. 136, 2019/1150, 11.7.2019, S. 57ff.
[37] Vgl. Art. 1 Abs. 1 i.V.m. EG 2 P2B-VO.

Plattformen.[38] Zudem liegt der Fokus des DA auf der gerechten Verteilung der Datenwertschöpfung, während die P2B-VO primär Wettbewerbs- und Transparenzaspekte reguliert[39].

1.3.7 NIS-2-Richtlinie (NIS-2-RL)

David Schönwerth, Bereichsleiter Data Economy, Bitkom e.V.

1.3.7.1 Regelungsinhalt der Netzwerk- und-Informationssicherheits-RL 2 (NIS-2-RL)

Die Netzwerk-und-Informationssicherheits-Richtlinie 2 (**NIS-2-RL**)[40] harmonisiert und erhöht die Sicherheitsanforderungen an öffentliche Stellen und bestimmte private Organisationen, erweitert den Kreis dieser Organisationen signifikant, verpflichtet Mitgliedsstaaten zur Erarbeitung von Cybersicherheitsstrategien und stärkt die behördliche Aufsicht sowie Kooperation.

1.3.7.2 Abgrenzung zum DA

Während der DA insbesondere Datenhalter[41], zur Bereitstellung von Daten verpflichtete Organisationen[42], Vertragsparteien von Datenverträgen[43] sowie Anbieter von Datenverarbeitungsdiensten[44]betrifft, adressiert die NIS-2-RL im nichtöffentlichen Bereich Unternehmen ab einer bestimmten Größe in kritischen Sektoren. In Bezug auf Normadressaten gibt es – insbesondere, aber nicht nur – bei Anbietern von sog. »Cloud-Computing-Diensten«[45] sowie Unternehmen des Maschinenbaus[46] wohl zahlreiche Überlappungen zwischen DA und NIS-2-RL.

[38] Vgl. Bundesnetzagentur, «Platform-to-Business-Verordnung Fairness und Transparenz für gewerbliche Nutzer von Online-Diensten«, zuletzt abgerufen am 25.07.2025, https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/P2B/start.html.
[39] Vgl. Bundesnetzagentur, «Platform-to-Business-Verordnung Fairness und Transparenz für gewerbliche Nutzer von Online-Diensten«, zuletzt abgerufen am 25.07.2025, https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/P2B/start.html.
[40] ABl. L 333, 2022/2555, 27.12.2022, S. 80ff.
[41] Kapitel 2, 5, 10 DA.
[42] Kapitel 3 DA.
[43] Kapitel 4 DA.
[44] Kapitel 6 - 8 DA.
[45] Art. 6 Nr. 30, Anhang 1 Nr. 8 NIS-2-RL.
[46] Anhang 2 Nr. 5 lit. d NIS-2-RL.

1.4 Potenzielle Spannungsfelder bei der Anwendung des DA

1.4.1 Datenschutzrecht

Bernd Daamen, Prokurist, BusinessCode GmbH

EG7

Die Einführung des DA markiert einen bedeutenden Wandel im europäischen Datenrecht. Ziel ist es, die Wertschöpfung aus industriellen- und IoT-Daten zu erweitern und die Trennung zwischen verschiedenen Datenquellen zu überwinden.

Art. 1 Abs. 5 DA: »Diese Verordnung gilt unbeschadet des Unionsrechts und des nationalen Rechts über den Schutz personenbezogener Daten, die Privatsphäre, die Vertraulichkeit der Kommunikation und die Integrität von Endgeräten, die für personenbezogene Daten gelten, die im Zusammenhang mit den in der vorliegenden Verordnung festgelegten Rechten und Pflichten verarbeitet werden, insbesondere der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie 2002/58/EG, einschließlich der Befugnisse und Zuständigkeiten der Aufsichtsbehörden und der Rechte der betroffenen Personen. Soweit Nutzer betroffene Personen sind, ergänzen die in Kapitel II dieser Verordnung festgelegten Rechte das Auskunftsrecht von betroffenen Personen und das Recht auf Datenübertragbarkeit gemäß Artikel 15 bzw. Artikel 20 der Verordnung (EU) 2016/679. Im Falle eines Widerspruchs zwischen der vorliegenden Verordnung und dem Unionsrecht in Bezug auf den Schutz personenbezogener Daten bzw. der Privatsphäre oder den im Einklang mit dem Unionsrecht erlassenen nationalen Rechtsvorschriften haben das Unionsrecht oder das nationale Recht zum Schutz personenbezogener Daten bzw. der Privatsphäre Vorrang.«

Dies betrifft zwar häufig nicht-personenbezogene Daten, umfasst jedoch auch personenbezogene Daten. Die parallele Geltung der Datenschutzgrundverordnung (**DSGVO**)[47] führt daher zu potenziellen Spannungsfeldern, die Unternehmen und Behörden vor neue Herausforderungen stellen.

Materiell

Der DA findet Anwendung auf eine Vielzahl von Akteuren, darunter Hersteller, Dateninhaber und Nutzer vernetzter Produkte. Er verpflichtet zur Bereitstellung von Daten an Nutzer und Dritte. Die DSGVO bleibt davon allerdings unberührt und geht im Kollisionsfall vor[48]. Der DA schafft keine Rechtsgrundlage i.S.v. Art. 6 Abs. 1 DSGVO.[49]

Dies bedeutet, dass eine Bereitstellung personenbezogener Daten gemäß DA nur dann zulässig ist, wenn eine entsprechende Rechtsgrundlage vorliegt. In der Praxis wird dies – jedenfalls sofern der Nutzer auch die (einzige) betroffene Person ist – häufig entweder eine (zumindest konkludente) Einwilligung der betroffenen Person nach Art. 6 Abs. 1 lit. a DSGVO oder zum Zweck der Vertragserfüllung nach Art. 6 Abs. 1 lit. b DSGVO sein. Für besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO sind darüber hinaus noch zusätzliche Anforderungen zu berücksichtigen.[50]

In der Folge könnte es daher in einer Vielzahl von Fällen an einer Rechtsgrundlage für die Herausgabe personenbezogener Daten fehlen. Dies wird insbesondere bei Mischdatensätzen, die sowohl personenbezogene als auch nicht-personenbezogene Daten enthalten, relevant. Die bisherige Praxis, dass diese Datensätze insgesamt als personenbezogen zu bewerten sind, wird durch die Regelungen des DA in Frage gestellt. Zukünftig ist diese Bewertung differenzierter vorzunehmen und eine entsprechende Entscheidung darüber zu treffen, welche Daten offengelegt werden dürfen und welche nicht.[51] Siehe hierzu im Übrigen auch Abschnitt 2.4.9.

Ein weiteres Spannungsfeld findet sich im Bereich des Datenzugangs und der Datenportabilität. Der Zugangsanspruch aus dem DA überschneidet sich inhaltlich mit dem Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO, sofern der Nutzer zugleich Betroffener ist. Allerdings geht der Anspruch aus dem DA inhaltlich weiter, da er auch nicht-personenbezogene Daten umfasst.[52] Somit können in der Praxis parallele Auskunfts- und Übertragbarkeitsansprüche aus beiden Verordnungen nebeneinander entstehen. Diese stellen jeweils unterschiedliche Anforderungen an die Identifikation, den Umfang und das Format der Daten.

Weiterhin könnten die Informationspflichten des DA zu Konflikten führen, da Art. 3 DA zusätzlich zu den datenschutzrechtlichen Informationspflichten nach Art. 13, 14 DSGVO gelten soll (EG 24 DA). Die Überschneidung der Informationskataloge könnte zu einer Überforderung der Verbraucher führen, wenn neben den obligatorischen

[47] ABl. L. 119, 2016/679, 4.5.2016, S. 1ff.
[48] Art. 1 Abs. 5 DA.
[49] IHK Rhein-Neckar, »Das neue EU-Datengesetz – Data Act«, Nr. 6514616, zuletzt abgerufen am 25.07.2025, https://www.ihk.de/rhein-neckar/recht/datenschutz-it-sicherheit/eu-datengesetz-6514616; EG 7 DA.
[50] IHK Rhein-Neckar, »Das neue EU-Datengesetz – Data Act«, Nr. 6514616 (https://www.ihk.de/rhein-neckar/recht/datenschutz-it-sicherheit/eu-datengesetz-6514616); EG 7 DA.
[51] HamBfDI, »Der Data Act als Herausforderung für den Datenschutz«, Stand 29.04.2025, S. 8, https://datenschutz-hamburg.de/news/der-data-act-wie-lassen-sich-datenzugang-und-datenschutz-vereinbaren.
[52] HamBfDI, »Der Data Act als Herausforderung für den Datenschutz«, Stand 29.04.2025, S. 9, https://datenschutz-hamburg.de/news/der-data-act-wie-lassen-sich-datenzugang-und-datenschutz-vereinbaren.

»Datenschutzhinweisen« auch noch »Data Act Hinweise« zur Verfügung gestellt werden.[53]

Sowohl die DSGVO als auch der DA verlangen angemessene technische und organisatorische Maßnahmen (TOMs) zum Schutz der Daten. Während die DSGVO dies in Art. 32 für personenbezogene Daten fordert, verlangt der DA vergleichbare Maßnahmen für alle Datenarten[54]. Welche TOMs konkret zu ergreifen sind, wird nach beiden Verordnungen anhand eines risikobasierten Ansatzes ermittelt. Somit empfiehlt es sich für Unternehmen, entsprechende Schutzmaßnahmen unabhängig vom Personenbezug der Daten zu implementieren.[55]

Aufsichtsrechtlich
Weiteres Konfliktpotenzial ergibt sich auch aus den Zuständigkeiten der Aufsichtsbehörden. Art. 37 Abs. 3 DA legt fest, dass die für die Überwachung nach der DSGVO zuständigen Behörden auch Aufsichtsbehörden nach dem DA sind, allerdings nur, soweit personenbezogene Daten betroffen sind. Für die Aufsicht in allen anderen Anwendungsfällen ernennt jeder Mitgliedsstaat eine oder mehrere Behörden[56]. Der derzeitige Referentenentwurf für das »Data-Act-Durchführungsgesetz« sieht als Aufsichtsbehörde für nicht-personenbezogene Daten die Bundesnetzagentur vor, was vereinzelt kritisiert wird[57]. Soweit der Schutz personenbezogener Daten vom DA umfasst ist, soll die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die Aufsichtsbehörde sein. Nach derzeitigem Stand wären auch die jeweiligen Landesdatenschutzbehörden dafür zuständig, die Einhaltung der DSGVO zu überwachen.[58]

Die parallele Anwendung von DA und DSGVO verlangt von Unternehmen zukünftig eine Datenstrategie, welche sowohl den Zugangs- und Teilungspflichten des DA als auch den bestehenden Datenschutzanforderungen der DSGVO gerecht wird.

[53] Felix Glocker, »Disharmonie zwischen Data Act und DS-GVO«, Stand 14.11.2023, zuletzt abgerufen am 12.08.2025, https://www.cmshs-bloggt.de/rechtsthemen/cmsdatalaw/disharmonie-zwischen-data-act-und-dsgvo/#.
[54] Art. 4 Abs. 6, Art. 5, Art. 17 Abs. 1 lit. g und Art. 19 Abs. 1 lit. b DA.
[55] HamBfDI, »Der Data Act als Herausforderung für den Datenschutz«, Stand 29.04.2025, S. 10, https://datenschutz-hamburg.de/news/der-data-act-wie-lassen-sich-datenzugang-und-datenschutz-vereinbaren.
[56] Art. 37 Abs. 1 DA.
[57] Virtuelles Datenschutzbüro, »Aufsichtsstruktur für die Durchsetzung des Data Act in Deutschland ist verfassungs- und europarechtswidrig«, Stand 14.03.2025, zuletzt abgerufen am 12.08.2025, https://www.datenschutz.de/aufsichtsstruktur-fuer-die-durchsetzung-des-data-act-in-deutschland-ist-verfassungs-und-europarechtswidrig/.
[58] HamBfDI, »Der Data Act als Herausforderung für den Datenschutz«, Stand 29.04.2025, S. 14f., https://datenschutz-hamburg.de/news/der-data-act-wie-lassen-sich-datenzugang-und-datenschutz-vereinbaren.

1.4.2 Geschäftsgeheimnisrecht

Ferdinand Schwarz, Rechtsanwalt, SKW Schwarz Rechtsanwälte Steuerberater Partnerschaft mbB

EG 31 DA

Der DA verpflichtet betroffene Unternehmen dazu, (Produkt-)Daten gegenüber Nutzern und Dritten offenzulegen und kann insofern zu einem Interessenkonflikt führen: (Produkt-)Daten können oftmals Geschäftsgeheimnisse beinhalten, die das Unternehmen grundsätzlich nicht an Dritte preisgeben möchte. Dazu werden sie im Rahmen der Umsetzung des DA aber faktisch gezwungen.

Der DA nimmt diesen Konflikt zum Geschäftsgeheimnisrecht grundsätzlich in den Blick. Die Leitgedanken des Gesetzgebers hierzu finden sich in EG 31 DA. Dort wird festgehalten, dass Dateninhaber nach dem DA grundsätzlich dazu verpflichtet sind, Daten gegenüber Nutzern oder Dritten offenzulegen, selbst wenn diese Daten unter den Schutz des Geschäftsgeheimnisrechts fallen. Das bedeutet: Dateninhaber können ein Datenzugangsverlangen nach dem DA nicht einfach mit der Begründung ablehnen, bestimmte Daten würden als Geschäftsgeheimnisse gelten.

Anders als für das Datenschutzrecht[59] sieht der DA demnach gerade keinen Vorrang des Geschäftsgeheimnisrechts gegenüber dem Datenzugang vor.[60] In Art. 8 Abs. 6 DA wird lediglich klargestellt, dass der DA keine allgemeine Pflicht zur Offenlegung von Geschäftsgeheimnissen über die Art. 4 und Art. 5 DA gesetzlich geregelten Fälle hinaus bestimmt.

Um die Vertraulichkeit von Geschäftsgeheimnissen dennoch sicherzustellen, sieht der DA vor allem einen vertraglichen Schutzmechanismus vor:[61] Datenzugangsansprüche des Nutzers (Art. 4 DA) sowie zugunsten Dritter (Art. 5 DA) setzen voraus, dass eine vertragliche Einigung über angemessene technische und organisatorische Maßnahmen (TOMs) getroffen wird. Wird eine solche Einigung nicht erzielt, nicht umgesetzt oder werden die Geschäftsgeheimnisse anderweitig verletzt, kann der Dateninhaber die Datenweitergabe unter bestimmten Voraussetzungen verweigern. Die näheren Anforderungen richten sich vor allem nach den Art. 4 Abs. 6 bis Abs. 8 (siehe Abschnitte 2.4.5. und 2.4.6.), Art. 5 Abs. 9 bis Abs. 11 (siehe Abschnitt 2.5.6) und Art. 11 DA.

Eine allgemeine Abwägungs- oder Entscheidungsbefugnis des Daten- bzw. Geheimnisinhabers, ob und gegenüber welchen Personen er seine vertraulichen Daten offenlegen möchte, gibt es nach dem DA gerade nicht. Der Inhaber kann seine Daten »nur« durch vertragliche und technische Maßnahmen schützen und muss also darauf »setzen«, dass die Nutzer bzw. Dritte diese wahren. Praktisch wird es aus Sicht des

[59] Vgl. Art. 1 Abs. 5 S. 4 DA.
[60] Wiebe, GRUR 2023, 1569 (1573); Grapentin, RDi 2023, 173 (181); Böken/Vocks, MMR 2024, 1016 (1019).
[61] Antoine, CR 2024, 73 (76).

Dateninhabers darauf ankommen, im Vorfeld der Zugangsgewährung die Umsetzung und Erfüllung der vertraglich festgelegten Schutzmaßnahmen sorgfältig zu prüfen und bei begründeten Zweifeln eine behördliche Entscheidung hierüber einzuholen[62].

Sind die vertraulichen Daten erstmal »in der Welt« und kommt es sodann zu einem Verstoß, ist es um die Geschäftsgeheimnisse des Dateninhabers oft nicht gut bestellt; zumal eine Offenlegung aufgrund der Natur des DA an einen sehr weiten Personenkreis erfolgt und der Nachweis der Vertraulichkeitsverletzung beim Dateninhaber liegt.[63] In Extremfällen mag es theoretisch sogar denkbar sein, dass eine Offenlegung von Informationen nach dem DA dazu führt, dass die Information als »allgemein bekannt« einzustufen ist und grundsätzlich ihren Geheimnischarakter verliert.[64] Der DA führt daher rein faktisch zu einer merklichen Schwächung des Geschäftsgeheimnisschutzes und wurde im Gesetzgebungsverfahren und in der Fachliteratur deshalb teilweise deutlich kritisiert.[65]

Zwar sieht der DA in den Art. 4 Abs. 8 und Art. 5 Abs. 11 DA bei Vorliegen von »außergewöhnlichen Umständen« das Recht des Dateninhabers vor, eine Offenlegung der Daten zu verweigern; diese Ausnahme setzt allerdings die hohe Wahrscheinlichkeit eines schweren wirtschaftlichen Schadens voraus und ist durch den Dateninhaber nachzuweisen. Als Beispiele nennt das Gesetz etwa die Einzigartigkeit und Neuartigkeit des vernetzten Produkts. Diese Hürden sind sehr hoch und ebenso ungewiss. Es ist zweifelhaft, ob sich diese Regelung als praxistauglicher »Ausweg« für Dateninhaber erweisen wird.

Ein weiteres Problem ergibt sich aus Art. 3 DA: Für Dateninhaber, die nach Art. 3 DA verpflichtet sind, Zugang zu Produktdaten soweit technisch möglich »direkt« zu gewähren, existiert keine entsprechende Regelung zum Schutz der Vertraulichkeit von Geschäftsdaten. Das Gesetz enthält hier offenbar eine Regelungslücke.[66] Dies wirft vor allem die Frage auf, ob sich Dateninhaber einstweilen entsprechend auf die oben genannten »Vorbehalte« zum Geschäftsgeheimnisschutz aus den Art. 4 und 5 DA berufen können, wenn sie Nutzern Datenzugang im Rahmen von Art. 3 DA gewähren.[67]

Zudem ist es wichtig im Auge zu behalten, dass sich die Frage nach dem »Verhältnis« von DA und Geschäftsgeheimnisschutz überhaupt erst dann stellt, wenn gleichzeitig (Produkt-)Daten im Sinne des DA und Geschäftsgeheimnisse betroffen sind. Als Erstes sollten betroffene Unternehmen daher ermitteln (dies sehen die Art. 4 und 5 DA ohnehin entsprechend vor), ob – und wenn ja, welche – der betroffenen Daten bzw. Datensätze als Geschäftsgeheimnisse zu klassifizieren sind.

Der DA definiert Geschäftsgeheimnisse in Art. 2 Nr. 18 DA im Sinne von Art. 2 Nr. 1 Richtlinie über den Schutz von Geschäftsgeheimnissen (**Geschäftsgeheimnis-RL**)[68]. Die Klassifizierung von Informationen und Daten als Geschäftsgeheimnissen richtet sich also nach Erfüllung der »herkömmlichen« und bekannten Anforderungen des

[62] Art. 4 Abs. 7 bzw. Art. 5 Abs. 10 i.V.m. Art. 37 DA.
[63] Grützmacher, CR 2024, 281 (286f.) Rn. 35.
[64] Böken/Vocks, MMR 2024, 1016 (1017).
[65] Näher zu den einzelnen Kritik- und Schwachpunkten Grapentin, RDi 2023, 173ff.; Grützmacher, CR 2024, 281 (289ff.).
[66] Vgl. ausführlich hierzu Grützmacher, CR 2024, 281 Rn. 5ff.
[67] Grützmacher, CR 2024, 281 (288f.) Rn. 43ff.
[68] ABl. L. 157, 2016/943, 8.6.2016, S. 1ff.

Geschäftsgeheimnisrechts. Insbesondere für Rohdaten- oder Rohdatenpools wird hier genau zu untersuchen sein, ob diese den Umständen und ihrer Zusammensetzung nach Geschäftsgeheimnisse darstellen, etwa da sie Rückschlüsse auf die Herstellung oder Funktionsweise des Geräts oder des Produkts zulassen.[69]

Die Ermittlung der Daten, die gleichzeitig Geschäftsgeheimnisse darstellen, hat zudem eine ganz praktische Bedeutung: Um in den Genuss der Ausnahmevorschriften für Geschäftsgeheimnisse zu gelangen und eine Offenbarung zu verhindern, muss der Dateninhaber darlegen, dass es sich um Geschäftsgeheimnisse handelt.[70] Es wird hier vor allem darauf ankommen, die ermittelten Datensätze sorgfältig zu kennzeichnen und entsprechend zu dokumentieren. Das ist schon deshalb bedeutsam, um sich nach »Scharfstellung« der Zugangsansprüche gegen eine Offenlegung adäquat verteidigen zu können.

Die Auswirkungen des DA auf das Geschäftsgeheimnisrecht lassen sich derzeit schwer einschätzen. Die teilweise lückenhaften und nicht unumstrittenen Regelungen des DA zum Geschäftsgeheimnisschutz lassen jedoch vermuten, dass es hier in der Umsetzung möglicherweise »knirschen« wird. Klarstellungen durch den Gesetzgeber bzw. die ausführenden Behörden wären hier hilfreich. Bis dahin gilt es, den bestehenden Regelungsspielraum zu analysieren und praxisgerechte Lösungen zu finden.

[69] Grützmacher, CR 2024, 281 (292); Grapentin, RDi 2023, 173 (175).
[70] Grützmacher, CR 2024, 281 (292).

2 IoT Data Sharing (Kapitel II DA)

2.1 Sachlicher Anwendungsbereich

2.1.1 Handelt es sich um ein vernetztes Produkt? (Art. 2 Nr. 5 DA)

Valentino Halim, Rechtsanwalt Tech, Data & AI, Junior Partner, Oppenhoff & Partner Rechtsanwälte Steuerberater mbB

EG 6, 15 DA

Als »vernetztes Produkt« definiert Art. 2 Nr. 5 DA »einen **Gegenstand, der Daten über** seine Nutzung oder Umgebung erlangt, generiert oder **erhebt und** der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang **übermitteln kann** und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist.« (Hervorhebung hinzugefügt)

Es handelt sich also um Gegenstände, die Daten über ihre Nutzung oder Umgebung generieren oder erheben und diese Daten übermitteln können. Erfasst sind physische Objekte, die Sensoren, Software oder andere Technologien enthalten oder nutzen, die Daten erzeugen oder aufnehmen, und diese Produktdaten elektronisch an andere Systeme oder Geräte – drahtlos oder kabelgebunden – übermitteln können. Das kann etwa über eine interne Schnittstelle, WLAN, Bluetooth oder eine Kabelverbindung erfolgen.

2.1.1.1 Positivbeispiele

Dementsprechend unterfallen dem DA grundsätzlich alle Geräte des Internet of Things (IoT). Hierzu zählen insbesondere vernetzte Fahrzeuge (Connected Cars), vernetzte Geräte im Bereich Haushalt (Smart Home) und Consumer Electronics (z. B. Smart TV). Auch vernetzte Gesundheits- und Medizingeräte sowie Industrie- und Landwirtschaftsmaschinen sind vernetzte Produkte[71] – ebenso wie Wearables wie Smartwatches oder Fitness Tracker.

2.1.1.2 Negativbeispiele

Umgekehrt nimmt die gesetzliche Definition bestimmte Produkte ausdrücklich aus. Die Hauptfunktion des Produkts darf nicht darin bestehen, Daten im Auftrag von Personen, die nicht der Nutzer sind, zu speichern, zu verarbeiten oder zu übertragen. Nicht umfasst ist deshalb IT-Infrastruktur zur Datenspeicherung – z. B. Server, Cloud-Infrastruktur –, die der jeweilige Eigentümer ausschließlich im Auftrag von Dritten betreibt.[72]

Auch reine Prototypen vernetzter Produkte unterfallen noch nicht dem Anwendungsbereich des DA.[73]

2.1.2 Handelt es sich um Produktdaten? (Art. 2 Nr. 15 DA)

EG 15 DA

Gegenstand des Datenzugangs- und Datenweitergabe sind Produktdaten und verbundene Dienstdaten, die bei der Nutzung eines vernetzten Produkts oder während der Erbringung eines verbundenen Dienstes generiert werden.

Produktdaten sind gesetzlich definiert als »**Daten, die durch** die Nutzung eines **vernetzten Produkts generiert** werden **und** die der Hersteller so konzipiert hat, dass sie **über** einen **elektronischen Kommunikationsdienst**, eine **physische Verbindung oder** einen **geräteinternen Zugang** von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – **abgerufen werden können**« (Art. 2 Nr. 15 DA). (Hervorhebung hinzugefügt)

[71] Vgl. EG 16 S. 3 DA; Wilkening/Müller, DB 2024, 166 (167).
[72] Vgl. EG 16 S. 4 DA; siehe auch Antoine, CR 2024, 1 (2).
[73] Vgl. Wilkening/Müller, DB 2024, 166 (167).

Erfasst sind alle Daten, die so konzipiert sind, dass sie von irgendjemandem abgerufen werden können. Produktdaten bezeichnen Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie von irgendjemandem – einem Nutzer, Dateninhaber oder Dritten, einschließlich des etwaigen Herstellers – aus dem vernetzten Produkt abgerufen werden können.[74] Die Erwägungsgründe führen als Beispiele »Daten über die Umgebung oder Interaktionen des vernetzten Produkts« an. Im Fall eines vernetzten Navigationsgeräts[75] sind Produktdaten etwa die Standorte zu einzelnen Zeitpunkten.

Wichtig ist dabei, dass der DA angesichts des weiten Datenbegriffs[76] grundsätzlich Daten jeder Art und jedweden Inhalts adressiert. So unterfallen auch nicht-personenbezogene Daten und nicht etwa nur personenbezogene Daten dem DA.

In sachlicher Hinsicht sind die bei der aktiven wie inaktiven Produktnutzung (z.B. Standby) generierten Daten unterschiedlicher Verarbeitungsstände vom DA umfasst. Gegenstand von Kapitel II des DA (IoT Data Sharing) sind neben Rohdaten (Primärdaten), d.h. automatisch generierten Daten ohne weitere Verarbeitung, auch zugehörige Metadaten, einschließlich des Kontexts und Zeitstempels. Ziel ist es, die dem Datenzugang und der Datenweitergabe unterliegenden Daten nutzbar zu machen[77]. Nicht vom DA umfasst sind dagegen aus generierten Roh- und Metadaten gefolgerte oder abgeleitete Daten (inferred data). Abgeleitete Daten entstehen aufgrund zusätzlicher Investitionen des Dateninhabers und sollen nicht umfasst sein. Dies betrifft etwa Daten, die im vernetzten Produkt von (mehreren) Sensoren abgeleitet und mittels proprietärer Algorithmen erhoben werden[78]. Dabei ist der Ausnahmetatbestand der abgeleiteten Daten nicht zu weit zu verstehen. Namentlich sind lediglich »aufbereitete Daten« nicht hiervon erfasst, sondern fallen in den sachlichen Anwendungsbereich des DA. Ob erfasste »aufbereitete Daten« oder vom DA nicht umfasste »abgeleitete Daten« vorliegen, soll davon abhängen, ob der Dateninhaber »wesentliche Investitionen« in die Daten vorgenommen hat[79]. Wo diese Grenze verläuft, dürfte im Einzelfall nicht einfach zu bestimmen sein und in der Praxis nicht unerhebliche Rechtsunsicherheiten hervorrufen.

Vom sachlichen Anwendungsbereich des DA ausgenommen sind außerdem spezifische Datentypen in bestimmten Zusammenhängen[80]. Unter anderem gilt Kapitel II des DA (IoT Data Sharing) etwa nicht für Inhalte in Bezug auf Leistung, Nutzung und Umgebung vernetzter Produkte und verbundener Dienstleistungen[81]. Hierzu zählen beispielweise Text- Audio- oder audiovisuelle Inhalte und Software, die nicht mit dem Produkt identisch ist.

[74] Vgl. EG 15 DA.
[75] Etzkorn, RDi 2024, 116 (117).
[76] Art. 2 Nr. 1 DA.
[77] EG 15, S. 8 - 13 DA.
[78] EG 15, S. 14 DA.
[79] EG 15, S. 10 DA.
[80] Art. 1 Abs. 2 DA.
[81] Art. 1 Abs. 2 lit. a DA.

2.1.3 Handelt es sich um einen verbundenen Dienst? (Art. 2 Nr. 6 DA)

Matthias Treude (Rechtsanwalt bei YPOG GmbH & Co. KG) im Auftrag der DKE-Data GmbH und Co. KG

EG 17 DA

2.1.3.1 Begriffsverständnis

Ein zentraler Begriff im sachlichen Anwendungsbereich des DA, insbesondere für die Datenteilungspflichten nach Kapitel II, ist der »verbundene Dienst«.

Art. 2 Nr. 6 DA konkretisiert »verbundener Dienst« als einen digitalen Dienst, der (1) entweder bereits zum Zeitpunkt des Erwerbs (Kauf, Miete, Leasing) so mit dem vernetzten Produkt verbunden ist, dass dieses ohne den Dienst eine oder mehrere seiner Funktionen nicht ausführen könnte, (2) oder nachträglich vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um dessen Funktionen zu ergänzen, zu aktualisieren oder anzupassen. Ausgenommen sind jedoch explizit elektronische Kommunikationsdienste.

Dabei bilden sich zwei grundlegende Kriterien heraus, die erfüllt sein müssen, um von einem »verbundenen Dienst« auszugehen:

- Der Datenaustausch zwischen vernetztem Produkt und Diensteanbieter muss bidirektional erfolgen und
- durch den verbundenen Dienst werden Funktionen des Produkts beeinflusst.[82] Unerheblich ist dabei, ob die Verbindung von Anfang an besteht oder später ergänzt wird.

[82] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 10, https://ec.europa.eu/newsroom/dae/redirection/document/108144.

Der Kern des Begriffs liegt in der funktionalen Verknüpfung zwischen einem digitalen Dienst und einem vernetzten Produkt. Ohne diese Verbindung könnte das Produkt entweder bestimmte Funktionen nicht erfüllen oder die bestehenden Funktionen des Produkts werden durch die Verbindung mit dem Dienst ergänzt bzw. angepasst. Daraus ergibt sich die besondere Bedeutung des Kriteriums des bidirektionalen Datenaustausches zwischen dem vernetzten Produkt und dem damit verbundenen Dienst.[83]

Gemeint ist eine intrinsische Beziehung zwischen Dienst und Produkt und damit ein Maß an Integration, welches über einen reinen Datenaustausch i.S.v. »Kommunikation« hinausgeht.[84] Der bloße Zugriff auf Daten des vernetzten Produkts genügt somit nicht, vielmehr muss die Verbindung eine derartige Qualität aufweisen, dass von einem steuernden Einfluss auf das Produkt auszugehen ist und nicht von bloßer Datenübertragung.

Verbundene Dienste können dabei nicht lediglich von den Herstellern, Verkäufern, Vermietern oder Leasinggebern entwickelt und erbracht werden, sondern auch von unabhängigen Dritten. Die Entwicklung verbundener Dienste durch Dritte entspricht im Übrigen auch der Zielvorgabe des DA, Innovation zu fördern.[85] Im Gegensatz dazu schützt der DA bei vernetzten Produkten die Investitionen der Hersteller, indem die Nutzung von Daten zur Entwicklung konkurrierender Produkte untersagt wird,[86]um Nachahmungen zu verhindern und Investitionen zu schützen. Für die Praxis bedeutet das, dass Drittanbieter etwa auf Fahrzeugdaten zugreifen können, um eigene digitale Wartungs- oder Versicherungsdienste zu entwickeln, die Entwicklung konkurrierender Fahrzeuge jedoch untersagt bleibt.

Die EU-KOM betont, dass die Bewertung der »Funktionen« vernetzter Produkte, die für die Einordnung eines verbundenen Dienstes von hoher Relevanz ist, eine fortlaufende und sich entwickelnde Aufgabe sei: Praxis und Auslegung durch die Gerichte würden eine wesentliche Rolle bei der Präzisierung dessen spielen.[87] Als Anhaltspunkte, ob ein digitaler Dienst zugleich ein verbundener Dienst sei, gibt die EU-KOM die folgenden Kriterien an:[88]

- Erwartungen der Nutzer an die Produktkategorie;
- Marketing für das vernetzte Produkt und/oder den Dienst;
- Vertragsverhandlungen;
- Austauschbarkeit des digitalen Dienstes;
- Vorinstallation des digitalen Dienstes auf dem vernetzten Produkt.

[83] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 10, https://ec.europa.eu/newsroom/dae/redirection/document/108144.
[84] Vgl. auch EG 17 DA.
[85] EG 16 DA.
[86] Siehe Art. 4 Abs. 10 DA und Abschnitt 2.4.7.
[87] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 10, https://ec.europa.eu/newsroom/dae/redirection/document/108144.
[88] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 10, https://ec.europa.eu/newsroom/dae/redirection/document/108144.

2.1.3.2 Positivbeispiele

Beispiele für die Kategorie der »verbundenen Dienste« sind vor allem sog. »Companion-Apps« zu Smart Devices. Diese Apps bieten essenzielle Dienste, die den Betrieb bzw. die erweiterten Nutzungsmöglichkeiten von Smart Devices ermöglichen und erweitern:

- Eine Smartphone-App, die zur Steuerung und Konfiguration einer smarten Heizungsanlage dient und ohne die wesentlichen Funktionen (z. B. Zeitpläne erstellen, Fernsteuerung) nicht nutzbar wären;
- Ein Dienst für die Einspeisung und Analyse von allgemeinen Verkehrsinformationen bei einem smarten Navigationssystem; Smarte Geschirrspül- oder Waschmaschinen, bei denen mittels Softwarelösung die Umweltauswirkung des Waschgangs anhand verschiedener Sensordaten in der Maschine gemessen und analysiert wird und der Waschgang entsprechend angepasst werden kann;
- Eine Cloud-Plattform, die für den Betrieb eines vernetzten Sicherheitssystems (z. B. Speicherung von Aufnahmen, Weiterleitung von Alarmen) erforderlich ist;
- Eine (cloudbasierte) Analysesoftware, die mit Industriesensoren verbunden ist, wobei die dabei generierten und verarbeiteten Sensordaten prädiktive Wartungshinweise ausgeben, die eine Kernfunktion des Gesamtpakets darstellen.

2.1.3.3 Negativbeispiele?

Im Gegensatz gelten Dienste nicht als verbundene Dienste, wenn sie sich nicht auf die Funktionalität eines vernetzten Produktes auswirken und durch sie keine Daten oder Befehle des Diensteanbieters an das vernetzte Produkt übermittelt werden. Hierunter fallen z. B. zusätzliche Beratungs-, Analyse- oder Finanzdienstleistungen oder regelmäßige Reparatur- und Wartungsdienste, die lediglich Voraussetzungen für den Betrieb sind.[89] Ebenso gelten weder die Stromversorgung noch die Bereitstellung von Konnektivität als verbundener Dienst.[90]

Als Beispiele für nicht verbundene Dienste sind unter anderem aufzuführen:

- Elektronische Kommunikationsdienste, die lediglich den Grundstein für die Weiterverwendung von Daten legen, selbst aber keine Funktion eines vernetzten Produkts beeinflussen.[91]
- One-Way-Dienste, die Daten lediglich in eine Richtung Daten übertragen, wie bspw. eine Wetter-App, die Daten von Wettersensoren lediglich anzeigt, nicht aber deren Funktion beeinflusst;
- Standard-Software (z. B. ein Webbrowser), die auf einem multifunktionalen Gerät (wie einem PC oder Smartphone, das auch zur Steuerung eines vernetzten Produkts verwendet wird) installiert ist, aber nicht spezifisch für die Funktion des vernetzten Produkts erforderlich ist oder diese ergänzt oder anpasst.

[89] EG 17 DA.
[90] EG 17 DA.
[91] EG 17 DA.

2.1.3.4 Grenzfälle

Dienste zur Funktionsverbesserung, aber nicht -notwendigkeit
Ein Dienst, der eine vorhandene Grundfunktion eines Produkts (z. B. Fitness-Tracking) zwar erweitert, aber die Grundfunktion am Gerät selbst weiterhin unverändert bleibt. Der Gesetzeswortlaut legt nahe, dass es nicht erst zum Totalausfall einer Funktion kommen muss, ausreichend kann sein, dass ein Dienst die Gerätefunktion spürbar verändert und dabei aktiv in den Betrieb des Produkts eingreift (z.B. neue Betriebsmodi eröffnet).

Smartphone-Apps
Apps, die nicht (primär) weitere Produkte beeinflussen (bspw. App zur Steuerung einer Heizungsanlage). Hier fiele bspw. eine Karten-App ein – während ein solcher Dienst bei einem Navigationsgerät regelmäßig als »verbunden« im Sinne des DA gelten wird, ist dies bei Smartphones schon nicht ganz klar, denn die Funktionalität eines Smartphones erschöpft sich nicht in der Navigation mit aktuellen Karten. Gleichzeitig stellt die Navigation eine Funktion dar, die das Produkt »Smartphone« nicht ohne diese Anwendung ausüben könnte. Im Zweifel wird eine Einzelfallabwägung ausschlaggebend sein: Werden in der App nur Karten angezeigt und Standortdaten genutzt, ohne das Gerät zu steuern oder dessen Betrieb zu verändern, wäre die Schwelle zur »Verbundenheit« vermutlich nicht überschritten. Sollte die App jedoch erkennbar Teil des Geräte-Ökosystems sein (z.B. vom Hersteller vorinstalliert und/oder im App-Store angeboten) und aktiv in Funktionen eingreifen (bspw. via automatischer Umstellung von System-Einstellungen wie Helligkeit, Energiesparmodus oder Hintergrundaktivitäten), würde man wohl von einem »verbundenen« Dienst« ausgehen.

2.1.3.5 Praxisrelevanz

Die Einordnung als »verbundener Dienst« ist relevant, da sie den Anwendungsbereich für bestimmte Daten (»verbundene Dienstdaten«, siehe Abschnitt 2.1.4) und damit verbundene Datenzugangs- und Informationspflichten[92] eröffnet. Anbieter verbundener Dienste können somit auch Dateninhaber sein,
da verbundene Dienste – unabhängig von der Datenerhebung durch das vernetzte Produkt selbst – für Nutzer relevante Daten generieren.

2.1.3.6 Zusammenfassung

»Verbundene Dienste« sind solche, die eng mit dem Betrieb vernetzter Produkte verknüpft sind und deren Aktivität oder Verhalten steuernd beeinflussen. Ein verbundener Dienst weist eine intrinsische Beziehung und Integration mit dem vernetzten Produkt dergestalt auf, dass Produktfunktionen angepasst oder ergänzt werden. Beispiele sind Companion-Apps zu Smart Devices, die (essenzielle) Funktionen ermöglichen. Grenzfälle sind Anwendungen, bei denen nicht klar ist, ob sie für die Funktion eines vernetzten Produkts unabdingbar sind. Dienste, die Daten nur auslesen

[92] Insb. Art. 3, 4 und 5 DA.

und anzeigen, wie bspw. Wetter-Apps, sind keine verbundenen Dienste. Zu virtuellen Assistenten siehe Abschnitt 2.1.5.

2.1.4 Handelt es sich um verbundene Dienstdaten? (Art. 2 Nr. 16 DA)

Filipp Revinzon, LL.M., Vay Technology GmbH |
Matthias Treude (Rechtsanwalt bei YPOG GmbH & Co. KG) im Auftrag der DKE-Data GmbH und Co. KG

EG 15 DA

2.1.4.1 Begriffsverständnis

Eng verknüpft mit dem »verbundenen Dienst« ist der Begriff der »verbundenen Dienstdaten«. Die Datenkategorie der »verbundenen Dienstdaten« ist dabei von den »Produktdaten«[93] abzugrenzen. »Verbundene Dienstdaten« sind in Art. 2 Nr. 16 DA legaldefiniert, wonach »verbundene Dienstdaten« Daten [sind], die

[1] die Digitalisierung von Nutzerhandlungen oder Vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen und

[2] vom Nutzer absichtlich aufgezeichnet oder als Nebenprodukt der Handlung des Nutzers während der Bereitstellung eines verbundenen Dienstes durch den Anbieter generiert werden.

Um die Datenkategorie »verbundene Dienstdaten« besser zu verstehen, schauen wir uns die einzelnen Elemente einmal genauer an:

[1] die Digitalisierung von Nutzerhandlungen oder Vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen

Im Gegensatz zu Produktdaten, die oft den physischen Zustand eines Geräts beschreiben, repräsentieren verbundene Dienstdaten digitale Aufzeichnungen (i) der Handlungen, die der Nutzer vornimmt, (ii) des Unterlassens von Handlungen durch den Nutzer oder (iii) Ereignisse, die während der Erbringung eines verbundenen Dienstes im Zusammenhang mit dem vernetzten Produkt stattfinden.[94]

Der Fokus liegt hier auf »Nutzerhandlungen« im Sinne von vom Nutzer durchgeführten Aktionen (»Der Nutzer stellt die Temperatur ein.«). Abweichend vom Wortlaut der Legaldefinition im DA sind jedoch nicht nur durch aktive Handlungen generierte Daten erfasst, sondern auch auf einem Unterlassen basierende generierte Daten (»Der Nutzer hat sonntags noch nie die Temperatur eingestellt.«).[95] Etwas komplexer wird es bei

[93] Vgl. insoweit Abschnitt 2.1.2.
[94] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 10, https://ec.europa.eu/newsroom/dae/redirection/document/108144.
[95] EG 15 DA; EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 6, https://ec.europa.eu/newsroom/dae/redirection/document/108144.

Ereignissen, die während der Erbringung eines verbundenen Dienstes im Zusammenhang mit dem vernetzten Produkt stattfinden:

[2] vom Nutzer absichtlich aufgezeichnet oder als Nebenprodukt der Handlung des Nutzers während der Bereitstellung eines verbundenen Dienstes durch den Anbieter generiert werden

Gemeint sind danach Daten, unabhängig davon, ob sie vom Nutzer gezielt aufgezeichnet werden oder als bloßes Nebenprodukt seiner Handlung entstehen. Es ist somit gerade nicht erforderlich, dass der Nutzer die Daten generieren möchte (»Nutzer gibt Präferenzen in den Einstellungen ein.«) oder sich über die Generierung überhaupt bewusst ist (»Die App protokolliert bestimmte Nutzeraktionen«). Vielmehr genügt der Umstand, dass sie während der Bereitstellung eines verbundenen Dienstes durch den Diensteanbieter generiert werden.

Wichtig ist dabei, dass der DA Daten jedweden Inhalts umfasst[96], und nicht etwa nur personenbezogene Daten.

2.1.4.2 Positivbeispiele

- Einstellungen, die ein Nutzer über die App eines verbundenen Dienstes vornimmt (z. B. eingestellte Temperatur am Thermostat-Interface der App, gewählter Waschgang in der Waschmaschinen-App; die Reaktion eines Fahrers auf eine Staumeldung eines vernetzten Navigationsgerätes).[97]
- Aufgezeichnete Informationen von vernetzten Produkten, wie bspw. Health-Data von Fitnesstrackern (vgl. insoweit aber auch Abschnitt 2.1.4.4).
- Nutzungsdaten eines Streaming-Dienstes (bspw. Steuerbefehle, Zeitpunkte der Wiedergabe, Geschwindigkeit), soweit sie nicht bloße Content-Wiedergabe dokumentieren, sondern Funktionen des verbundenen Dienstes steuern oder verändern (z.B. Geräteeinstellungen, Profil-/Konfigurationsänderungen). In Grenzfällen ist strikt zu trennen zwischen contentbezogenen Nutzungsprotokollen (ausgenommen) und funktionalen Steuer-/Einstelldaten (potenziell erfasst).
- Nutzungsprotokolle des verbundenen Dienstes, die zeigen, wann und wie der Nutzer mit der Dienstoberfläche interagiert hat, um das Produkt zu steuern (z. B. Zeitstempel des Ein-/Ausschaltens über die App).
- Vom verbundenen Dienst generierte Fehlerprotokolle oder Diagnosedaten, die auf einer Nutzeraktion (z. B. Start eines Diagnosevorgangs über die App) oder einem vom Produkt über den Dienst gemeldeten Ereignis basieren und im Dienst aufgezeichnet werden.

[96] Art. 1 Abs. 2 DA.
[97] Etzkorn, RDi 2024, 116 (117).

2.1.4.3 Negativbeispiele

Allgemeine Daten/Informationen, die der Nutzer beim Dienstanbieter hinterlegt hat (Modellnummer, Adresse, Zahlungsdaten), sofern sie nicht direkt eine digitalisierte Nutzerhandlung im Kontext des Produktes darstellen.

Daten, die der Anbieter des verbundenen Dienstes aus verbundenen Daten »ableitet«. Voraussetzung dafür ist, dass sie das Resultat »zusätzlicher Investitionen in die Zuweisung von Werten oder Erkenntnissen sind«[98]. Gemeint sind damit Ergebnisse, die ein komplexer proprietärer Algorithmus ausgibt.[99] Sie stellen keine direkte Abbildung von Nutzerhandlungen oder Ereignissen selbst dar.[100]

2.1.4.4 Grenzfälle

Im Wesentlichen sollte hier die Abgrenzung zu »Produktdaten« relevant sein:

Vom verbundenen Dienst verarbeitete Produktdaten
Produktdaten (z. B. Sensordaten), die erst nach Verarbeitung oder Aggregation durch den verbundenen Dienst für den Nutzer sichtbar/nutzbar werden. Sind die verarbeiteten Daten »verbundene Dienstdaten«? Fraglich, wenn sie immer noch primär die Produktnutzung/-umgebung widerspiegeln. Die Protokollierung der Verarbeitung selbst oder Nutzeraktionen zur Initiierung der Verarbeitung könnten Dienstdaten sein. Art. 2 Nr. 17 DA zielt auf die Digitalisierung von Nutzerhandlungen/Vorgängen ab.

Automatisierte Aktionen basierend auf Nutzereinstellungen
Daten, die entstehen, wenn der verbundene Dienst aufgrund einer vom Nutzer zuvor getroffenen Einstellung (z. B. Zeitplan) automatisch eine Aktion auslöst (z. B. Windschutzscheibe in den Wintermonaten heizen). Dies stellt wohl eine Digitalisierung eines Vorgangs dar, der auf einer (früheren) absichtlichen Nutzerhandlung basiert und könnte daher in die Kategorie der »verbundenen Dienstdaten« einzuordnen sein; dagegen spricht wiederum, dass auch manche »eindeutigen« Produktdaten, wie z. B. die KfZ-Geschwindigkeit, auf einer absichtlichen Nutzerhandlung basieren und ggf. sogar durch frühere Handlungen beeinflusst sind (Einstellung am Tempomat, Geschwindigkeitslimit).

2.1.4.5 Zusammenfassung

Der Begriff der »verbundenen Dienstdaten« ist eng mit dem »verbundenen Dienst« verknüpft. Nach Art. 2 Nr. 16 DA sind verbundene Dienstdaten solche, die Nutzerhandlungen oder Vorgänge im Zusammenhang mit einem vernetzten Produkt »digitalisieren«. Diese Daten werden entweder absichtlich vom Nutzer aufgezeichnet oder entstehen als Nebenprodukt der Nutzerhandlung während der Bereitstellung des verbundenen Dienstes durch den Anbieter. Der Fokus liegt auf Daten, die durch die Interaktion des Nutzers mit dem Dienst entstehen und sich auf das vernetzte Produkt beziehen. Im Gegensatz dazu sind Produktdaten solche, die direkt durch die Nutzung des vernetzten Produkts selbst generiert werden. Der Hauptunterschied liegt in der

[98] EG 15 DA.
[99] EG 15 DA.
[100] EG 25 DA.

Herkunft und dem Auslöser der Daten: Produktdaten stammen direkt vom physischen Gerät, während verbundene Dienstdaten aus der Interaktion mit einem digitalen Dienst resultieren.

2.1.5 Handelt es sich um einen virtuellen Assistenten? (Art. 2 Nr. 31 DA)

Filipp Revinzon, LL.M., Vay Technology GmbH

EG 23 DA

> Art. 2 Nr. 31 DA: »virtuelle Assistenten« Software, die Aufträge, Aufgaben oder Fragen verarbeiten kann, auch aufgrund von Eingaben in Ton- und Schriftform, mit Gesten oder Bewegungen, und die auf der Grundlage dieser Aufträge, Aufgaben oder Fragen den Zugang zu anderen Diensten gewährt oder die Funktionen von vernetzten Produkten steuert;

2.1.5.1 Schutzzweck

Der Europäische Gesetzgeber sieht in virtuellen Assistenten eine immer mehr genutzte alternative Nutzungsform zur klassischen Bedienung vernetzter Geräte. Mit Blick auf die Digitalisierung des Verbraucherumfelds sowie des beruflichen Umfelds stellen virtuelle Assistenten – so die Annahme – eine benutzerfreundliche Schnittstelle für die Wiedergabe von Inhalten, die Erlangung von Informationen oder Aktivierung von mit dem Internet verbundenen Produkten dar.

Die Entwicklung der vergangenen Jahre bestätigt diese Einschätzung eindrucksvoll: Verbraucher interagieren beispielsweise in Smart-Home-Umgebungen immer häufiger per Sprachbefehl mit vernetzten Geräten, während die klassische Bedienung über Touchscreens oder Smartphone-Apps deutlich an Bedeutung verliert.

Vor diesem Hintergrund wird der durch den Europäischen Gesetzgeber partiell angeordnete Gleichlauf virtueller Assistenten mit vernetzten Produkten bzw. verbundenen Diensten insbesondere gemäß Art. 1 Abs. 4 DA und EG 23 DA besser nachvollziehbar – ersetzen virtuelle Assistenten bereits heute die ursprünglich-klassische Interaktionsart von Benutzern mit vernetzten Produkten, so sollten für diese auch, soweit möglich und nötig, vergleichbare Regeln gelten.

2.1.5.2 Definition

Der DA definiert »virtuelle Assistenten« in Art. 2 Nr. 31 DA als Software, die Aufträge, Aufgaben oder Fragen verarbeiten kann, auch aufgrund von Eingaben in Ton- und Schriftform, mit Gesten oder Bewegungen, und die auf der Grundlage dieser Aufträge, Aufgaben oder Fragen den Zugang zu anderen Diensten gewährt oder die Funktionen von vernetzten Produkten steuert.

Mit Blick auf das Regelungsziel des DA sollen im Kontext von virtuellen Assistenten insbesondere spezifische und im weiteren Verlauf näher zu erläuternde Daten aus der Interaktion mit virtuellen Assistenten unter das Datenzugangsrecht fallen, d. h. unterschiedlichen Akteuren am Markt in Echtzeit und ohne Zusatzkosten übertragen bzw. zugänglich gemacht werden können.

Welche Daten konkret unter das Zugangsrecht fallen, zeigt der folgende Abschnitt.

2.1.5.3 Anwendungsbeispiele

Der Europäische Gesetzgeber sieht in virtuellen Assistenten »zentrale [...] Zugangstore [..., die] erhebliche Mengen relevanter Daten darüber erfassen, wie Nutzer mit Produkten interagieren, die mit dem Internet verbunden sind, einschließlich solcher, die von Dritten hergestellt werden, und [das Potenzial haben] die Nutzung der vom Hersteller bereitgestellten Schnittstellen, wie Touchscreens oder Smartphone-Apps, [zu] ersetzen.«

Anwendungsbeispiele von virtuellen Assistenten im Sinne der Definition können somit beispielsweise Mobile-Device-Software, Smart-Home-Einrichtungen, oder Auto-Assistenten sein.

Nicht erfasst sind hingegen beispielsweise reine Informations- oder Automatisierungs-Chat-Bots, die zwar Text verarbeiten und Fragen beantworten, aber keine Geräte- oder Dienstaktionen im engeren Sinne auslösen können.

2.1.5.4 Positiv- und Negativbeispiele

Vor dem Hintergrund des partiellen Gleichlaufes virtueller Assistenten mit vernetzten Produkten bzw. verbundenen Diensten insbesondere gemäß Art. 1 Abs. 4 DA und EG 23 DA sollen nur solche Daten vom Umfang DA erfasst sein, die »aus der Interaktion zwischen dem Nutzer und einem vernetzten Produkt oder verbundenen Dienst über den virtuellen Assistenten anfallen […]«. Daten, die hingegen »[v]om virtuellen Assistenten erstellt [… werden, und] nicht mit der Verwendung eines vernetzten Produkts oder verbundenen Dienstes zusammenhängen«, bleiben außen vor.

Konkret unterscheidbar sind hierbei die folgenden Datenkategorien:

- Roh-Audio, z. B. Sprachbefehle;
- Transkripte, z. B. ausgeschriebene Texte ausgesprochener Sätze;
- Intent-Payload, z. B. JSON-Dateien;
- Produktsensorik, z. B. Temperatur, GPS-Kennzahlen, Drehzahlwerte;
- Kontext-Parameter, z. B. Time-Stamps, Batteriestatus der verwendeten Hardware oder der Geräuschpegel in der Umgebung;
- ML-Modell-Logs, z. B. Trainings- und/oder Versionsprotokolle;
- System-Health-Logs, z. B. Speicherstatus, CPU-Auslastung etc.

Nicht erfasst sind hingegen intern aggregierte Statistiken und Auswertungen wie z. B. Logs von Werbeeinspielungen, Crashes u. ä.

2.1.5.5 Veranschaulichung am Beispiel

Am Beispiel eines Smart-Home-Assistenten lässt sich dies wie folgt veranschaulichen: sowohl die Roh-Audio-Datei der durch Nutzer gesprochenen Wörter als auch der reine Text »Bitte dimme das Licht um 50%« wären erfasst. Ebenso erfasst wären der Intent-Payload {intent:"SetBrightness",slots:{value:"20"}} als JSON-Datei sowie die individuellen Zuordnungs-IDs des Dimmers sowie die Werte der ursprünglichen und neuen Helligkeitsstufe. Zugleich erfasst werden das konkrete Setting bei Abgabe des Sprachbefehls, also der Interaktionszeitpunkt mit dem Smart-Home-Assistenten, die Lautstärke der Umgebung (str.) sowie die konkrete Positionierung des Assistenten im

Raum (str.). Schließlich sind die Versionsnummer des Assistenten und aktuelle Auslastung (u. a. Speicherauslastung, Rechenleistung und Akkustand) der verwendeten Hardware erfasst. Nicht erfasst wären hingegen Hersteller-interne Statistiken (z.B. 0,8% der Nutzer haben am Stichtag die Dimm-Funktion in kategorisierbaren Intervallen verwendet), oder beispielsweise interne Akustik-Modellierungs-Systeme, um die Stimme des Assistenten im Raum besser ausrichten und anpassen zu können respektive Informationen zur Hardware etc.

2.1.5.6 Zusammenfassung

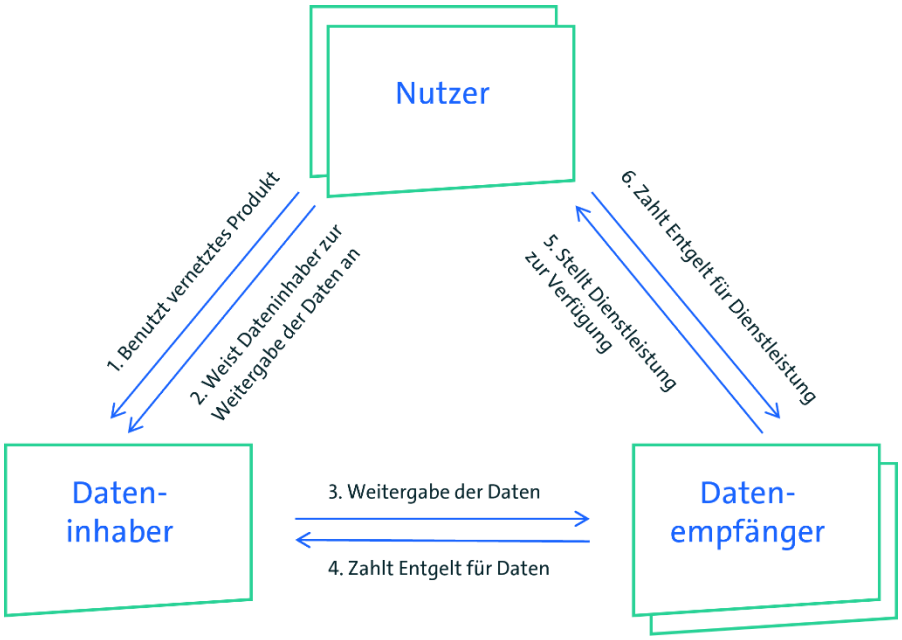
Virtuelle Assistenten haben sich in den letzten Jahren vom reinen Gadget hin zum bevorzugten Interface vernetzter Produkte entwickelt. Sie verdrängen Schritt für Schritt die bislang 'klassischen' Touch- und App-Bedienungen im Smart-Home-Umfeld. Der DA greift diese Entwicklung auf, indem er virtuelle Assistenten weitgehend denselben Pflichten unterwirft wie vernetzte Produkte bzw. verbundene Dienste.

Während die durch den DA erfassten Datenkategorien grundsätzlich normativ klar abgrenzbar sind, werden praktische Anwendungsfragen herausfordernd bleiben; insbesondere zur konkreten Abgrenzung virtueller Assistenten von verbundenen Diensten, die künftig vor allem eine funktionsbezogene Betrachtung im Einzelfall erfordern wird.

2.2 Persönlicher Anwendungsbereich

Dr. Lukas Semmelmayer, LL.B. Digital Law, Syndikusrechtsanwalt, ADAC e.V.

2.2.1 Bin ich Dateninhaber? (Art. 2 Abs. 13 DA)



Semmelmayer, 2025.

> Art. 2 Nr. 13 DA: »Dateninhaber« [ist] eine natürliche oder juristische Person, die nach dieser Verordnung, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat;

2.2.1.1 Positivliste

Dateninhaber ist, wer rechtmäßig Daten sammelt, die der Nutzer eines vernetzten Produkts oder verbundenen Dienstes (z.B. IoT-Geräte bzw. damit verbundene Companion-Apps oder virtuelle Assistenten, vgl. Abschnitt 2.1) generiert[101]. Da Hersteller vernetzter Produkte[102] und Entwickler verbundener Dienste[103] in der Regel die Kontrolle über den Zugang zu generierten Daten haben, gelten sie als Dateninhaber im Sinne des DA[104]. Vernetzte Produkte können so konzipiert sein, dass bestimmte Daten direkt von einem Datenspeicher auf dem Gerät oder von einem entfernten Server, an den die Daten übermittelt werden, zugänglich gemacht werden. Bei dem Server kann es sich um die eigenen lokalen Serverkapazitäten des Herstellers oder um die eines Dritten oder eines Cloud-Diensteanbieters handeln.[105]

Der DA gilt für Hersteller vernetzter Produkte, die in der Europäischen Union in Verkehr gebracht werden, sowie für Anbieter verbundener Dienste in der Europäischen Union, unabhängig vom Ort ihrer Niederlassung[106].

Mit der Dateninhaberschaft fällt oftmals die datenschutzrechtliche Verantwortlichkeit gem. Art. 4 Nr. 7 DSGVO zusammen.[107] Auftragsverarbeiter gem. Art. 4 Nr. 8 DSGVO

[101] Art. 2 Nr. 13 DA verweist auf eine Verpflichtung »nach dieser Verordnung«, die wiederum von der Definition des Dateninhabers abhängt, was als Zirkelschluss angesehen wird. Überdies gilt der letzte Halbsatz des Art. 2 Nr. 13 DA, der lediglich darauf abstellt, dass der Dateninhaber Daten »während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat«, als redaktionelles Versehen des Gesetzgebers. Auch die sonstige Generierung von Produktdaten ist nach dem Sinn und Zweck des Data Act von der Definition erfasst (Frank/Freifrau von Imhoff, RInPrax 2025, 51 Rn. 6).
[102] BeckOK DatenschutzR/Schemmel, Art. 3 DA Rn. 6; Assion/Willecke, MMR 2023, 805 (807); Hartl/Vogel, LTZ 2024, 104 (107).
[103] BeckOK DatenschutzR/Schemmel, Art. 3 DA Rn. 6; Assion/Willecke, MMR 2023, 805 (807).
[104] Vgl. EG 6 S. 1, 14 und 22 DA; Specht-Riemenschneider, MMR 2022, 809 (813); Störing/Mondry, RInPrax 2024 Rn. 13; Hartl/Vogel, LTZ 2024, 104 (105); Bomhard/Merkle, RDi 2022, 168 Rn. 6.
[105] BeckOK DatenschutzR/Schild, Art. 2 DA Rn. 80; vgl. EG 22 DA.
[106] Sog. Marktortprinzip, Art. 1 Abs. 3 lit. a DA.
[107] Assion/Willecke, MMR 2023, 805 (807); Paal/Cornelius/Seeland, RDV 2025, 5 (9).

gelten hingegen nicht als Dateninhaber, da sie Daten nur im Auftrag des Herstellers verarbeiten[108]. Die Verpflichtungen aus der DSGVO bleiben vom DA unberührt[109].

Neben natürlichen Personen, wie Einzelkaufleuten, und juristischen Personen, wie Aktiengesellschaften und Gesellschaften mit beschränkter Haftung, können grundsätzlich auch Personengesellschaften, wie offene Handelsgesellschaften und Kommanditgesellschaften, Dateninhaber sein.

2.2.1.2 Grenzfälle

Umstritten ist, ob auch Verkäufer und Vermieter von vernetzten Produkten oder Anbieter von verbundenen Diensten Dateninhaber sein können.[110] Hiergegen spricht, dass nur Hersteller und Entwickler die notwendigen Zugriffsmöglichkeiten technisch umsetzen können. Verkäufer, Vermieter oder Anbieter sind hierzu üblicherweise nicht in der Lage, es sei denn, sie sind gleichzeitig auch Hersteller bzw. Entwickler.[111]

2.2.1.3 Negativliste

Während der Begriff »Dateninhaber« öffentliche Stellen im Allgemeinen nicht einschließt, kann er öffentliche Unternehmen umfassen[112]. Personen, die eine rein faktische Kontrolle über Produktdaten oder damit verbundene Dienstleistungsdaten erlangen, wie beispielsweise Arbeitnehmer, Auditoren oder Hacker, gelten nicht als Dateninhaber.[113] Auch Kleinst- und Kleinunternehmen sind von der Verpflichtung zur Zugänglichmachung von Produktdaten und verbundenen Dienstdaten ausgenommen (Unternehmen, die weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 10 Mio. Euro nicht überschreitet)[114]. Das Gleiche gilt für Unternehmen, die seit weniger als einem Jahr als mittlere Unternehmen einzustufen sind (Unternehmen, die weniger als 250 Personen beschäftigen und deren Jahresumsatz 50 Mio. Euro bzw. dessen Jahresbilanz 43 Mio. Euro nicht überschreitet). Für diese mittleren Unternehmen sowie für ihre vor weniger als einem Jahr auf den Markt gebrachten vernetzten Produkte gilt eine Übergangszeit[115].

Es ist auch möglich, dass eine Person Nutzer eines vernetzten Produkts ist, ohne dass es einen Dateninhaber gibt. Dies könnte bspw. der Fall sein, wenn ein Nutzer ein vernetztes Produkt erwirbt, bei dem die Daten direkt auf den Rechner des Nutzers übertragen werden und der Hersteller keinen Zugriff auf die Daten hat. In diesem Fall gibt es keinen Dateninhaber, da nur der Nutzer Zugriff auf die Daten hat.[116]

[108] Vgl. EG 22 DA.
[109] Vgl. EG 7 DA.
[110] Schmidt-Kessel, MMR 2024, 75 (77ff.); Hartl/Vogel, LTZ 2024, 104 (107).
[111] HK-DatenR/Denga, Art. 2 DA Rn. 63; BeckOK DatenschutzR/Schemmel, Art. 3 DA Rn. 6.
[112] Vgl. EG 63 DA.
[113] Bomhard/Merkle, RDi 2022, 168 Rn. 6.
[114] Vgl. Art. 7 Abs. 1 UAbs. 1 und EG 41 DA.
[115] Vgl. Art. 7 Abs. 1 UAbs. 2, EG 41 DA; HK-DatenR/Denga, Art. 2 DA Rn. 62.
[116] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 16, https://ec.europa.eu/newsroom/dae/redirection/document/108144.

2.2.2 Bin ich Nutzer? (Art. 2 Abs. 12 DA)

EG 18 DA

> Art. 2 Nr. 12 DA: »Nutzer« [ist] eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt;

2.2.2.1 Positivliste

Nutzer sind natürliche oder juristische Personen, die Eigentümer eines vernetzten Produkts oder Inhaber bestimmter Rechte auf Zugang zum vernetzten Produkt sind (z. B. aufgrund Miet- oder Leasingvertrag), sowie Personen, die verbundene Dienste für das vernetzte Produkt in Anspruch nehmen[117].

Für die Nutzung datengenerierender vernetzter Produkte ist in der Regel die Einrichtung eines Nutzerkontos erforderlich.[118] Ein solches Konto ermöglicht die Identifizierung des Nutzers durch den Dateninhaber (vgl. Abschnitte 2.4.4 und 6.2.2). Es kann auch als Kommunikationsmittel und zur Einreichung und Bearbeitung von Anträgen auf Datenzugang verwendet werden. Der Zugang sollte dem Nutzer auf der Grundlage einfacher Antragsverfahren gewährt werden, die eine automatische Ausführung ermöglichen und keine Prüfung oder Genehmigung durch den Hersteller oder Dateneigner erfordern. Ist eine automatische Ausführung des Antrags auf Datenzugriff nicht möglich, sollte der Hersteller den Nutzer darüber informieren, wie er anderweitig auf die Daten zugreifen kann. Zudem sollte es den Nutzern ermöglicht werden, ihre Konten und die damit verbundenen Daten zu löschen, insbesondere wenn das Eigentum an dem Produkt auf eine andere Person übertragen wird oder wenn andere Personen das vernetzte Produkt nutzen[119].

Sind mehrere Entitäten als Nutzer anzusehen, z. B. bei gemeinsamem Eigentum oder wenn Eigentümer, Mieter oder Leasingnehmer gemeinsame Rechte auf Zugang zu den Daten oder an deren Nutzung haben, so sollte es die Gestaltung des vernetzten Produkts oder Dienstes jedem Nutzer ermöglichen, auf die von ihm erzeugten Daten zuzugreifen. Hersteller oder Entwickler eines vernetzten Produkts, das in der Regel von mehreren Personen genutzt wird, sollten die erforderlichen Mechanismen vorsehen,

[117] EG 18 DA.
[118] HK-DatenR/Denga, Art. 2 DA Rn. 58.
[119] Vgl. EG 21 DA; EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 22, https://ec.europa.eu/newsroom/dae/redirection/document/108144.

damit gegebenenfalls getrennte Benutzerkonten für verschiedene Personen eingerichtet oder dasselbe Benutzerkonto von mehreren Personen genutzt werden kann[120].

Der Nutzer des vernetzten Produkts oder verbundenen Dienstes muss in der EU ansässig sein[121]. Neben natürlichen Personen, wie Verbrauchern, können auch Unternehmen, unabhängig von ihrer Rechtsform, Nutzer sein.[122]

2.2.2.2 Negativliste

Der Nutzer muss zur Nutzung rechtlich befugt sein, zumindest als berechtigter Besitzer. Ausgeschlossen sind rein tatsächliche unberechtigte Nutzungen.[123]

> Art. 2 Nr. 14 DA: »Datenempfänger« [ist] eine natürliche oder juristische Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und dem vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer rechtlichen Verpflichtung aus anderem Unionsrecht oder aus nationalen Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen wurden, Daten bereitstellt;

2.2.3 Bin ich Datenempfänger? (Art. 2 Abs. 14 DA)

2.2.3.1 Positivliste

Das grundlegende Prinzip des DA ist die Autonomie des Nutzers über die von ihm generierten Daten. Grundsätzlich werden Daten gemäß des DA daher nur auf Antrag des Nutzers an einen Datenempfänger weitergegeben (vgl. Abschnitt 2.5).[124] Über das Nutzerkonto (vgl. Abschnitt 2.2.2.1) sollte es die Möglichkeit geben, einen solchen Antrag zu stellen. Der DA ermöglicht es, Nutzern vernetzter Produkte, Folgemarkt-

[120] Vgl. EG 21 DA.
[121] Art. 1 Abs. 3 lit. b DA.
[122] Hartl/Vogel, LTZ 2024, 104 (106).
[123] Specht-Riemenschneider, MMR 2022, 809 (813f.); HK-DatenR/Denga, Art. 2 DA Rn. 53.
[124] HK-DatenR/Denga, Art. 2 DA Rn. 66.

Dienste, Nebendienste und sonstige Dienste zu nutzen, die auf Daten basieren, welche von in diesen Produkten eingebauten Sensoren erhoben wurden[125]. Der Datenempfänger ist gegenüber dem Nutzer umfassend verpflichtet[126]. Der vom DA oftmals zitierte »Dritte«, ist ein Unterfall des Datenempfängers.[127]

Neben natürlichen Personen und juristischen Personen können auch Personengesellschaften Datenempfänger sein, soweit sie zu Zwecken ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handeln.

2.2.3.2 Grenzfälle

Erhält ein Datenempfänger auf Antrag des Nutzers Daten von einem Dateninhaber, ist er nicht berechtigt, diese Daten an einen anderen Dritten weiterzugeben oder vom Dateninhaber zu verlangen, dass die Daten direkt an einen Dritten übermittelt werden, es sei denn, der Nutzer verlangt dies[128]. Der Sinn und Zweck des DA spricht jedoch dafür, dass ein Auftragsverarbeiter, der ausschließlich im Namen und unter der Kontrolle des Datenempfängers handelt, kein »weiterer Dritter« im Sinne des DA ist, sondern im Lager des Datenempfängers steht[129]. Die entscheidende Frage ist daher in der Praxis, ob ein technischer Vermittler als »anderer Dritter« im Sinne von Art. 6 Abs. 2 lit. c DA (mit den beschriebenen Einschränkungen) anzusehen ist oder ob er in den Bereich der Datenempfänger fällt, d. h. als Teil des Datenempfängers zu betrachten ist.

2.2.3.3 Negativliste

Der Datenempfänger muss seinen Sitz in der Europäischen Union haben, damit ihm Daten bereitgestellt werden können[130]. Die Parteien können zwar freiwillig vereinbaren, Daten an einen Empfänger außerhalb der EU (innerhalb der Grenzen der DSGVO) weiterzugeben, doch kann der Dateninhaber nach dem DA nicht dazu verpflichtet werden.[131]

Keine tauglichen Datenempfänger sind sog. »Torwächter« (engl. »Gatekeeper«) im Sinne des DMA (vgl. Art. 5 Abs. 3 DA; ausführlich hierzu Abschnitt 2.5.4). Angesichts der weitgehenden Möglichkeiten dieser Unternehmen, Daten zu erwerben, ist es nach dem DA nicht obligatorisch, solchen Torwächtern ein Datenzugangsrecht einzuräumen[132].

[125] EG 16 DA.
[126] Vgl. Art. 6 DA.
[127] Specht-Riemenschneider, MMR 2022, 809 (821); Störing/Mondry, RInPrax 2024 Rn. 15.
[128] Vgl. Art. 6 Abs. 2 lit. c DA.
[129] Vgl. auch EG 22 und 40 DA.
[130] Vgl. Art. 1 Abs. 3 lit. d und EG 5 DA.
[131] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 23, https://ec.europa.eu/newsroom/dae/redirection/document/108144.
[132] Vgl. EG 40 DA; EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 23, https://ec.europa.eu/newsroom/dae/redirection/document/108144.

2.3 Design Obligation (Art. 3 DA)

Valentino Halim, Rechtsanwalt Tech, Data & AI, Junior Partner, Oppenhoff & Partner Rechtsanwälte Steuerberater mbB

EG 20, 21, 22, 24, 25 DA

Entsprechend den Regelungszielen des DA sollen Nutzer direkten Zugang zu Daten erhalten, die während der Nutzung von vernetzten Produkten oder verbundenen Diensten generiert werden. [133]

Art. 3 Abs. 1 DA sieht eine entsprechende »Designpflicht« (design obligation) für Hersteller vernetzter Produkte und Anbieter verbundener Dienste vor. Danach sind vernetzte Produkte und verbundene Dienste by design so zu konzipieren und zu gestalten, dass Produktdaten und verbundene Dienstdaten für Nutzer zugänglich sind (access by design).[134] Hersteller und Anbieter müssen den Datenzugang bereits in der Entwicklungsphase von Produkten und Diensten berücksichtigen. Dies muss by default, also standardmäßig erfolgen.[135]

Dies bedeutet, dass vernetzte Produkte und verbundene Dienste so gestaltet werden müssen, dass die generierten Produktdaten und verbundenen Dienstdaten zugänglich sind. Dies umfasst zusätzlich auch relevante Metadaten, die für die Nutzung und Interpretation der generierten Daten erforderlich sind. Diese Verpflichtung soll sicherstellen, dass Nutzer ihre Daten effektiv nutzen können.

Für die design obligation gilt eine Übergangsfrist. Hersteller und Anbieter müssen access by design für vernetzte Produkte und verbundene Dienste gewährleisten, die nach dem 12. September 2026 in Verkehr gebracht werden.[136] Anders als bzgl. des

[133] Vgl. EG 22 DA.
[134] Vgl. Wilkening/Müller, DB 2024, 166 (167).
[135] Antoine, CR 2024, 1 (2).
[136] Siehe Art. 50 DA.

Inverkehrbringens von vernetzten Produkten finden sich dazu in den DA FAQ jedoch keine Erläuterungen bezüglich verbundener Dienste.[137] Allerdings ist die Dauer der Entwicklungszyklen des jeweiligen Produkts oder Dienstes zu berücksichtigen. In vielen Fällen sind die Vorgaben zum Datenzugang by design bereits jetzt im Rahmen der Forschung und Entwicklung zu beachten.

2.3.1 Art und Weise der Bereitstellung (Art. 3 Abs. 1 DA)

Der DA macht detaillierte Vorgaben zur Art und Weise der Bereitstellung. Zum einen soll der Datenzugang einfach, sicher und für den Nutzer stets unentgeltlich sein. Zum anderen sind die Daten in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format bereitzustellen – wenn möglich in elektronischer Form.[138]

Der Zugang zu Daten ist »einfach«, wenn die Daten ohne unverhältnismäßigen Aufwand bereitgestellt werden können. Daran fehlt es nicht schon deshalb, weil der Zugang einen gewissen Bearbeitungsaufwand erfordert. Indes ist der Zugang nicht mehr einfach, wenn das vernetzte Produkt nicht dafür ausgelegt ist, Daten direkt am Gerät abzurufen,[139] z. B. weil es über keine datenfähige Nutzerschnittstelle verfügt. Maßgeblich ist, ob die technische Gestaltung des Produkts einen unmittelbaren Datenzugriff erlauben, oder ob zusätzliche Maßnahmen erforderlich sind, die über den normalen Bearbeitungsaufwand hinausgehen.

»Maschinenlesbar« sind Dokumente, die so strukturiert sind, dass die darin enthaltenen Daten und deren Struktur leicht von Software erkannt und extrahiert werden kann.[140] Dazu zählen z. B. Formate wie XML oder CSV, während dies auf PDF-Dateien nicht zutrifft. Nicht alle elektronischen Formate eignen sich gleichermaßen für die weitere Verarbeitung. Es bleibt abzuwarten, ob sich z. B. in bestimmten Sektoren Formatstandards herausbilden.[141]

2.3.2 Direkter Datenzugriff (Art. 3 Abs. 1 DA)

Dabei muss die Bereitstellung – soweit dies relevant und technisch durchführbar ist – direkt erfolgen. Ist ein direkter Datenzugang nicht möglich, etwa aus technischen Gründen, kann der Nutzer vom Dateninhaber verlangen, die ohne weiteres verfügbaren Daten (einschließlich Metadaten), entweder direkt an ihn[142], oder unmittelbar an einen Dritten[143] bereitzustellen.

2.3.3 Positivbeispiele für direkten Datenzugriff (Art. 3 Abs. 1 DA)

[137] DA; EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 9, https://ec.europa.eu/newsroom/dae/redirection/document/108144.
[138] Antoine, CR 2024, 1 (5).
[139] Vgl. nach EG 20.
[140] Siehe EG 21 RL 2013/37/EU.
[141] Ausführlich Kaesling, GRUR 2024, 821 (825).
[142] Art. 4 Abs. 1 DA.
[143] Art. 5 Abs. 1 DA.

Der Anforderung des access by design wird etwa Genüge getan, wenn der Hersteller oder Anbieter eine Benutzeroberfläche bereitstellt, über die der Nutzer die entsprechenden Daten entweder direkt vom vernetzten Gerät oder von einem externen Server des Herstellers bzw. Anbieters oder eines Dritten (z.B. eines Cloud-Dienstanbieters) abrufen kann.[144] Nutzen mehrere Nutzer ein IoT-Gerät, ist es aufgrund der daraus resultierenden unterschiedlichen Berechtigungen zur Nutzung möglich und angezeigt, den Zugang zu den jeweiligen Daten über individuelle Nutzerkonten zu regeln.[145]

2.3.4 Lesbarkeit als direkter Datenzugriff (Art. 3 Abs. 1 DA)

Der DA regelt nicht ausdrücklich, was mit »Zugänglichmachung« von Produktdaten oder verbundenen Dienstdaten gemeint ist. So ist bislang nicht geklärt, ob es hierfür genügt, einen sog. In-situ-Zugang (lat. »am (Ursprungs-)Ort«) einzurichten, bei dem die Daten nur in einer geschützten Umgebung des Dateninhabers einsehbar sind. Bejahendenfalls würde die bloße Lesbarkeit der Daten ausreichen, um der Datenzugangspflicht zu genügen, was erhebliche Beschränkungen für den Nutzer bedeuten kann. Die mögliche Datennutzung hängt schließlich von der technischen Umgebung ab, die der Dateninhaber z. B. in dem bereitgestellten Gerät implementiert hat.[146]

Überwiegend wird dies mit Verweis auf eine erhöhte Datensicherheit für ausreichend gehalten,[147] da bei einem In-situ-Zugang z. B. Datenübermittlungen entfielen. Indes widerspricht die Beschränkung auf einen solchen Zugang den Zielen des DA, da die Nutzbarkeit der Daten und deren Integration mit Daten anderer Dateninhaber erheblich erschwert würde. Behörden und Gerichte könnten daher die bloße Lesbarkeit in einer vom Dateninhaber bestimmten In-situ-Umgebung als unzureichend für eine »Zugänglichmachung« einstufen. Unternehmen sind in dieser praxisrelevanten Frage bis zu einer gerichtlichen Klärung einer Rechtsunsicherheit ausgesetzt.[148]

Das Datenzugangsrecht gilt nicht absolut. Vielmehr kann der Datenzugang eingeschränkt sein, um den Schutz von Geschäftsgeheimnissen, die Produktsicherheit oder den Schutz personenbezogener Daten zu gewährleisten (siehe insb. Abschnitte 1.4.1 und 1.4.2).[149]

2.3.5 Informationspflichten (Art. 3 Abs. 2, 3 DA)

Ergänzend zu access by design enthält der DA vorvertragliche datenbezogene Informationspflichten, die gegenüber dem Nutzer von vernetzten Produkten und

[144] Vgl. EG 22 DA.
[145] Vgl. EG 21 DA.
[146] Ehlen/Sebulke CR 2024, 84 (86); Mendelsohn/Richter in Steinrötter, »Europäische Plattformregulierung«, 1. Aufl. 2023, § 20 Rn. 37.
[147] Specht-Riemenschneider MMR 2022, 809 (815); Kaesling GRUR 2024, 821 (824); Ehlen/Sebulke CR 2024, 84.
[148] Ehlen/Sebulke CR 2024, 84 (86).
[149] Apel/Huber, JuS 2024, 410 (412).

Anbietern von verbundenen Diensten vor Abschluss eines Kauf-, Miet- oder Leasingvertrags über ein vernetztes Produkt erfüllt werden müssen[150].

Vor Abschluss eines entsprechenden Vertrages muss der Verkäufer, Vermieter oder Leasinggeber – der auch der Hersteller sein kann – dem Nutzer klare und verständliche Informationen über die vom Produkt generierten Daten bereitstellen[151]. Dies umfasst Angaben zu Art, Format und geschätzter Menge der Daten, und – soweit verfügbar – zu Datenstrukturen, Formaten, Klassifizierungssystemen, Taxonomien und Codelisten. Zudem sind Angaben zur Ausübung der Nutzerrechte, zur Speicherung und zum Abruf der Daten sowie zu den Nutzungsbedingungen und der Dienstqualität von Schnittstellen (z. B. APIs) oder Software Development Kits bereitzustellen.[152]

Die Informationspflicht kann z. B. durch eine gleichbleibende URL-Adresse erfüllt werden, die als Weblink oder QR-Code zugänglich ist und auf die relevanten Informationen verweist. Es muss dem Nutzer möglich sein, die Informationen zu speichern und unverändert wiederzugeben. Zwar ist der Verkäufer, Vermieter oder Leasinggeber nicht verpflichtet, die Daten unbegrenzt zu speichern. Er sollte aber eine angemessene Speicherdauer festlegen.

Für den Erwerb von verbundenen Diensten sieht Art. 3 Abs. 3 DA entsprechende vorvertragliche Informationspflichten vor. Diese sind umfangreicher und umfassen zusätzlich z. B. Angaben dazu, ob der Dateninhaber beabsichtigt, Dritten die Datennutzung im Rahmen der vereinbarten Zwecke zu gestatten.

Die vorvertraglichen Informationen erleichtern dem Nutzer den Datenzugang. Ändern sich die Informationen während der Lebensdauer des Produkts oder der Vertragslaufzeit, etwa durch einen geänderten Verwendungszweck der Daten, müssen diese Änderungen dem Nutzer ebenfalls mitgeteilt werden.

Diese Informationspflicht tritt neben die Informationspflichten nach Art. 12, 13, 14 DSGVO, die betroffenen Personen in der Praxis in Datenschutzinformationen (sog. Datenschutzerklärungen) bereitzustellen sind. Sie gilt auch für den potenziellen Dateninhaber, wenn ein Vertrag über die Erbringung eines verbundenen Dienstes abgeschlossen wird.

In der Praxis wird der Dateninhaber die Informationen bezüglich des vernetzten Produkts nur in vergleichsweise wenigen Fällen selbst dem (End-)Nutzer bereitstellen müssen. Häufig schließt der Dateninhaber lediglich Verträge mit Großhändlern oder Großkunden, nicht aber mit dem (End-)Nutzer. Ist der Dateninhaber nicht Vertragspartner des (End-)Nutzers, trifft ihn die vorvertragliche Informationspflicht nur indirekt.

Auch z.B. bei IoT-Geräten, die vom Erstnutzer auf dem Zweitmarkt weiterverkauft werden, wird die vorvertragliche Informationspflicht des Herstellers in der Praxis eingeschränkt sein.[153] Dieser kann den Nutzerwechsel in der Regel nur dann feststellen, wenn das IoT-Gerät mit einem Nutzerkonto verbunden ist, das eine Registrierung oder Authentifizierung des neuen Nutzers erfordert (vgl. Abschnitt

[150] Art. 3 DA.
[151] Art. 3 Abs. 2 DA.
[152] Vgl. EG 24 DA.
[153] Vgl. dazu im Zusammenhang mit Datennutzungsvereinbarungen Henke, VuR 2024, 403, (405).

2.2.2.1). Ohne eine solche Verknüpfung bleibt der Wechsel des Nutzers für den ursprünglichen Anbieter faktisch unbemerkt, was die Erfüllung der Informationspflicht erschwert.

2.4 Datenteilungspflicht mit Nutzer (Art. 4 DA)

Dr. Robert Wilkens, Rechtsanwalt, Syndikusrechtsanwalt, Regulatory Advisory l Forensic, KPMG AG Wirtschaftsprüfungs-gesellschaft, Leipzig || Stina Neuenfeldt, LL.M., Senior Manager, Regulatory Advisory l Forensic, KPMG AG, Wirtschaftsprüfungs-gesellschaft, Frankfurt a. M. || Tim Sauerhammer, Rechtsanwalt, Reed Smith LLP

EG 20, 26, 27 DA

2.4.1 Indirekter Zugriff (Art. 4 Abs. 1 DA)

EG 15, 20 DA

Soweit das vernetzte Produkt oder der verbundene Dienst den Nutzern keinen direkten Zugang (access by design) ermöglicht (siehe Abschnitt 2.3), müssen die Daten nach Art. 4 Abs. 1 DA jedenfalls indirekt bereitgestellt werden. Indirekte Bereitstellung meint einen Mechanismus, bei dem Nutzer nicht selbst (autonom) auf die Daten zugreifen können, sondern eine Bereitstellung der Daten auf Verlangen gegenüber dem Dateninhaber erfolgt. Ausreichend ist ein einfaches Verlangen der Nutzer auf elektronischem Wege, soweit dies technisch durchführbar ist. Beispielsweise über ein Nutzerkonto, auf dem Nutzer eine Anfrage zum Zugriff auf Daten stellen können (vgl. Abschnitt 2.2.2.1).

Gegenstand der indirekten Bereitstellung sind im Ausgangspunkt alle generierten Rohdaten, sowie Daten, die vor der Weiterverarbeitung und Auswertung aufbereitet wurden, um sie verständlich und nutzbar zu machen (siehe Abschnitt 2.1).

Anders als beim direkten Zugriff müssen aber nur diejenigen Daten bereitgestellt werden, die der Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann, sog. »ohne Weiteres verfügbare Daten«. Daten, die bei der Produktnutzung generiert werden, müssen nicht bereitgestellt werden, wenn das Produkt nicht dafür ausgelegt ist, dass Daten außerhalb der jeweiligen Komponente gespeichert oder übertragen werden. Der Dateninhaber ist lediglich verpflichtet, die Daten in der Form bereitzustellen, in der sie ihm tatsächlich vorliegen. Das bedeutet jedoch nicht, dass der Dateninhaber gezwungen wäre, die von ihm aus den Rohdaten oder den aufbereiteten Daten gewonnenen Erkenntnisse oder Analysen zur Verfügung zu stellen. Auf diese abgeleiteten Daten haben Nutzer grundsätzlich keinen Anspruch (siehe bereits oben 2.1). Es besteht auch keine Pflicht zur Aufbereitung der Rohdaten – etwa durch

Standardisierung oder Bereinigung –, sofern solche Maßnahmen mit wesentlichen Investitionen verbunden wären.

Die Daten müssen (1) unverzüglich, (2) einfach, (3) sicher, (4) unentgeltlich, (5) in einem umfassenden, gängigen und maschinenlesbaren Format, (6) in der gleichen Qualität wie für den Dateninhaber bereitgestellt werden und (7) – soweit relevant und technisch durchführbar – kontinuierlich in Echtzeit.

2.4.2 Vertragliche Beschränkungen (Art. 4 Abs. 2 DA)

EG 30 DA

Der DA sieht vor, dass Dateninhaber und Nutzer ausnahmsweise Einschränkungen hinsichtlich des Zugangs, der Nutzung oder der Weitergabe von Daten vertraglich regeln können. Dies ist jedoch nur unter bestimmten Bedingungen zulässig. Voraussetzung ist, dass gesetzlich festgelegte Sicherheitsanforderungen für ein vernetztes Produkt betroffen sind. In solchen Fällen können Nutzer und Dateninhaber gemeinsam vereinbaren, den Zugang oder die Weitergabe von Daten vertraglich zu beschränken – allerdings nur, wenn andernfalls eine schwerwiegende nachteilige Auswirkung auf die Gesundheit oder Sicherheit von Personen bestehen könnte. Diese Ausnahmeregelung wird auch als »safety and security handbrake« bezeichnet.

Verweigert der Dateninhaber den Zugang zu den Daten unter Berufung auf eine solche Gefährdung, ist er verpflichtet, dies unverzüglich der zuständigen Behörde zu melden und die Gründe für die Entscheidung nachvollziehbar darzulegen.

2.4.3 Wahlmöglichkeiten oder Rechte des Nutzers (Art. 4 Abs. 4 DA)

EG 38 DA

Die Ausübung der Rechte auf indirekte Bereitstellung und die in diesem Zusammenhang bestehenden Wahlmöglichkeiten der Nutzer dürfen nicht unangemessen erschwert werden. Dateninhabern ist es untersagt, Nutzer in ihrer Autonomie, Entscheidungsfreiheit oder Wahlfreiheit zu beeinflussen, etwa durch Anbieten von Wahlmöglichkeiten nicht neutraler Weise oder Tricks in der Gestaltung digitaler Benutzeroberflächen und -schnittstellen. Insbesondere ist es unzulässig, Nutzer durch irreführende oder manipulative Gestaltungen dazu zu bringen, bestimmte (nachteilige) Entscheidungen zu treffen. In diesem Zusammenhang sollten Dateninhaber bei der Gestaltung ihrer digitalen Schnittstellen nicht auf sogenannte »Dark Patterns« zurückgreifen (vgl. Rechtsgedanken des Art. 25 DSA). »Dark Patterns« sind Gestaltungstechniken, die dazu dienen, Nutzer zu ungewollten Entscheidungen zu verleiten oder sie zu täuschen.

Beispiele problematischer Praktiken:

- Gestalten der Benutzerschnittstelle in einer Art und Weise, dass bestimmte Auswahlmöglichkeiten stärker hervorgehoben werden und Nutzer andere Auswahlmöglichkeiten kaum wahrnehmen.

- Manipulieren des Informationsflusses durch Hervorheben oder Weglassen von Informationen.
- Erzeugen einer Drucksituation durch vorgegebene Dringlichkeit.
- Wiederholtes Auffordern der Nutzer, eine Wahl zu treffen, obwohl bereits eine Wahl getroffen wurde.
- Standardmäßiges Ablehnen von Datenzugangsanfragen ohne Prüfung.
- Verlangen offensichtlich nicht erforderlicher oder unangemessener Schutzmaßnahmen.

2.4.4 Überprüfung der Nutzereigenschaft (Art. 4 Abs. 5 DA)

EG 21, 29 DA

Dateninhaber können die Identität eines Nutzers überprüfen, um festzustellen, ob eine Berechtigung auf Zugang zu den Daten besteht.

Nach dem DA soll die Nutzeridentifizierung »geeignet« sein – gleichzeitig aber keine Informationen verlangen, die über das »erforderliche Maß« hinausgehen. In der Praxis wirft dies die Frage auf, wie die Identitätsprüfung zuverlässig erfolgen kann, ohne dabei gegen die Beschränkung der Erforderlichkeit zu verstoßen. Eine klare Abgrenzung und Best Practices fehlen bislang. Klar ist nur, dass der gesamte Prozess für die Nutzer »einfach« und »sicher« gestaltet werden muss (siehe oben zu Art. 4 Abs. 1 DA).

Dateninhaber haben bei der Ausgestaltung des Identifizierungsmechanismus Gestaltungsspielraum. Nach der EU-KOM sollten dabei folgende Faktoren berücksichtigt werden:

- Art des Produkts,
- Typ des Nutzers (z. B. Verbraucher oder gewerblicher Nutzer),
- voraussichtliche Anzahl der Nutzer,
- Häufigkeit der zu erwartenden Datenzugriffe,
- Vorhandensein spezifischer Mechanismen zum Nachweis der Berechtigung (z. B. Registrierung des Fahrzeughalters),
- Kosten der Einrichtung unterscheidbarer Nutzerkonten und deren Benutzerfreundlichkeit.

Das pauschale Fordern von Personalausweis-Scans dürfte in den meisten Fällen zu weit gehen. Die EU-KOM sieht perspektivisch die EU Digital Identity Wallet als mögliche Lösung für die Nutzeridentifizierung. Solange sich diese aber noch in der Entwicklung befindet, bleibt keine andere Möglichkeit, als die Identifikation auf anderem Wege vorzunehmen.

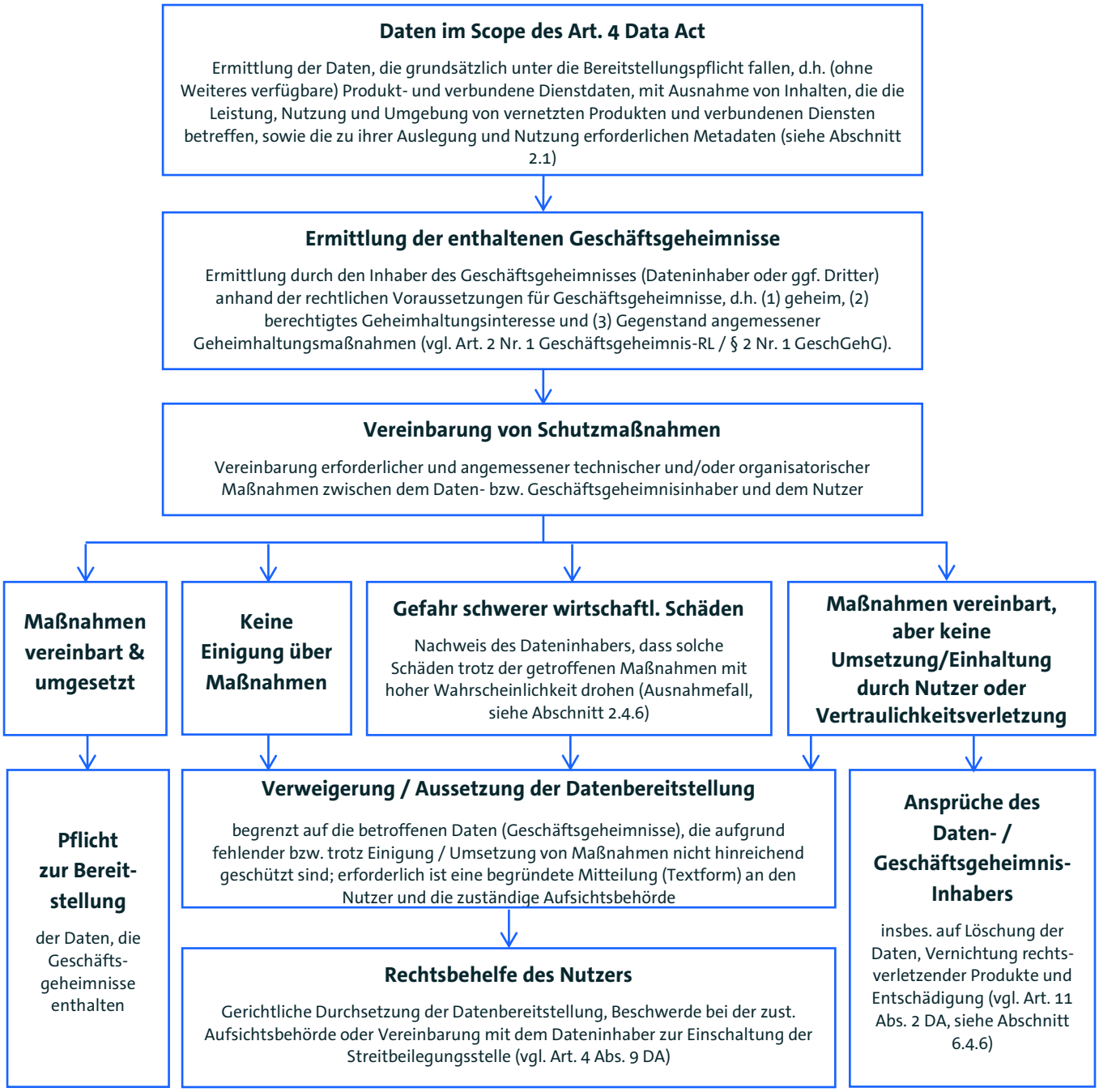
Da die Nutzung vernetzter Produkte in der Regel die Einrichtung eines Nutzerkontos erfordert, liegt es nahe, die Nutzer über dieses Konto in Kombination mit der

persönlichen E-Mail-Adresse zu identifizieren. Soweit mehrere Personen das Produkt nutzen, sollte aber gewährleistet sein, dass eine zuverlässige Zuordnung der Nutzerdaten möglich ist, z.B. durch Einrichtung getrennter Nutzerkonten für einzelne Personen (vgl. Abschnitte 2.2.2.1 und 6.2.2).

Protokolldaten und ähnliche Informationen über den Zugang des Nutzers zu den Daten dürfen nur so lange aufbewahrt werden, wie es für die ordnungsgemäße Bearbeitung des Zugangsverlangens oder für die Sicherheit und Wartung der Dateninfrastruktur erforderlich ist. Da es sich dabei oftmals um personenbezogene Daten handeln dürfte, sind auch die Anforderungen des Datenschutzes zu beachten. Die Speicherung von Informationen sollte daher auf das notwendige Minimum beschränkt werden.

2.4.5 Geschäftsgeheimnisse (Art. 4 Abs. 6, 7 DA)

Dateninhaber müssen grundsätzlich Zugang auch zu solchen Daten gewähren, die Geschäftsgeheimnisse darstellen, jedoch dürfen sie (bzw. der ggf. personenverschiedene Geschäftsgeheimnisinhaber) mit dem Nutzer zuvor bestimmte Schutzmaßnahmen vereinbaren. Nur soweit sich ein Nutzer weigert, solche Maßnahmen zu vereinbaren oder umzusetzen, oder wenn im Einzelfall trotz aller vereinbarten und vom Nutzer umgesetzten Maßnahmen ein schwerer wirtschaftlicher Schaden durch die Offenlegung von Geschäftsgeheimnissen droht (siehe Abschnitt 2.4.6), darf der Dateninhaber die Datenbereitstellung verweigern oder aussetzen, wobei er dies jeweils dem Nutzer und der zuständigen Aufsichtsbehörde in Textform mitteilen und begründen muss. Hält der Nutzer die Verweigerung / Aussetzung für nicht rechtmäßig, kann er seinen Anspruch auf Datenbereitstellung gerichtlich durchsetzen und/oder auf die Rechtsbehelfe nach Art. 4 Abs. 9 DA (Herbeiführung der Entscheidung durch die zuständige Aufsichtsbehörde oder Einschaltung der Streitbeilegungsstelle) zurückgreifen.



Wilkens, Neuenfeldt, 2025.

Der DA ändert somit nichts an den einschlägigen rechtlichen Bestimmungen zum Schutz von Geschäftsgeheimnissen. Allerdings reicht es hierbei nicht aus, dass ein Dateninhaber pauschal behauptet, die bereitzustellenden Daten enthielten Geschäftsgeheimnisse. Vielmehr muss der Dateninhaber bzw. (falls es sich nicht um dieselbe Person handelt) der Inhaber des Geschäftsgeheimnisses zunächst einmal konkret ermitteln, welche der grundsätzlich nach Art. 4 Abs. 1 DA bereitzustellenden Daten (siehe Abschnitt 2.1) als Geschäftsgeheimnisse geschützt sind.

Der DA verweist bei der Definition von »Geschäftsgeheimnissen« auf die Geschäftsgeheimnis-RL, sodass hierbei dieselben Voraussetzungen gelten, d. h. die

Informationen sind geheim und gerade deshalb von kommerziellem Wert und sie sind Gegenstand von den Umständen entsprechend angemessenen Geheimhaltungsmaßnahmen (siehe Abschnitt 1.4.2).

Um solche Geheimhaltungsmaßnahmen auch im Rahmen der Datenbereitstellungspflicht nach dem DA aufrechtzuerhalten, kann der Daten- bzw. Geschäftsgeheimnisinhaber mit dem Nutzer zuvor angemessene technische und organisatorische Maßnahmen vereinbaren, die erforderlich sind, um die Vertraulichkeit der weitergegebenen Daten, insbesondere gegenüber Dritten, zu wahren.

Beispiele für technische und organisatorische Maßnahmen zum Geschäftsgeheimnisschutz:

- Mustervertragsklauseln,
- Vertraulichkeitsvereinbarungen,
- strenge Zugangsprotokolle,
- technische Normen,
- Anwendung von Verhaltenskodizes,
- Verschlüsselung,
- Firewalls,
- getrennte Speicherung,
- Einschaltung einer vertrauenswürdigen dritten Partei

Welche Maßnahmen dabei »erforderlich« und »angemessen« sind, hängt vom konkreten Einzelfall ab. So kann es bspw. einen Unterschied machen, ob dem Nutzer ein Datenzugang dort gewährt wird, wo die Daten gespeichert sind, oder ob die Daten vollständig an den Nutzer übermittelt werden (was deren Nutzbarkeit für den Nutzer erhöht, für den Dateninhaber aber das Maß an Kontrolle reduziert). Mit Blick auf die jeweiligen Umstände müssen die verschiedenen Interessen der Parteien (u. a. Aufwand des Nutzers und dessen Interesse an den Daten; Geheimhaltungsinteresse des Geschäftsgeheimnisinhabers und mögliche Folgen einer Offenlegung) gegeneinander abgewogen werden, ohne dass dabei die beabsichtigte Wirkung des DA unterlaufen wird, möglichst viele Daten verfügbar zu machen.

Sofern die Daten, bei denen es sich um Geschäftsgeheimnisse handelt, grundsätzlich unter die Bereitstellungspflicht fallen, darf der Dateninhaber deren Bereitstellung nur in den folgenden drei Fällen verweigern bzw. aussetzen:

- Mit dem Nutzer konnte keine Einigung über die erforderlichen und angemessenen Schutzmaßnahmen erzielt werden;
- Der Nutzer hat die vereinbarten Maßnahmen nicht umgesetzt oder die Vertraulichkeit der Geschäftsgeheimnisse verletzt oder
- Der Dateninhaber kann nachweisen, dass er aufgrund außergewöhnlicher Umstände trotz der vom Nutzer getroffenen Schutzmaßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch die

Offenlegung von Geschäftsgeheimnissen erleiden wird (siehe zu diesem Ausschlussgrund im Einzelnen Abschnitt 2.4.6).

In allen der drei o.g. Fälle gilt, dass die Verweigerung / Aussetzung nur in Bezug auf die Daten erfolgen darf, für die die genannten Voraussetzungen auch vorliegen. D. h. alle übrigen Daten sind (weiterhin) bereitzustellen. In allen drei Fällen muss der Dateninhaber seine Entscheidung zur Verweigerung / Aussetzung einschließlich einer Begründung sowohl dem betroffenen Nutzer (unverzüglich) als auch der zuständigen Aufsichtsbehörde in Textform mitteilen. Eine ordnungsgemäße Begründung in Bezug auf die Fälle (1) und (2) beinhaltet jedenfalls die Angabe der betreffenden Daten und weshalb es sich bei diesen um Geschäftsgeheimnisse handelt sowie Informationen darüber, welche Maßnahmen nicht vereinbart oder umgesetzt wurden bzw. bei welchen Geschäftsgeheimnissen die Vertraulichkeit verletzt wurde. Die Entwürfe der Mustervertragsklauseln der entsprechenden Expertengruppe der EU-KOM[154] sehen zum Schutz von Geschäftsgeheimnissen insbesondere folgende Vereinbarungen vor:

Mustervertragsklauseln zum Geschäftsgeheimnisschutz insb.:

- Recht des Geschäftsgeheimnisinhabers, nach entsprechender Information an den Nutzer zusätzliche Schutzmaßnahmen einseitig umzusetzen oder solche mit dem Nutzer zu vereinbaren, wenn die zu Beginn vereinbarten Maßnahmen unzureichend sind;
- bei Aussetzen/Verweigern der Datenbereitstellung: Pflicht des Dateninhabers, die bestimmten Daten (die Geschäftsgeheimnisse enthalten) weiter vorzuhalten, bis sie im Rahmen der Vereinbarung bereitgestellt werden können;
- Regelungen zum Umgang mit später hinzukommenden Geschäftsgeheimnissen (insbesondere mit Blick auf ggf. zusätzlich bereitzustellende Daten);
- Informationspflichten des Nutzers gegenüber dem Dateninhaber bei beabsichtigter Weitergabe von Geschäftsgeheimnissen an Dritte sowie
- ggf. Auditrechte, um die Einhaltung der vereinbarten Maßnahmen durch unabhängige Dritte überprüfen zu lassen.

Ist der betroffene Nutzer der Ansicht, dass die Verweigerung / Aussetzung nicht rechtmäßig ist (bspw. weil die Daten gar keine Geschäftsgeheimnisse darstellen oder die verlangten Schutzmaßnahmen nicht erforderlich oder nicht angemessen sind), kann er sein Recht auf Datenbereitstellung gerichtlich durchsetzen. Daneben bietet der DA in Art. 4 Abs. 9 DA jedoch noch zwei weitere Rechtsbehelfe:

[154] Expert Group on B2B data sharing and cloud computing contracts, «Final Report of the Expert Group on B2B data sharing and cloud computing contracts", 02.04.2025, zuletzt abgerufen am 27.08.2025, https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/116180/download.

1. Der Nutzer kann eine Beschwerde bei der zuständigen Behörde einreichen, die daraufhin unverzüglich entscheidet, ob und unter welchen Bedingungen die Weitergabe der Daten beginnt oder wieder aufgenommen wird, oder
2. Der Nutzer kann mit dem Dateninhaber vereinbaren, gemäß Art. 10 Abs. 1 DA eine Streitbeilegungsstelle mit der Angelegenheit zu befassen.

Soweit es sich bei den Daten, die Geschäftsgeheimnisse darstellen, um personenbezogene Daten handelt, ist zudem zu beachten, dass die oben beschriebenen Ausnahmen von den Datenzugangsrechten in keiner Weise die Rechte der betroffenen Personen (bei denen es sich auch um den Nutzer i.S.d. DA handeln kann) auf Zugang und Datenübertragbarkeit gemäß der DSGVO beschränken.

2.4.6 Handbrake-Mechanismus bei außergewöhnlichen Umständen (Art. 4 Abs. 8 DA)

EG 31 DA

Unter außergewöhnlichen Umständen ist die Ablehnung eines Datenzugangsverlangens im Einzelfall zudem dann möglich, wenn der Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, nachweisen kann, dass er trotz der vom Nutzer getroffenen technischen und organisatorischen Maßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch die Offenlegung von Geschäftsgeheimnissen erleiden wird. Der Wortlaut des Gesetzes (»außergewöhnliche Umstände«, »Einzelfall«) deutet bereits darauf hin, dass es sich hierbei um eine eng auszulegende Ausnahmevorschrift handelt.

Ein »schwerer wirtschaftlicher Schaden« geht mit schweren irreparablen wirtschaftlichen Verlusten einher. Alle o.g. Voraussetzungen muss der Dateninhaber »nachweisen« können. Abstrakte Vermutungen reichen hierfür nicht aus, der Nachweis muss vielmehr auf der Grundlage objektiver Fakten hinreichend begründet werden. Der DA nennt in diesem Zusammenhang insbesondere die Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, die Art und den Vertraulichkeitsgrad der verlangten Daten sowie die Einzigartigkeit und Neuartigkeit des vernetzten Produkts. Zudem könnte auch etwaigen negativen Auswirkungen auf die Cybersicherheit Rechnung getragen werden.

Der hinreichend begründete Nachweis ist dem Nutzer vom Dateninhaber unverzüglich in Textform vorzulegen. Darüber hinaus muss der Dateninhaber der zuständigen Aufsichtsbehörde die verweigerte Datenweitergabe mitteilen. Das Datenzugangsverlangen darf hierbei nur für die betroffenen speziellen Daten abgelehnt werden, für die die o.g. Voraussetzungen im Einzelfall auch tatsächlich erfüllt sind; alle übrigen Daten sind hingegen bereitzustellen.

Hält der Nutzer die Ablehnung für nicht rechtmäßig, kann er seinen Anspruch auf Datenbereitstellung gerichtlich durchsetzen und/oder auf die Rechtsbehelfe nach Art. 4 Abs. 9 DA (Herbeiführung der Entscheidung durch die zuständige Aufsichtsbehörde oder Einschaltung der Streitbeilegungsstelle) zurückgreifen.

2.4.7 Non-compete (Art. 4 Abs. 10 DA)

EG 27, 32 DA

Grundsätzlich dürfen Nutzer die unter dem DA erhaltenen Daten zu allen beliebigen (rechtmäßigen) Zwecken verwenden. Um die Innovationsanstrengungen der Dateninhaber bzw. Produkthersteller zu schützen, macht Art. 4 Abs. 10 DA von diesem Grundsatz der freien Verwendbarkeit aber drei Ausnahmen. Danach ist die Nutzung der erhaltenen Daten für folgende Zwecke untersagt:

- Zur (eigenen) Entwicklung eines vernetzten Produkts, das mit dem vernetzten Produkt, von dem die Daten stammen, im Wettbewerb steht;
- zur Weitergabe an einen Dritten mit der Absicht der Entwicklung eines vernetzten Produkts, das mit dem vernetzten Produkt, von dem die Daten stammen, im Wettbewerb steht, oder
- um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers oder ggf. des Dateninhabers zu erlangen.

Ob ein mithilfe der erlangten Daten entwickeltes bzw. zu entwickelndes vernetztes Produkt mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht, ist nach kartellrechtlichen Grundsätzen zu beurteilen. Im Wesentlichen kommt es hierfür darauf an, ob die Produkte auf demselben Produktmarkt miteinander konkurrieren, da sie aufgrund ihrer Merkmale, Preise und Verwendungszwecke von den Nutzern als austauschbar oder ersetzbar betrachtet werden.

Nicht von dem Verwendungsverbot umfasst sind hingegen (auf Basis der erlangten Daten entwickelte) Innovationen, die sich auf nachgelagerte Märkte beziehen, bspw. zu Zwecken der Reparatur oder der Verlängerung der Lebensdauer des vernetzten Produkts, von dem die Daten stammen, oder zur Erbringung diesbezüglicher Folgemarkt-Dienste. Denn in diesem Bereich soll der DA gerade dazu führen, dass mehr Konkurrenz ermöglicht wird. Zu solchen Zwecken dürfen die erlangten Daten daher insbesondere auch für das Reverse Engineering (Nachkonstruktion) genutzt werden, sofern dem nicht das sonstige Unionsrecht oder das nationale Recht (vgl. für Deutschland aber insbesondere die Erlaubnis nach § 3 Abs. 1 Nr. 2 GeschGehG) entgegensteht.

Das Verbot gilt ebenfalls nicht für die Entwicklung verbundener Dienste auf Basis der aus einem vernetzten Produkt erlangten Daten. Auch insoweit ist es gerade das Ziel des DA, mehr Konkurrenz und Innovationen zu fördern.

2.4.8 Nutzungsverbot, Zwangsmittel und Lücken in der Infrastruktur (Art. 4 Abs. 11 DA)

Ein Nutzer darf keine Zwangsmittel einsetzen oder Lücken in der zum Schutz der Daten bestehenden technischen Infrastruktur eines Dateninhabers ausnutzen, um Zugang zu Daten zu erlangen. Dies gilt auch dann, wenn ein Dateninhaber den Datenzugang zu Unrecht verweigert. Vielmehr muss der Nutzer in diesem Fall den Weg über die gerichtliche Durchsetzung oder die Rechtsbehelfe des Art. 4 Abs. 9DA (Herbeiführung

der Entscheidung durch die zuständige Aufsichtsbehörde oder Einschaltung der Streitbeilegungsstelle) gehen.

Bei einer Aufhebung oder Änderung der technischen Schutzmaßnahmen durch einen Nutzer stehen dem Dateninhaber (oder ggf. dem personenverschiedenen Inhaber eines betroffenen Geschäftsgeheimnisses) die Ansprüche aus Art. 11 Abs. 2 DA zu, insbesondere auf Entschädigung, Löschung der Daten und ggf. Vernichtung rechtsverletzender Produkte.

2.4.9 Rechtsgrundlage bei personenbezogenen Daten (Art. 4 Abs. 12 DA)

Die Datenbereitstellungspflicht nach dem DA gilt sowohl für nicht-personenbezogene als auch für personenbezogene Daten. In Bezug auf personenbezogene Daten sind jedoch auch die Vorgaben der DSGVO zu beachten. Denn bei personenbezogenen Produkt- oder verbundenen Dienstdaten gelten DA und DSGVO nebeneinander, wobei im Fall von Widersprüchen die Vorgaben der DSGVO zum Schutz personenbezogener Daten Vorrang haben (siehe Abschnitt 1.4.1).

Nach der DSGVO ist eine Verarbeitung (u. a. die Offenlegung, Übermittlung oder Erhebung) personenbezogener Daten durch andere als die betroffene Person (d. h. die Person, auf die sich die jeweiligen Daten beziehen) grundsätzlich nur dann erlaubt, wenn hierfür eine einschlägige Rechtsgrundlage (bspw. eine Einwilligung der betroffenen Person) besteht. Im Zusammenhang mit der Bereitstellung personenbezogener Produkt- oder verbundenen Dienstdaten nach dem DA ist dies immer nur dann unproblematisch, wenn der Nutzer, dem die Daten bereitgestellt werden, auch die (einzige) betroffene Person ist, auf die sich die Daten beziehen. Denn der Nutzer benötigt in diesem Fall keine Rechtsgrundlage für den Erhalt der ihn selbst betreffenden Daten; der Dateninhaber benötigt zwar eine datenschutzrechtliche Rechtsgrundlage für die Übermittlung / Offenlegung, jedoch ist diese ohne Weiteres gegeben, da das Datenzugangsverlangen des Nutzers (d. h. der betroffenen Person) gleichsam eine (jedenfalls konkludente) Einwilligung darstellt.

Anders ist dies in Fällen, in denen ein Nutzer von einem Dateninhaber die Bereitstellung personenbezogener Produkt- oder verbundener Dienstdaten verlangt, die sich (auch) auf andere Personen beziehen als den Nutzer selbst, d. h. in allen Fällen, in denen der »Nutzer« i.S.d. DA nicht die »betroffene Person« i.S.d. DSGVO ist. Für diese Fälle stellt Art. 4 Abs. 12 DA noch einmal ausdrücklich klar, dass der Dateninhaber personenbezogene Daten, die bei der Nutzung eines vernetzten Produktes oder verbundenen Dienstes generiert werden, dem Nutzer nur dann bereitstellen darf, wenn es für die Verarbeitung eine gültige datenschutzrechtliche Rechtsgrundlage gibt. In welchem Maß den Dateninhaber dabei eine Prüfpflicht trifft, ist bislang offen. Ratsam ist für Dateninhaber jedenfalls, sich die datenschutzrechtliche Zulässigkeit der Bereitstellung personenbezogener Daten eines Dritten zumindest vom Nutzer bestätigen zu lassen.

Eine (informierte und freiwillige) Einwilligung der betroffenen Person(en) stellt in jedem Fall eine gültige Rechtsgrundlage für die von dieser Einwilligung umfassten Verarbeitungsvorgänge dar. Fehlt es an einer solchen Einwilligung, hängt es von den

konkreten Umständen und der Art der personenbezogenen Daten ab, ob bzw. welche sonstige Rechtsgrundlage in Betracht kommt:

- Für die Verarbeitung besonderer Kategorien personenbezogener Daten (bspw. Gesundheitsdaten) bedarf es einer Rechtsgrundlage nach Art. 9 DSGVO;
- die Verarbeitung sonstiger personenbezogener Daten kann ggf. auf eine der Rechtsgrundlagen aus Art. 6 DSGVO gestützt werden (bspw. ein überwiegendes berechtigtes Interesse);
- bei einem Zugriff auf Daten aus einem (Telekommunikations-) Endgerät sind die Voraussetzungen des § 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) zu beachten.

Fehlt es an einer Rechtsgrundlage für die Bereitstellung der personenbezogenen Daten, müssen bzw. dürfen diese auch nach dem DA nicht bereitgestellt werden. Ggf. besteht jedoch die Möglichkeit, die Produkt- bzw. verbundenen Dienstdaten um die personenbezogenen Daten zu bereinigen, für deren Bereitstellung es keine Rechtsgrundlage gibt, sodass nur die übrigen Daten bereitgestellt werden. Eine andere Möglichkeit bietet ggf. eine Anonymisierung der personenbezogenen Daten durch Entfernung der Personenbezüge, wodurch diese Daten nicht mehr den Regelungen der DSGVO unterfallen. Solche Anonymisierungsmaßnahmen führen laut den DA-FAQs der EU-KOM (Nr. 13) auch nicht dazu, dass die dadurch generierten (anonymisierten) Daten als abgeleitete Informationen (siehe Abschnitt 2.1.2 für Produktdaten) gelten, die nicht mehr dem Anwendungsbereich der Datenbereitstellungspflicht unterfallen.

Aufgrund der zahlreichen rechtlichen Herausforderungen, die sich in Bezug auf personenbezogene Daten im Spannungsfeld von DA und DSGVO ergeben, sollte bei diesbezüglichen Beurteilungen und Entscheidungen in der unternehmerischen Praxis stets der Datenschutzbeauftragte des betreffenden Unternehmens eingebunden werden.

2.4.10 Erfordernis eines Vertrags mit dem Nutzer (Art. 4 Abs. 13 DA)

Ein Dateninhaber darf ohne Weiteres verfügbare Daten (siehe Abschnitte 2.1 und 2.4.1), bei denen es sich um nicht-personenbezogene Daten handelt, nur auf der Grundlage eines Vertrags mit dem Nutzer nutzen. Insoweit werden nicht-personenbezogene Daten unter dem DA sogar stärker geschützt als personenbezogene Daten, da Letztere ggf. auch ohne eine Einwilligung bzw. ohne eine Vereinbarung mit der betroffenen Person genutzt werden dürfen (etwa aufgrund eines überwiegenden berechtigten Interesses).

Ein solcher Datennutzungsvertrag unterliegt jedoch keinem Kopplungsverbot. D.h., dass ein (potenzieller) Dateninhaber bspw. den Verkauf oder die Nutzung eines vernetzten Produkts bzw. die Erbringung eines verbundenen Dienstes davon abhängig machen kann, dass der Nutzer einem solchen Nutzungsvertrag zustimmt und der Gegenseite damit ein Datennutzungsrecht einräumt, auch wenn die so vereinbarte Nutzung über das hinausgeht, was bspw. für die Erbringung eines verbundenen Dienstes erforderlich wäre (dies jedenfalls insoweit als nicht die Grenze zur Missbräuchlichkeit überschritten wird).

Fehlt es hingegen an einem solchen Vertrag, dürfen die ohne Weiteres verfügbaren (nicht-personenbezogenen) Daten durch den Dateninhaber nicht genutzt werden. Bei wechselnden Nutzern muss daher (bspw. über separate Nutzeraccounts) sichergestellt werden, dass mit jedem neuen Nutzer – nachweisbar – ein solcher Datennutzungsvertrag geschlossen wird.

Auch wenn ein entsprechender Datennutzungsvertrag besteht, existieren bestimmte gesetzliche Verwendungsverbote für die ohne Weiteres verfügbaren (nicht-personenbezogenen) Daten: Ebenso wie es dem Nutzer verboten ist, die erhaltenen Daten zu nutzen, um Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Produktherstellers oder Dateninhabers zu erlangen (siehe Abschnitt 2.4.7), ist es umgekehrt auch dem Dateninhabern durch den DA verboten, solche Daten zu verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers zu erlangen. Darüber hinaus ist es dem Dateninhaber verboten, solche Daten auf eine (andere) Art zu verwenden, die die gewerbliche Position des Nutzers auf den Märkten, auf denen dieser tätig ist, untergraben könnte.

2.4.11 Verbot der Bereitstellung von Daten an Dritte (Art. 4 Abs. 14 DA)

Während es einem Nutzer grundsätzlich freisteht, die nicht-personenbezogenen Daten aus seinen Produkten an Dritte weiterzugeben, dürfen Dateninhaber solche Daten nur zum Zwecke der Erfüllung ihres Vertrags mit dem Nutzer an Dritte weitergeben. Laut den DA FAQs der EU-KOM (Nr. 29) ist hierbei auf den Datennutzungsvertrag nach Art. 4 Abs. 13 DA (siehe Abschnitt 2.4.10) abzustellen. Dies bedeutet, dass ein Dateninhaber nicht-personenbezogene Produktdaten nur insoweit an Dritte weitergeben darf, wie er dies mit dem Nutzer im Rahmen des Datennutzungsvertrags vereinbart hat. Demgegenüber wäre eine nicht mit dem Nutzer vertraglich vereinbarte Weitergabe von Produktdaten an Dritte, egal zu welchen (kommerziellen oder nichtkommerziellen) Zwecken, unrechtmäßig. Abhängig von ihrer konkreten Vereinbarung mit dem Nutzer, müssen Dateninhaber Dritte ggf. auch vertraglich verpflichten, die von ihnen erhaltenen Daten nicht erneut weiterzugeben.

2.5 Datenteilungspflicht mit Dritten (Art. 5 DA)

Dr. Daniel Meßmer, Partner, SKW Schwarz Rechtsanwälte Steuerberater Partnerschaft mbB

EG 30, 33, 34, 57 DA

2.5.1 Anwendungsbereich (Art. 5 Abs. 1 DA)

Art. 5 DA regelt die gesetzliche Pflicht des Dateninhabers, ohne Weiteres verfügbare Daten[155] und zugehörige Metadaten[156] auf Verlangen des Nutzers einem von diesem benannten Datenempfänger[157] bereitzustellen.

Die Vorschrift ergänzt Art. 4 DA (siehe Abschnitt 2.4). Während Art. 4 DA die Datenbereitstellung unmittelbar an den Nutzer selbst betrifft, betrifft Art. 5 DA Fälle, in denen der Nutzer die Daten nicht für sich selbst, sondern für einen von ihm benannten Dritten anfordert.

Anders als das Recht des Nutzers auf (eigenen) Datenzugang nach Art. 4 DA wird die Pflicht des Dateninhabers zur Bereitstellung der Daten an einen Datenempfänger nach Art. 5 DA nicht dadurch ausgeschlossen, dass der Nutzer nach Maßgabe von Art. 3 DA (»Access by Design«) direkt am vernetzten Produkt oder verbundenen Dienst auf die Daten zugreifen kann.

2.5.2 Bereitstellung auf Anforderung des Nutzers, Auswahl des Datenempfängers (Art. 5 Abs. 1 DA)

Die Bereitstellung an einen Datenempfänger erfolgt gemäß Art. 5 Abs. 1 DA auf Verlangen des Nutzers oder einer im Namen des Nutzers handelnden Person. Für die Identifizierung des Nutzers gelten dabei grundsätzlich dieselben Maßgaben, die auch für einen Datenzugang nach Art. 4 DA (vgl. Abschnitt 2.4.4) Anwendung finden[158].

Der Nutzer kann im Rahmen von Art. 5 DA exklusiv über die Bereitstellung der Daten an einen Datenempfänger disponieren. Insbesondere darf der Dateninhaber die Daten nicht ohne ein Verlangen des Nutzers eigenmächtig an Dritte weitergeben[159].

Die Auswahl des Datenempfängers liegt dabei ebenfalls allein beim Nutzer. Der Dateninhaber darf die Bereitstellung an den vom Nutzer benannten Datenempfänger nicht aufgrund der Person des Datenempfängers ablehnen (Ausnahme: Torwächter gemäß DMA, siehe Abschnitt 2.5.4). Insbesondere ist der Dateninhaber auf eine entsprechende Anforderung des Nutzers, gerade auch zur Datenbereitstellung an einen Wettbewerber des Dateninhabers, verpflichtet.

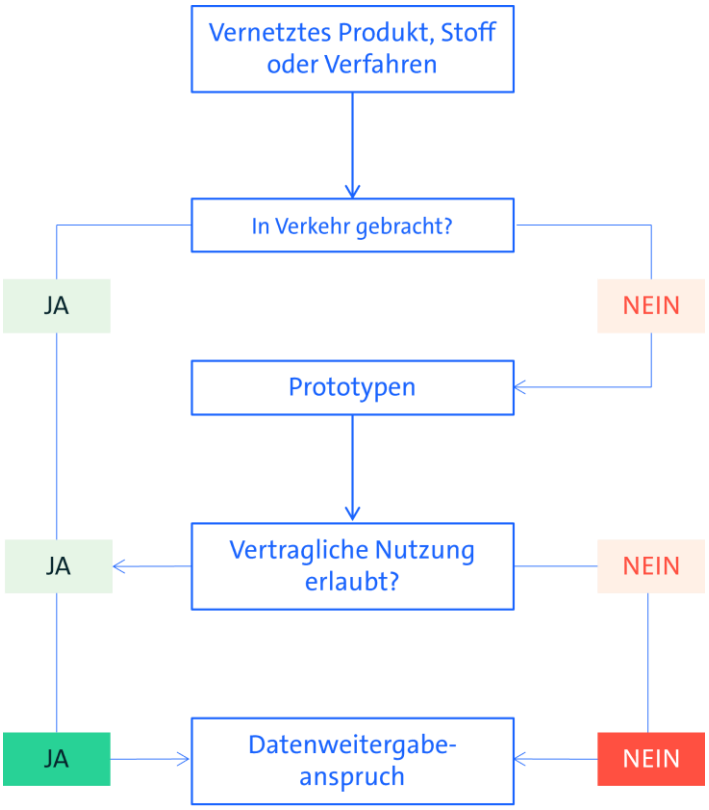
2.5.3 Prototypenregelung (Art. 5 Abs. 2 DA)

Swen Hildebrandt, Konzern Sicherheit & Resilienz, Volkswagen AG

Das Recht aus Art. 5 Abs. 1 DA wird durch Art. 5 Abs. 2 DA in einer sachbezogenen Ausnahme eingeschränkt: Prototypen nach dem EG 14 S. 1 DA[160]. Wörtlich heißt es dazu in Art. 5 Abs. 2 DA, der Datenweitergabeanspruch gilt »nicht für ohne Weiteres verfügbare Daten im Zusammenhang mit der Prüfung neuer vernetzter Produkte,

[155] Art. 2 Nr. 17 DA.
[156] Art. 2 Nr. 2 DA.
[157] Art. 2 Nr. 14 DA.
[158] Art. 5 Abs. 4 DA.
[159] Art. 8 Abs. 4 DA.
[160] Vgl. EG 14 DA.

Stoffe oder Verfahren, die noch nicht in Verkehr gebracht werden, es sei denn, ihre Verwendung durch Dritte ist vertraglich genehmigt.«[161] Solche Prototypen fallen ausdrücklich nicht in den Anwendungsbereich der Datenteilungspflichten vom DA. Der Gesetzgeber betrachtet diese Vorab-Versionen eines Produkts als besonders schutzwürdig, da ihr Herstellungsstadium noch nicht abgeschlossen ist. Diese Regelung stellt sicher, dass Daten aus der Prototypenentwicklung bis zur Markteinführung vertraulich bleiben. Mit anderen Worten: Solange sich ein vernetztes Produkt in der Entwicklungs- und Testphase befindet und noch nicht auf dem Markt angeboten wird, besteht kein Anspruch des Nutzers, diese Daten an Dritte weiterleiten zu lassen – außer der Hersteller hat eine solche Nutzung durch Dritte vertraglich erlaubt. Die Zielsetzung dieser Ausnahme ist klar: Schutz von Geschäftsgeheimnissen und Know-how in der sensiblen Entwicklungsphase.[162] Folgende Abbildung visualisiert die Prototypenregelung nach Art. 5 Abs. 2 DA.



Hildebrandt, 2025.

2.5.4 DMA-Klausel (Art. 5 Abs. 3 DA)

Als Datenempfänger ausdrücklich ausgeschlossen sind durch Art. 5 Abs. 3 DA allerdings Gatekeeper (Torwächter) im Sinne von Art. 3 DMA. Gatekeeper können vom Nutzer also nicht als Datenempfänger benannt werden (vgl. Abschnitt 2.2.3.3). Art. 5 Abs. 3 DA adressiert Gatekeeper unmittelbar und untersagt diesen etwa, Nutzer dafür zu

[161] Art. 5 DA.
[162] Vbw (Vereinigung der Bayerischen Wirtschaft), »Data Act Leitfaden«, Stand 09/2024, S. 32, https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2024/Downloads/vbw-Leitfaden-Data-Act-September-2024.pdf.

gewinnen, sie als Datenempfänger zu benennen. Gatekeeper müssen die Bereitstellung der Daten damit wohl aktiv ablehnen, wenn sie vom Nutzer als Datenempfänger gegenüber dem Dateninhaber benannt werden.

Dem Dateninhaber selbst obliegt es hingegen wohl nicht, jeden benannten Datenempfänger auf eine Qualifizierung als Gatekeeper im Sinne von Art. 3 DMA zu überprüfen. Man könnte Art. 5 Abs. 4 (»Überprüfung, ob eine ...Person...als Dritter einzustufen ist«) i.V.m. Abs. 3 DA (»Torwächter ...gilt nicht als ...zugelassener Dritter«) aber auch dahingehend verstehen, dass der Dateninhaber diese Prüfung durchführen muss.

2.5.5 Umfang der Datenbereitstellung gegenüber dem Datenempfänger

Der Dateninhaber muss dem vom Nutzer ausgewählten Datenempfänger im Rahmen von Art. 5 DA grundsätzlich in demselben Umfang Daten bereitstellen, den Art. 4 DA auch für die Bereitstellung der Daten an den Nutzer selbst vorsieht (siehe Abschnitt 2.4.1). Konkret bezieht sich Art. 5 DA damit ebenfalls auf die »ohne Weiteres verfügbaren Daten« sowie die zu deren Auslegung und Nutzung erforderliche »Metadaten«.

Diese Daten müssen vom Dateninhaber dabei unverzüglich, für den Nutzer unentgeltlich, in derselben Qualität, einfach, sicher und in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden. Soweit relevant und technisch durchführbar, muss die Bereitstellung kontinuierlich und in Echtzeit erfolgen. Insoweit kann auf die Erläuterungen zu Art. 4 DA verwiesen werden, siehe Abschnitt 2.4.

2.5.5.1 Durchführung der Datenbereitstellung

Für die Umsetzung der Datenbereitstellung gegenüber dem Datenempfänger verweist Art. 5 Abs. 1 DA auf Art. 8 und 9 DA: Art. 8 DA enthält Vorgaben an die vertraglichen Bedingungen zwischen Dateninhaber und Datenempfänger (siehe Abschnitt 2.6). Daran anknüpfend regelt Art. 9 DA, ob und inwieweit der Dateninhaber vom Datenempfänger eine Gegenleistung für die Durchführung der Datenbereitstellung verlangen kann.

Der Einsatz von Zwangsmittel oder das Ausnutzen etwaiger Sicherheitslücken in der vom Dateninhaber zur Verwaltung der Daten eingesetzten Infrastruktur ist dem Dritten durch Art. 5 Abs. 5 DA ausdrücklich untersagt. So soll die Einhaltung des vom DA für die Datenbereitstellung vorgesehenen Verfahrens und der vorherige Abschluss eines den Anforderungen der Art. 8 und 9 DA entsprechenden Vereinbarung zwischen Dateninhaber und Datenempfänger sichergestellt werden.

Umgekehrt darf der Dateninhaber ohne Weiteres verfügbare Daten gemäß Art. 5 Abs. 6 DA ohne Genehmigung des und »die technische Möglichkeit, diese Genehmigung jederzeit einfach zu widerrufen«[163] für den Dritten nicht dazu verwenden, um Einblicke

[163] Art. 5 Abs. 6 DA.

in die wirtschaftliche Lage, Vermögensverhältnisse oder Produktionsmethoden des Dritten zu erlangen.

2.5.6 Personenbezogene Daten und Geschäftsgeheimnisse

Einschränkungen der Pflicht des Dateninhabers zur Datenbereitstellung an einen Datenempfänger können bestehen, wenn die ohne Weiteres verfügbaren Daten ganz oder teilweise personenbezogen sind oder es sich dabei um Geschäftsgeheimnisse handelt.

Enthalten die ohne Weiteres verfügbaren Daten, deren Bereitstellung der Nutzer vom Dateninhaber anfordert personenbezogene Daten eines Dritten, darf eine Bereitstellung dieser personenbezogenen Daten gemäß Art. 5 Abs. 7 DA nur erfolgen, wenn für die in der Bereitstellung liegenden Datenverarbeitung eine Rechtsgrundlage vorliegt. Der DA stellt in EG 7 ausdrücklich klar, dass der DA selbst keine datenschutzrechtliche Rechtsgrundlage darstellt. Gemäß Art. 1 Abs. 5 DA gehen die Vorschriften zum Schutz von personenbezogenen Daten dem DA vor. Art. 5 Abs. 13 DA stellt zudem klar, dass die Rechte betroffener Personen zum Schutz personenbezogener Daten durch eine Anforderung gemäß Art. 5 Abs. 1 DA nicht beeinträchtigt werden dürfen.

Falls eine entsprechende Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten nicht vorliegt, ist der Dateninhaber zur Bereitstellung der Daten gegenüber dem Datenempfänger nicht verpflichtet. Vielmehr ist ihm eine Weitergabe in diesem Fall gesetzlich untersagt.

Der Dateninhaber ist nach dem DA allerdings wohl auch nicht dazu verpflichtet, selbst für eine solche Rechtsgrundlage zu sorgen, um Art. 5 Abs. 1 DA nachkommen zu können. Bei Ausübung der Rechte von Art. 5 Abs. 1 DA wird er regelmäßig nicht als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO anzusehen sein. Denn jedenfalls legt er die Zwecke der Datenbereitstellung nicht fest, sondern führt vielmehr lediglich die ihm gesetzlich auferlegte Pflicht aus. In welchem Maß dem Dateninhaber dennoch Prüf- oder Sorgfaltspflichten obliegen, ist bislang offen. Ratsam ist für Dateninhaber jedenfalls, sich die datenschutzrechtliche Zulässigkeit der Bereitstellung personenbezogener Daten eines Dritten an den Datenempfänger vom Nutzer bestätigen zu lassen.

Weitere Einschränkungen der Datenbereitstellung können sich ergeben, soweit es sich bei den ohne Weiteres verfügbaren Daten um Geschäftsgeheimnisse (siehe Abschnitt 1.4.2) des Dateninhabers oder eines Dritten handelt (vgl. hierzu entsprechend auch die Ausführungen unter Abschnitt 2.4.5). Art. 5 Abs. 9 DA sieht für diesen Fall vor, dass der Inhaber des Geschäftsgeheimnisses sich mit dem Datenempfänger auf angemessene technische und organisatorische Maßnahmen zum Schutz des Geschäftsgeheimnisses verständigt. Gelingt dies nicht oder werden diese Maßnahmen vom Datenempfänger nicht umgesetzt oder verletzt, kann der Dateninhaber gemäß Art. 5 Abs. 10 DA die Bereitstellung verweigern oder – im Fall einer bereits begonnenen Bereitstellung – aussetzen. Dies muss der zuständigen Behörde durch den Dateninhaber mitgeteilt werden.

Nur unter außergewöhnlichen Umständen, in denen ein Geschäftsgeheimnis eines Datenempfängers durch angemessene Maßnahmen nicht ohne eine verbleibende hohe Wahrscheinlichkeit schwerwiegender wirtschaftlicher Schäden ausgeräumt werden könnte, kann der Dateninhaber die Bereitstellung für den Einzelfall ablehnen. Das stellt eine enge Ausnahmeregelung dar. Tritt dieser Fall ein, muss dies gegenüber der zuständigen Behörde mitgeteilt und begründet werden.

In beiden der vorgenannten Fälle hat der Nutzer gemäß Art. 5 Abs. 12 DA die Möglichkeit, die Entscheidung des Dateninhabers anzufechten, indem er Beschwerde bei der zuständigen Behörde einreicht oder im Einvernehmen mit dem Dateninhaber eine Streitbeilegungsstelle anruft.

2.6 Bedingungen, unter denen Dateninhaber Datenempfängern Daten bereitstellen (Art. 8 DA)

Jan-Dierk Schaal, Rechtsanwalt, Equity Partner, SKW Schwarz Rechtsanwälte Steuerberater Partnerschaft mbB |
Franziska Wulf, Wissenschaftliche Mitarbeiterin, SKW Schwarz Rechtsanwälte Steuerberater Partnerschaft mbB

EG 42, 43, 44, 45 DA

2.6.1 FRAND-Maßstab

Wesentlicher Bestandteil des DA ist die vertragliche Regelung der Datenzugangsansprüche. Insoweit regelt Art. 5 DA, dass der Nutzer verlangen kann, dass der Dateninhaber die Daten des vernetzten Produkts oder verbundenen Dienstes Dritten bereitstellt. Diese Bereitstellung muss für den Nutzer unentgeltlich erfolgen. Dies bedeutet jedoch nicht, dass der Dateninhaber mit dem Datenempfänger keine Konditionen für die Weitergabe vereinbaren könnte. Dies jedenfalls, soweit der Datenempfänger ein Unternehmen ist, mithin die Datenweitergabe »im Rahmen von Geschäftsbeziehungen zwischen Unternehmen« erfolgt, also B2B.

Die Bedingungen und Konditionen dieses Datenzugangsanspruchs werden in Art. 8 DA konkretisiert. Die Weitergabe hat insoweit unter Anwendung des FRAND-Maßstabes zu erfolgen. Der FRAND-Maßstab wird auch in anderen Rechtsbereichen als wesentliches Element einer wettbewerbsfördernden Gestaltung der Zugangsrechte angesehen. Rechnung wird dabei dem Umstand getragen, dass der Dateninhaber aufgrund seines direkten Datenzugriffs eine Vormachtstellung innehat, was die dritte Partei besonders schutzbedürftig macht. Die FRAND-Bedingungen sind im Einzelnen fair, reasonable and non-discriminatory. Der Dateninhaber muss die Daten also zu fairen, angemessenen und nichtdiskriminierenden Bedingungen zur Verfügung stellen. Zudem hat er dies laut Art. 8 DA in transparenter Weise zu machen. Während Art. 4 DA die technische Ausgestaltung des Datenzugangs konkretisiert, bezieht sich Art. 8 DA

mithin auf die vertragliche Ausgestaltung. Laut Art. 41 DA ist die EU-KOM verpflichtet, bis Mitte September 2025 unverbindliche Mustervertragsklauseln zu erstellen, um so die Handhabung in der Praxis zu erleichtern. Ein Entwurf wurde durch die entsprechende Expertengruppe im April 2025 vorgelegt.[164]

2.6.1.1 Faire Bedingungen

Eine faire Datenbereitstellung zeichnet sich dadurch aus, dass die Bedingungen für den Datenzugang ausgewogen und gerecht sind. Dies wird durch EG 5 DA unterstrichen, der den Sinn der Regelung darin sieht, die Ausnutzung vertraglicher Ungleichgewichte zu verhindern, was einen fairen Datenzugang erschweren würde.

2.6.1.2 Angemessene Bedingungen

Die Angemessenheit soll sich auf eine entsprechende Vergütung für das Teilen der Daten beziehen. Näher konkretisiert wird diese Anforderung in Art. 9 DA, der regelt, welche Kostenpositionen bei der Berechnung der Gegenleistung vom Dateninhaber berücksichtigt werden dürfen. EG 46 DA geht davon aus, dass zur Angemessenheit der Vergütung Leitlinien seitens der EU-KOM erlassen werden. Zu berücksichtigen ist bei der Ermittlung der Angemessenheit der Vergütung, dass diese sich nicht nach dem Wert der Daten bestimmen kann, da diese Gegenleistung keine Bezahlung für die Daten selbst darstellt, sondern den Aufwand des Dateninhabers bei der Datengenerierung und durch die Datenweitergabe und die damit verbundenen Kosten kompensieren soll[165].

2.6.1.3 Nichtdiskriminierende Bedingungen

Hinsichtlich des Nichtdiskriminierungsgrundsatzes betont EG 45 DA explizit, dass die Frage der Weitergabe von Daten und deren Konditionen nicht von der Größe des Datenempfängers abhängig gemacht werden soll. Zudem formuliert EG 45 DA eine Beweislastumkehr. Hiernach soll keine rechtswidrige Diskriminierung vorliegen, wenn der Dateninhaber für die Bereitstellung von Daten unterschiedliche Vertragsklauseln vorsieht, sofern er nachweisen kann, dass diese Unterschiede aus objektiven Gründen gerechtfertigt sind. Um dieser Pflicht nachkommen zu können, ist Dateninhabern zu raten, regelmäßig relevante Informationen zu sammeln, um sie im Falle eines Ersuchens bereitstellen zu können.

2.6.2 Inhaltskontrolle

Art. 8 DA stellt einen Bezug auf Kapitel IV DA her, wo in Art. 13 DA eine Liste von Arten missbräuchlicher Vertragsklauseln zu finden sind. Insoweit regelt Art. 13 DA die Inhaltskontrolle für alle Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen. Art. 8 Abs. 2 DA stellt ebenfalls klar, dass Vertragsklauseln, die der Inhaltskontrolle des Art. 13 DA nicht standhalten, für die

[164] Expert Group on B2B data sharing and cloud computing contracts, «Final Report of the Expert Group on B2B data sharing and cloud computing contracts", 02.04.2025, zuletzt abgerufen am 27.08.2025, https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/116180/download.
[165] Vgl. EG 47 DA.

jeweils andere Partei nicht bindend sind. Im Hinblick darauf, dass beide Regelungen vorsehen, dass die Parteien durch nach Art. 13 DA unzulässige Klauseln nicht gebunden werden, kann die Regelung in Art. 8 DA lediglich ein Verweis auf die detailliertere Regelung des Art. 13 DA sein. Hinsichtlich der Rechtsfolge sind sowohl Art. 8 DA als auch Art. 13 DA eindeutig: Ein Verstoß führt lediglich dazu, dass der Dateninhaber als Klauselsteller die entsprechende Verpflichtung nicht durchsetzen kann; sie führt jedoch nicht zur Unwirksamkeit oder gar Nichtigkeit der Vereinbarung.

2.6.3 Nutzerzentrierung

Art. 8 Abs. 4 DA regelt explizit, dass Daten vom Dateninhaber nur dann bereitgestellt werden dürfen, wenn der Nutzer dies verlangt hat. Dabei verweist die Vorschrift auf Kapitel II DA. Dort regelt bereits Art. 5 Abs. 1 DA die Anspruchsgrundlage, nach welcher der Nutzer die Datenweitergabe an einen Dritten vom Dateninhaber verlangen kann. In beiden Vorschriften wird die wesentliche Rolle des Verlangens des Nutzers für die Herausgabe der Daten deutlich. Daher dürfen Daten nur auf ausdrückliches Verlangen des Nutzers weitergegeben werden bzw. soweit dies im Datennutzungsvertrag festgelegt ist (vgl. Abschnitte 2.4.10 und 2.4.11). f

2.6.4 Sensible Informationen und Geschäftsgeheimnisse

Der DA verdeutlicht in Art. 8 den Grundsatz, dass keine weitgehenden Informationspflichten zwischen den Vertragsparteien bestehen und Geschäftsgeheimnisse grundsätzlich nicht offenzulegen sind.

Art. 8 Abs. 5 DA legt fest, dass lediglich Informationen, die erforderlich sind, um die Einhaltung der Pflichten des DA oder sonstigem Unionsrecht und der vereinbarten Vertragsklauseln zu gewährleisten, herauszugeben sind. Dies soll verdeutlichen, dass insbesondere keine Auskunft über etwaige Geschäftsideen oder den angestrebten Nutzungszweck gegeben werden muss.

Art. 8 Abs. 6 DA sieht vor, dass mit der Datenbereitstellungspflicht nicht auch die Pflicht zur Offenlegung von Geschäftsgeheimnissen einhergeht. Die Gesetzesformulierung »es sei denn, im Unionsrecht, einschließlich des Artikels 4 Absatz 6 und des Artikels 5 Absatz 9 der vorliegenden Verordnung, oder in im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften ist etwas anderes vorgesehen« mag zu dem Verständnis führen, diese dort genannten Regelungen würden eine Pflicht zur Offenlegung von Geschäftsgeheimnissen beinhalten. Vertreter dieses Verständnisses kritisieren einen vorrangigen Geschäftsgeheimnisschutz mit der Begründung einer daraus resultierenden unangemessenen Privilegierung des Datenhalters: daher wird sich dafür ausgesprochen, diesen Absatz zu streichen, wodurch es Aufgabe des nationalen Gesetzgebers werden würde, den Geschäftsgeheimnisschutz zu koordinieren.[166]

[166] Drexl, «Position Statement of the Max Planck Institute on the Proposal for a Data Act" Rn. 283f., zuletzt abgerufen am 09.07.2025, https://www.ip.mpg.de/en/research/research-news/position-statement-on-the-eu-data-act.html.

Einem anderen Verständnis nach regeln die dort genannten Vorschriften vielmehr erweiterte Pflichten zur Ergreifung und Vereinbarung technischer und organisatorischer Maßnahmen zum Schutz der in den Daten verkörperten Geheimnisse, wenn diese weitergegeben werden. Demnach wird vertreten, dass diese Regelung mithin keinen Ausnahmetatbestand zum grundsätzlichen Geschäftsgeheimnisschutz darstellt, sondern diesen nochmals absichert.

2.6.5 Verhältnis zu anderen Vorschriften

Teilweise erscheint die Regelung des Art. 8 DA als Wiederholung oder Doppelung bereits an anderer Stelle im DA vorhandener Regelungen, was verständlicherweise zu der Frage führt, ob der Gesetzgeber hiermit in Art. 8 DA eine über die anderen Regelungen hinausgehenden oder überschießenden Regelungsinhalt schaffen wollte. Eine ausdrückliche Vorrangregelung enthält der DA diesbezüglich jedoch nicht, was sicherlich noch zu Kontroversen hinsichtlich der Auslegungen der jeweiligen Vorschriften führen wird. In der Literatur gibt es bereits vereinzelte Lösungsversuche. Stellenweise wird die Systematik so erklärt, dass Kapitel II DA die wesentlichen Voraussetzungen des Datenzugangs und der Nutzung regelt, während Kapitel III und IV DA an ein schon bestehendes Datenzugangsrecht anknüpfen und die Modalitäten im Einzelnen festlegen.[167] Somit scheint Art. 8 DA, dessen Überschrift »Bedingungen, unter denen Dateninhaber Datenempfängern Daten bereitstellen« lautet, die allgemein geltenden Vorschriften der anderen Artikel des DA zusammenzufassen und explizit zu unterstreichen, dass diese auch und erst recht im vertraglichen Verhältnis zwischen Dateninhaber und Datenempfänger gelten.

[167] Pauly/Wichert/Baumann, MMR 2024, 211 (211); Schmidt-Kessel, MMR 2024, 75 (80).

3 Cloud Switching (Kapitel VI, VIII DA)

3.1 Sachlicher Anwendungsbereich (Art. 2 Abs. 8 DA)

Dr. Viola Bensinger (Anwältin), Greenberg Traurig Germany, LLP | Jana Rudt (Anwältin), Greenberg Traurig Germany, LLP | Dr. Jannis Dietrich-Webb (Anwalt), Greenberg Traurig Germany, LLP

EG 80, 81 DA

Kapitel VI DA adressiert ausschließlich sogenannte »Datenverarbeitungsdienste« (»**DVD**«).[168] Nur Angebote, die als DVD zu qualifizieren sind, unterfallen den ausgedehnten Pflichten zum sog. »Cloud Switching«, die in diesem Teil der Verordnung geregelt sind. Bedauerlicherweise schafft die von der EU-KOM bereitgestellte Definition eines Datenverarbeitungsdienstes den Anbietern digitaler Dienste keine Klarheit darüber, welche Angebote möglicherweise als DVD einzuordnen wären.

Gemäß Art. 2 Nr. 8 DA ist ein DVD »eine digitale Dienstleistung, die einem Kunden bereitgestellt wird und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen zentralisierter, verteilter oder hochgradig verteilter Art ermöglicht, die mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können«.

Wie die EU-KOM selbst feststellt, fällt hierunter eine »beträchtliche Zahl von Diensten mit einer sehr großen Bandbreite an unterschiedlichen Anwendungszwecken, Funktionen und technischen Strukturen«[169]. Außerdem werden laut EU-KOM DVD typischerweise entweder als Infrastructure-as-a-Service (»**IaaS**«), als Platform-as-a-Service (»**PaaS**«) oder Software-as-a-Service (»**SaaS**«) Dienste bereitgestellt.[170] Relativierend wird angemerkt, dass dieser Katalog nicht abschließend sei,[171] sodass der verwendeten Formulierung folgend, nicht jeder IaaS, PaaS oder SaaS-Dienst auch einen DVD darstellen muss,[172] und somit der Hinweis nahezu ins Leere läuft.

[168] Vgl. bereits die offizielle Kapitelüberschrift ("Wechsel zwischen Datenverarbeitungsdiensten").
[169] EG 81 S. 1 DA.
[170] EG 81 S. 2 DA.
[171] EG 81 S. 3f. DA.
[172] Umkehrschluss daraus, dass es sich hierbei nur um "Modelle" zur Bereitstellung von DVD handeln soll (EG 81 S. 3f. DA).

Angesichts dieses breiten Feldes möglicher DVD ist also vor allem die Bedeutung der einzelnen o.g. Definitionsbestandteile für die Bestimmung darüber entscheidend, welche Angebote als DVD einzuordnen sind. Nachfolgend werden die Definitionsbestandteile im Detail dargestellt, was den Anwendungsbereich des DA wiederum überraschend stark einschränkt.

Zusammengefasst kann anhand der Definitionsmerkmale festgehalten werden, dass Datenverarbeitungsdienste zunächst alle gemeinsam haben, dass sie nicht-physische Angebote darstellen, die über das Internet (oder vergleichbare Netze) bereitgestellt werden. Die Dienste müssen dazu so bereitgestellt werden, dass Kunden mindestens im Ansatz eine Konfigurationsmöglichkeit haben, gleichzeitig darf aber keine aufwändige Ersteinrichtung, Konfiguration oder Absprache mit dem Anbieter erforderlich sein. Schließlich dürfen die Dienste nicht auf »fester« Hardware angeboten werden, sondern diese muss bedarfsgesteuert angepasst werden können (Cloud-Prinzip). Im Detail:

3.1.1 Digitale Dienstleistung, die einem Kunden bereitgestellt wird

Das erste Definitionsmerkmal eines DVD ist vergleichsweise inhaltsleer: Im gesamten DA bleibt offen, was eine »digitale Dienstleistung« konkret sein soll. Ein solches weites Verständnis der digitalen Dienstleistung kann im Zweifelsfall (auch) auf die bloße elektronische Bereitstellung heruntergebrochen werden.[173] »Kunde« eines solchen Dienstes kann wiederum jede natürliche oder juristische Person sein, solange ein Nutzungsvertrag über den DVD besteht.[174] Vorbehaltlich gerichtlicher Klarstellung dürfte auch das tendenziell weit zu verstehen sein und neben »echten« Verträgen auch reine »EULA-Modelle« (bei denen lediglich den Lizenzbestimmungen zugestimmt werden muss) einschließen. Die Dienste müssen offenbar auch nicht entgeltlich erbracht werden.

Praktische Auswirkung
Kein DVD liegt vor, wenn lediglich physische Waren oder Räume bereitgestellt werden (z. B. Server-Racks oder Teile von Datencentern). Ebenfalls aus dem Anwendungsbereich scheiden Web-Angebote aus, die keinen Vertragsschluss erfordern (wie oft bei frei auf Websites verfügbaren Angeboten).

3.1.2 Flächendeckend und auf Abruf verfügbar

Aus den Merkmalen, »flächendeckend und auf Abruf verfügbar« zu sein, folgt vor allem, dass DVD jederzeit und von jedem Ort aus erreichbar sein müssen, faktisch also internetbasiert (oder mittels vergleichbarer Technologien) angeboten werden müssen. Die Erwägungsgründe geben zu diesen Merkmalen wenig relevante Informationen und auch die uneinheitliche deutsche Übersetzung[175] hilft nicht viel weiter, sodass es nahe

[173] Dafür spricht i.E. auch der Vergleich mit der Definition eines "digitalen Dienstes" in der NIS2-Richtlinie, (EU) 2022/2555; vgl. zur Verwandtschaft mit der NIS2-Richtlinie auch NK Data Act/Linardatos, 2. Aufl. 2025, Art. 23 DA Rn. 19.
[174] Art. 3 Nr. 30 DA.
[175] Der in der englischen (Ursprungs-)Fassung verwendete Begriff "ubiquitous" wurde dabei in der deutschen Sprachfassung DVD als "flächendeckend", im erläuternden EG 80 S. 4 DA dagegen als "ortsunabhängig" übersetzt.

liegt, dass hiermit lediglich der Charakter von DVD als nicht-stationäre Dienste klargestellt wird, auf die (in der Regel über das Internet)[176] von verschiedenen Geräten (und Orten) nach Wahl des Kunden zugegriffen werden kann.[177]

Praktische Auswirkung
Alle Dienste, die lediglich an bestimmten Orten bereitgestellt werden (Beispiel: (a) Feste Terminals in Einkaufscentern, (b) Leih-Tablets in Museen und Galerien oder (c) bloße physische Hardware – etwa Server in Datencentern – soweit nicht auch eine digitale Zugriffsmöglichkeit eingeräumt wird) scheiden aus dem Anwendungsbereich aus.

3.1.3 Netzzugang zu einem gemeinsam genutzten Pool von Rechenressourcen ermöglichen

Eines der interessanteren (und zukünftig wohl vornehmlich von der Rechtsprechung auszufüllenden) Definitionsmerkmale der DVD ist, dass diese den Netzzugang zu einem gemeinsam genutzten Pool von Rechenressourcen ermöglichen sollen. Was damit gemeint ist, erschließt sich erst auf den zweiten Blick und unter Hinzuziehen der Erwägungsgründe:

Die Definition von »Rechenressourcen« meint letztlich jede Hard- oder Software-Lösung,[178] und ist somit sehr vage formuliert. Dass es sich hierbei aber um einen »gemeinsam genutzten Pool« handeln soll, verengt den Anwendungsbereich nicht unerheblich. Die Ressourcen eines DVD müssen nämlich gerade mehreren »Nutzern«[179] bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen (können).[180] Die eigentliche (Daten-)Verarbeitung soll dabei allerdings für jeden Nutzer getrennt erfolgen und nur dieselbe elektronische Ausrüstung genutzt werden.[181]

Praktische Auswirkung
Durch die Verwendung von dedizierter Hardware, die jeweils nur einzelnen Empfängern zur Verfügung steht, scheiden solche Dienste aus dem Regelungspaket für DVD aus. Bis es allerdings eine Klarstellung zum »Nutzer«-Begriff (also den Empfängern der Dienste) gibt, genügt es bereits, wenn die Nutzung des Dienstes durch verschiedene Personen zulässig ist, um trotz dedizierter Hardware doch wieder als DVD qualifizierbar zu sein (vorausgesetzt alle anderen Merkmale liegen vor).

[176] Vgl. auch NK Data Act/Linardatos, 2. Aufl. 2025, Art. 23 DA Rn. 28.
[177] So i.E. auch Pommerening/Nickel, RDi 2024, 289 (290).
[178] EG 80 S. 2 DA verweist weitreichend auf "Ressourcen wie etwa Netze, Server oder sonstige virtuelle oder physische Infrastrukturen, Software – einschließlich Tools zur Entwicklung von Software –, Speicher, Anwendungen und Dienste" und ergänzend wird in EG 81 S. 3 und 4 DA wird allgemein nur von einer Kombination von IKT-Ressourcen gesprochen, was im Ergebnis nur den Schluss zulässt, dass hiermit potentiell jegliche Informations- und Telekommunikationstechnik bzw. jede Kombination daraus umschrieben werden soll.
[179] Es ist misslich, dass die Bereitstellung laut EG 80 S. 7 DA an mehrere "Nutzer" erfolgen soll, denn hierbei handelt es sich eigentlich um einen in Art. 2 Abs. 12 DA definierten Begriff. Dieser passt im vorliegenden Kontext allerdings offensichtlich nicht, da der definierte Nutzer-Begriff nur Benutzer von "vernetzten Produkten" adressiert, sodass ein redaktionelles Versehen auf der Hand liegt. Naheliegend scheint daher, dass es weder um den definierten "Nutzer", noch um den Kunden (also Vertragspartner) gehen soll, sondern letztlich nur gemeint sein dürfte, dass mehrere Personen die Ressourcen gemeinsam nutzen können. Hier ist aber gerichtliche Klarstellung abzuwarten.
[180] EG 80 S. 7 DA.
[181] EG 80 S. 7 DA.

3.1.4 Konfigurierbar, skalierbar und elastisch

Der »Cloud-Ansatz« des DA wird durch die Anforderung für DVD, »konfigurierbar, skalierbar und elastisch« zu sein, besonders deutlich. Hiernach müssen DVD bedarfsgesteuert die eingesetzte Hardware zur Bewältigung von Anfragen anpassen können – denn »skalierbar« sind nur Dienste, die flexible Zuweisung von Ressourcen, unabhängig von ihrem geografischen Standort, vornehmen (können), um Nachfrageschwankungen auszugleichen.[182] Das Konzept der Skalierbarkeit wird durch die »Elastizität« der Ressourcen, d. h. die Fähigkeit, diese Ressourcen entsprechend der Arbeitslast und der Nachfrage schnell zu erhöhen oder zu verringern,[183] sogar noch verstärkt.

Auf die nötige »Konfigurierbarkeit« der Ressourcen geht der DA hingegen nicht weiter ein, was (erneut) der Rechtsprechung die Auslegung eines elementaren Elements überlässt. Nach allgemeinem Sprachgebrauch dürfte entscheidend sein, ob die Kunden[184] die Möglichkeit haben, die bereitgestellten IKT-Ressourcen zu beeinflussen (zu konfigurieren). Es bleibt aber völlig offen, ob die Konfigurierbarkeit allein auf Hardware- oder Software-Ebene genügt oder beides möglich sein muss. Je nachdem, wie eng oder weit dieser Begriff zukünftig durch die Gerichte interpretiert wird, könnten dadurch alle Dienste/Produkte aus dem Anwendungsbereich ausscheiden, die keine echte technische Konfigurationsmöglichkeit für die Kunden bieten, sondern allenfalls einzelne Parameter (z. B. die Nutzerzahl oder der gebuchte Speicherplatz) dem Kunden zur Auswahl überlassen. Gleichermaßen könnte der Begriff aber auch weiter verstanden werden, sodass es ausreichen würde, wenn der Kunde in der Lage ist, einzelne Merkmale der Dienstleistung, einschließlich nichttechnischer Elemente, zu ändern. Fest steht vorerst, dass hiernach ein Mindestmaß an Einfluss der Kunden auf das bereitgestellte Produkt bestehen muss.

Praktische Auswirkung
Dienste, die auf dediziert zugeordneten Rechenressourcen betrieben werden (z. B. »traditionelle« SaaS-Anwendungen oder reine Hosting-Dienste[185] oder »Private-Cloud«-Anwendungen) fallen, im Gegensatz zu solchen, die mittels einer »echten« Cloud bereitgestellt werden, nicht unter die Definition von DVD. Gleichermaßen scheiden alle »Fertigprodukte« aus dem Anwendungsbereich aus, die keinerlei Konfigurationsmöglichkeit für die Kunden bieten.

3.1.5 Zentralisierte, verteilte oder hochgradig verteilte Art

Die Verweise auf »zentralisierte« und »verteilte« (bzw. »hochgradig verteilte«) Bereitstellung sind relativ inhaltsleer und unterstreichen lediglich, dass neben »klassischen« Bereitstellungsmodellen auch moderne geräte- und

[182] EG 80 S. 5 DA.
[183] Vgl. EG 80 S. 6 DA.
[184] Vom Wortlaut her ist es nicht eindeutig, dass die Kunden die Konfigurationsmöglichkeit haben müssen. Allerdings scheint es zumindest fernliegend, dass es genügen soll, wenn die Anbieter selbst ihre Dienste konfigurieren können müssen – letzteres wäre schließlich bei jedem kommerziellen Angebot der Fall. Ob hingegen eine Konfiguration auch durch einzelne Benutzer möglich sein muss, ist nicht im Wortlaut angelegt, sodass das Abstellen auf die Kunden (die in der Definition genannt sind) naheliegt.
[185] NK Data Act/Linardatos, 2. Aufl. 2025, Art. 23 DA Rn. 22.

standortübergreifende technische Lösungen als DVD erfassbar sind. Die »verteilte« Bereitstellung von IKT-Ressourcen bedeutet nur, dass vernetzte Computer oder Geräte untereinander kommunizieren und sich koordinieren.[186] Da die Definition jedoch auch »zentralisierte« Ressourcen umfasst, wird klar, dass es sich gerade nicht um Exklusivitätsmerkmale von DVD handelt, sondern auch »klassische« zentralisierte Bereitstellungsarten von Ressourcen (z. B. auf einem einzelnen Server) erfasst sein sollen.

Praktische Auswirkung
Auch Internet of Things-Modelle (insb. EDGE-Computing) und andere dezentrale Systeme können – neben klassischen zentralisierten Systemen – DVD darstellen.

3.1.6 Rasche Bereitstellung und Freigabe mit minimalem Verwaltungsaufwand oder minimaler Interaktion

Schließlich sollen DVD sich dadurch qualifizieren, dass sie »mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können«. Dieses Merkmal dürfte praktisch zu einer nicht unerheblichen Begrenzung des Spektrums möglicher DVD führen und komplexere Hard- oder Softwarelösungen ausschließen, sofern diese eine mehr als minimale erstmalige Integration bzw. Implementierungsleistung erfordern.

Zwar liefern die Erwägungsgründe hierzu nur einen Beispielsfall, wonach minimaler Verwaltungsaufwand und minimale Interaktion zwischen Anbieter und Kunde besteht, wenn Kunden[187] sich »ohne Interaktion mit den Anbieter […] Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz selbst zuweisen können«.[188] Es scheint aber insofern darum zu gehen, dass ein DVD schnell konfiguriert (siehe bereits Abschnitt 3.1.4) und dann bereitgestellt werden kann und Kunden dazu nicht mehr als »minimalen« Aufwand oder Interaktion mit dem Anbieter benötigen. Es ist hier unerheblich, ob der Konfigurationsaufwand schwerpunktmäßig beim Kunden liegt oder dieser durch den Anbieter erfolgt, aber dazu mehr als minimale Interaktionen (also insb. Absprache) mit dem Kunden erforderlich sind.[189] Auch scheiden solche Dienste aus, die zwar vollständig vom Anbieter für die Kunden konfiguriert werden (also ohne Interaktion oder Verwaltungsaufwand für/mit den Kunden), bei denen diese Konfiguration und anschließende Bereitstellung/Freigabe aber nicht mehr »rasch« erfolgt.[190]

Praktische Auswirkung
Angebote, die nicht »von der Stange« sind oder mehr als minimale Konfiguration erfordern, scheiden als DVD aus. Das dürfte insbesondere für komplexere Softwarelösungen und für jeglichen Bezug sonstiger Ressourcen gelten, wenn dieser

[186] Vgl. EG 80 S. 8 DA; erfasst soll außerdem das "EDGE"-Computing sein, bei dem die Verarbeitung direkt am Ort der Datenerhebung erfolgt (vgl. EG 80 S. 9 und 10 DA).
[187] An dieser Stelle sind also die Vertragspartner und nicht nötiger Weise jeder einzelne Benutzer gemeint.
[188] Vgl. EG 80 S. 3 DA.
[189] Dies folgt daraus, dass per Definition Verwaltungsaufwand und Interaktion alternativ nebeneinander stehen.
[190] Was "rasch" ist, wird erneut von der Rechtsprechung auszufüllen sein. Angesichts des digitalen Hintergrunds der Regelung und der in diesem Bereich typischen sofortigen Bereitstellungsmöglichkeit, kann aber davon ausgegangen werden, dass die Bereitstellungszeit tendenziell sehr gering ist (so auch HK-DatenR/Linardatos, 2. Aufl. 2025, DA Art. 23 Rn. 26).

zunächst eine genauere Abstimmung erfordert. Da gleichzeitig eine Konfigurierbarkeit aber zwingendes Merkmal jedes DVD ist, bleiben vor allem Angebote übrig, die den Kunden eine Wahlmöglichkeit verschiedener Optionen einräumen, ohne darüber hinaus Abstimmungen mit dem Kunden zu erfordern.

3.2 Persönlicher Anwendungsbereich

Dr. Viola Bensinger (Anwältin), Greenberg Traurig Germany, LLP | Jana Rudt (Anwältin), Greenberg Traurig Germany, LLP | Dr. Jannis Dietrich-Webb (Anwalt), Greenberg Traurig Germany, LLP

Ergänzend zum sachlichen Anwendungsbereich stellt sich die Frage, welche Personen oder Unternehmen in den persönlichen Anwendungsbereich von Kapitel VI DA fallen. Die Regelungen der Art. 23 ff. DA erstrecken sich dabei auf die Kategorien »Anbieter«, »Kunden« und »Beteiligte«.

Die Art. 23 ff. DA verpflichten Anbieter von Datenverarbeitungsdiensten ausdrücklich zur Einhaltung der dort festgelegten Vorgaben. Der Begriff »Anbieter« wird im DA nicht gesondert definiert, umfasst jedoch sowohl natürliche als auch juristische Personen, unabhängig von der Größe des Unternehmens.[191] Ausgenommen vom Anwendungsbereich sind hingegen Akteure, die keine Datenverarbeitungsdienste anbieten, wie beispielsweise Arbeitnehmer, Entwicklungsdienstleister oder Zulieferer.[192]

Der Begriff des »Kunden« ist im DA weit gefasst und umfasst nach der Legaldefinition in Art. 2 Nr. 30 DA »eine natürliche oder juristische Person, die mit einem Anbieter von Datenverarbeitungsdiensten eine vertragliche Beziehung eingegangen ist, um einen oder mehrere Datenverarbeitungsdienste in Anspruch zu nehmen«. Diese Definition schließt sowohl Verbraucher als auch Unternehmer ein,[193] unabhängig davon, ob die Vertragsbeziehung mit dem Datenverarbeitungsdienst entgeltlich oder unentgeltlich ist.[194] Nach EG 91 DA können Kunden selbst Anbieter von solchen Diensten sein, was den Austausch und die Migration zwischen verschiedenen Dienstleistern erleichtern soll. Damit wird der Anwendungsbereich des Kapitels VI DA auf ein breites Spektrum von Akteuren ausgeweitet.

Nach Art. 27 DA arbeiten »alle Beteiligten« nach Treu und Glauben zusammen. Unter den »Beteiligten« werden sowohl die bisherigen als auch die übernehmenden Anbieter des Datenverarbeitungsdienstes verstanden.[195] Der Kunde, der den Wechsel initiiert, gehört ebenfalls zu den Beteiligten, da er von der Zusammenarbeit der Anbieter profitiert.[196] Darüber hinaus können auch Dritte eine Rolle spielen. Laut EG 85, 89 DA

[191] Determann, in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 36 Rn. 21.
[192] Determann, in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 3 Rn. 99f.
[193] Linardatos, in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 23 Rn. 15.
[194] Schild, in: BeckOK DatenschutzR, 51. Aufl. 2025, Art. 2 DA Rn. 168.
[195] Linardatos in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 27 Rn. 6f.
[196] Linardatos in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 27 Rn. 6f.

können solche Dritte im Namen des Kunden oder des ursprünglichen Anbieters eingeschaltet werden, um den Wechselprozess zu unterstützen. Insgesamt umfasst der Begriff »Beteiligte« somit alle Akteure, die direkt oder indirekt am Wechselprozess beteiligt sind.

Zusammenfassend lässt sich festhalten, dass der persönliche Anwendungsbereich des Kapitels VI DA breit gestaltet ist, um eine effektive Umsetzung der Vorschriften zum Cloud Switching zu gewährleisten. Die Verpflichtungen erstrecken sich über Anbieter von Datenverarbeitungsdiensten, Kunden und Dritte, die aktiv am Wechselprozess beteiligt sind.

3.3 Geografischer Anwendungsbereich

Dr. Viola Bensinger (Anwältin), Greenberg Traurig Germany, LLP |
Dr. Paul Dürr (Anwalt), Greenberg Traurig Germany, LLP |
Dr. Ricarda Seifert (Anwältin), Greenberg Traurig Germany, LLP

3.3.1 Art. 1 Abs. 3 DA

Der geografische Anwendungsbereich des DA ist in Art. 1 Abs. 3 DA geregelt. Dort heißt es, dass der DA für »Anbieter von Datenverarbeitungsdiensten, unabhängig vom Ort ihrer Niederlassung, die Kunden in der Union solche Dienste erbringen« gilt[197]. Diese Formulierung klingt zunächst eindeutig nach dem bereits aus der DSGVO bekannten[198], sogenannten »Marktortprinzip«, nach dem das betreffende EU-Recht auch für Unternehmen gilt, die außerhalb der EU ansässig sind, aber ihre Dienstleistungen innerhalb des EU-Marktes anbieten. Im Fall des DA lässt die Formulierung jedoch Interpretationsspielraum offen: Unklar bleibt, ob sich die Regelung auf Dienstleistungen bezieht, die innerhalb der EU erbracht werden, oder ob entscheidend ist, dass die Kunden ihren Sitz in der EU haben. Warum der Gesetzgeber – anders als etwa in der KI-VO[199] oder dem DSA[200] – eine so offene und damit missverständliche Formulierung gewählt hat, lässt sich weder aus den Erwägungsgründen noch aus sonstigen Auslegungshilfen ableiten.

Zwar werden in der Praxis gerade Datenverarbeitungsdienste häufig am Standort des Kunden erbracht, insbesondere im Kontext multinationaler Unternehmensstrukturen (dazu nachfolgend), bei denen der Sitz/Standort des Kunden nicht zwingend mit dem Ort der Leistungserbringung übereinstimmt, kann die durch die Formulierung verursachte rechtliche Unklarheit aber erhebliche Auswirkungen haben. Für Datenverarbeitungsdienste, die definitionsgemäß aus der Ferne und über Netzwerke bereitgestellt werden, erscheint es deshalb überzeugend, Art. 1 Abs. 3 lit. f DA – entgegen der überwiegenden Ansicht in der bisher zu dieser Frage vorhandenen

[197] Art. 1 Abs. 3 lit. f DA.
[198] Art. 3 DS-GVO.
[199] siehe Art. 2 Abs. 1 lit. a - c DA.
[200] siehe Art. 2 Abs. 1 DA.

Literatur[201] – so auszulegen, dass er sich auf Dienstleistungen bezieht, die für Kunden mit Sitz/Standort in der EU erbracht werden. Das gilt gerade für Cloud-Dienste, bei denen unklar ist, ob sie am Standort des Anbieters, des Empfängers oder der genutzten technischen Infrastruktur wie etwa Servern oder Rechenzentren als erbracht gelten sollen. Es ist kaum anzunehmen, dass der Gesetzgeber den Anwendungsbereich des DA an derart unbeständige und schwer greifbare Kriterien knüpfen wollte.

3.3.2 Multinationale Konstellationen

Besondere Auswirkungen hat die Auslegung von Art. 1 Abs. 3 lit. f DA in Konstellationen, in denen der Vertrag mit einer Unternehmenseinheit außerhalb der EU geschlossen wurde, die Datenverarbeitungsdienste aber auch (oder ausschließlich) von verbundenen Unternehmen oder Niederlassungen innerhalb der EU genutzt werden. Zur Veranschaulichung lässt sich folgendes Beispiel anführen:

Ein US-amerikanischer Mutterkonzern schließt einen Vertrag über Cloud-Dienstleistungen mit einem Anbieter außerhalb der EU. Die tatsächliche Nutzung der Dienste erfolgt jedoch überwiegend durch Tochtergesellschaften in der EU. Obwohl der Vertrag nur zwischen dem US-Unternehmen und dem außereuropäischen Dienstleister besteht, stellt sich die Frage, ob die europäischen Niederlassungen – als tatsächliche Nutzer der Dienste – ebenfalls als »Kunden« im Sinne des DA zu betrachten sind.

Hier ist unklar, ob unter »Kunde« nur die vertragsschließende Partei zu verstehen ist, oder auch andere Entitäten, die die angebotenen Leistungen erhalten oder nutzen. Die Definition des »Kunden« im DA[202] spricht allerdings dafür, Art. 1 Abs. 3 lit. f DA derart auszulegen, dass es für die Qualifikation als »Kunde« auf den Sitz des Vertragspartners ankommt, also jeweils die Entität, die den Vertrag mit dem Dienstanbieter abgeschlossen hat. Dennoch besteht ein gewisses Risiko, dass Gerichte den DA großzügiger auslegen und als Kunden auch diejenige Entität verstehen, die die Leistungen tatsächlich in Anspruch nimmt. Dann könnten über diesen Weg auch Unternehmen in der EU von den im DA vorgesehenen Wechselrechten profitieren, die selbst nicht Vertragspartner des Dienstanbieters sind.

3.3.3 Praktische Konsequenzen

Aus der hier vertretenen Auslegung des Art. 1 Abs. 3 DA ergeben sich folgende Konsequenzen für die Praxis:

- Verträge mit Kunden mit Sitz/Standort in der EU unterfallen dem Anwendungsbereich des DA, unabhängig davon, wo die Leistung tatsächlich erbracht wird.
- Der Sitz des Dienstanbieters ist für die geografische Anwendbarkeit des DA nicht von Bedeutung. Daraus folgt, dass auch die **gezielte Auswahl eines EU- bzw. Nicht-**

[201] Specht-Riemenschneider, in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 1 Abs. 3 Rn. 50; Veil, in: BeckOK DatenschutzR, 51. Aufl. 2025, Art. 1 DA Rn. 193; Schreiber/Pommerening/Schoel, in: Schreiber/ Pommerening/Schoel, Der neue Data Act (DA), 2. Auflage 2024, § 3 Rn. 13.
[202] Art. 2 Nr. 30 DA.

EU-Standortes des Anbieters für den Abschluss des Datenverarbeitungsvertrags **irrelevant ist**.

- Der DA findet in den meisten Fällen **keine Anwendung**, wenn der Vertrag mit einem **Kunden außerhalb der EU** geschlossen wurde, unabhängig davon, wo die Leistung tatsächlich erbracht wird.[203]

3.3.4 Eigenständiger Regelungsbereich des Art. 1 Abs. 1 DA?

Art. 1 Abs. 1 DA bezweckt die Schaffung einheitlicher Vorschriften für den Umgang mit Daten. In der Literatur wird teilweise diskutiert, ob dieser Absatz einen eigenen Regelungsbereich darstellt.[204] Wäre dies der Fall, würde die Harmonisierung auf EU-Ebene nur die ausdrücklich genannten Bereiche erfassen – etwa die Datenbereitstellung, den Wechsel zwischen Datenverarbeitungsdiensten, Schutz vor unbefugtem Drittzugriff sowie die Förderung von Interoperabilität, also der Fähigkeit verschiedener Systeme, nahtlos zusammenzuarbeiten, Informationen auszutauschen und diese Informationen korrekt zu verarbeiten und zu nutzen, auch wenn sie von unterschiedlichen Anbietern stammen oder auf unterschiedlichen Technologien basieren. Dagegen spricht mitunter der Wortlaut der Norm, der diese Bereiche »unter anderem« nennt und auf eine umfassende Harmonisierung hindeutet.

3.4 Zeitlicher Anwendungsbereich

Dr. Viola Bensinger (Anwältin), Greenberg Traurig Germany, LLP |
Dr. Paul Dürr (Anwalt), Greenberg Traurig Germany, LLP |
Dr. Ricarda Seifert (Anwältin), Greenberg Traurig Germany, LLP

Der DA gilt ab dem 12. September 2025.[205] Der Gesetzgeber hat jedoch nicht ausdrücklich klargestellt, ob die Verordnung – insbesondere Kapitel VI DA – ausschließlich für Verträge gilt, die nach diesem Datum geschlossen werden oder aber auch auf bereits bestehende Verträge Anwendung findet.

Bislang fehlt es zu dieser Frage an behördlichen Auslegungsrichtlinien und gefestigten Stellungnahmen in der juristischen Fachliteratur.[206] Die EU-KOM scheint von der Geltung auch für bestehende Verträge auszugehen.[207] Für diese Annahme ließe sich anführen, dass für Kapitel VI – anders als für Kapitel IV – des DA keine ausdrückliche

[203] In multinationalen Unternehmensstrukturen entscheidet nach hiesiger Auslegung – auch bei tatsächlicher Nutzung der Dienste durch Entitäten innerhalb der EU – allein der Sitz des Vertragspartners als Kunden über die Anwendbarkeit des Data Acts. Es ist aber nicht auszuschließen, dass Gerichte den Begriff des Kunden weiter auslegen und entsprechend zu einer Anwendbarkeit des Data Acts in Abhängigkeit vom Standort der die Dienste nutzenden Entitäten gelangen werden.
[204] Veil, in: BeckOK DatenschutzR, 51. Aufl. 2025, Art. 1 DA Rn. 12; Specht-Riemenschneider, in: Specht/Hennemann, Data Act/Data Governance Act, Art. 1 Rn. 32.
[205] Art. 50 Abs. 2 DA.
[206] Von einer Anwendung des DA auf Bestandsverträge ausgehend, soweit keine Ausnahmen vorgesehen sind, allerdings Hennemann, in: Specht/Hennemann, Data Act/Data Governance Act, Art. 50 Rn. 5.
[207] EU-KOM, Standard Contractual Clauses (SCCs) - Switching and Exit, Termination, Security and Business Continuity Webinar, 10. April 2025.

Übergangsphase im Gesetzestext vorgesehen ist,[208] der Gesetzgeber also im Umkehrschluss hier von einer Anwendbarkeit auf bestehende Verträge auszugehen scheint.[209]

Das Fehlen einer Übergangsregelung ließe sich aber ebenso gut als Argument dafür anführen, dass der Gesetzgeber durch das Weglassen einer ausdrücklichen Regelung zur Anwendbarkeit von Kapitel VI auf bestehende Verträge eine rückwirkende Geltung gerade nicht vorgesehen hat. Diese Auslegung wird auch von Art. 25 DA gestützt, der verlangt, dass vertragliche Pflichten »eindeutig in einem schriftlichen Vertrag« festgelegt sein müssen, was nahelegt, dass neue Regelungen zwischen den Parteien vertraglich vereinbart und nicht nur einseitig festgelegt werden sollen – eine Pflicht, die sich nur für Neuverträge erfüllen lässt. Zudem bestehen verfassungsrechtliche Bedenken gegen die Anwendung auf bestehende Verträge: Eine rückwirkende Anwendung auf Altverträge könnte sowohl gegen EU-Recht als auch gegen nationales Verfassungsrecht verstoßen. Rückwirkende Gesetze sind grundsätzlich unzulässig, wenn sie in bestehende Rechtspositionen eingreifen und berechtigte Erwartungen der Vertragsparteien beeinträchtigen. Auch die Schaffung neuer Kündigungsrechte könnte als unzulässiger Eingriff in die unternehmerische Freiheit gewertet werden. Insgesamt sprechen daher einige Argumente gegen eine rückwirkende Anwendung von Kapitel VI DA.

3.5 Beseitigung von Wechselhürden (Art. 23 DA)

Florian Schwind, Rechtsanwalt, Reed Smith LLP |
Lukas Willecke, Rechtsanwalt, Reed Smith LLP

EG 78, 85, 91, 93 DA

3.5.1 Allgemeines sowie Sinn und Zweck des Art. 23 DA

Art. 23 bildet die zentrale Grundlage für die Regelungen des Kapitel VI zum Wechsel zwischen Datenverarbeitungsdiensten und legt die Pflichten fest, die durch die nachfolgenden Art. 24 – 31 und 34 DA konkretisiert werden.

Sinn und Zweck dieser Vorschrift ist es, die Wechselmöglichkeiten für Kunden von Datenverarbeitungsdiensten zu erleichtern (spiegelbildlich gesprochen also »Lock-in-Effekte« abzubauen), die Interoperabilität von Daten sowie Mechanismen und Diensten für die Weitergabe zu verbessern und praktische Hindernisse wie hohe Kosten, lange Bearbeitungszeiten, unklare Verträge oder technische Probleme (bspw. Inkompatibilität der Daten) für einen Anbieterwechsel zu beseitigen. Damit soll insbesondere der Aufwand für den Kunden sowohl in zeitlicher als auch in finanzieller Hinsicht reduziert werden. Zugleich zielt die Maßnahme auf die Förderung eines

[208] Vgl. Art. 50 Abs. 1 DA.
[209] So zu verstehen etwa Hennemann, in: Specht/Hennemann, Data Act/Data Governance Act, Art. 50 Rn. 5.

stärker wettbewerbsorientierten, offenen und innovationsfreundlichen Marktes für Datenverarbeitungsdienste in der Europäischen Union ab.

> Art. 2 Nr. 34 DA definiert Wechsel als »den Prozess, an dem ein Quellenanbieter von Datenverarbeitungsdiensten, ein Kunde eines Datenverarbeitungsdienstes und gegebenenfalls ein übernehmender Anbieter von Datenverarbeitungsdiensten beteiligt sind und bei dem der Kunde eines Datenverarbeitungsdienstes von der Nutzung eines Datenverarbeitungsdienstes zur Nutzung eines anderen Datenverarbeitungsdienstes der gleichen Dienstart oder eines anderen Dienstes, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird oder der einem einer IKT-Infrastruktur in eigenen Räumlichkeiten angeboten wird, auch durch Extraktion, Umwandlung und Hochladen der Daten, wechselt«.

Hintergrund der Einführung ist die Zurückhaltung der Datenverarbeitungsdienste, sich eigene Verhaltensregeln auf Grundlage der Datenverkehrsverordnung[210] zu geben. Der europäische Gesetzgeber sah deshalb die Notwendigkeit, regulatorische Mindestverpflichtungen festzulegen. Diese sollen sämtliche vorkommerziellen, gewerblichen, technischen, vertraglichen und organisatorischen Hindernisse beseitigen, die Kunden von Datenverarbeitungsdiensten daran hindern könnten, den Anbieter zu wechseln, Verträge zu kündigen, neue Verträge mit anderen Anbietern abzuschließen, ihre exportierbaren Daten und digitalen Vermögenswerte zu übertragen oder mehrere Anbieter parallel zu nutzen (sog. Multi-Cloud-Ansatz).

3.5.2 Der Begriff des »Wechsels«

Heruntergebrochen geht es um den Prozess, bei dem ein Kunde von einem Datenverarbeitungsdienst – insbesondere Cloud- und vergleichbaren Diensten – flexibel zu einem anderen Anbieter derselben Dienstart oder zu einer eigenen IKT-Infrastruktur wechselt oder mehrere Datenverarbeitungsdienste gleichzeitig in Anspruch nehmen möchte. Der Begriff ist folglich weit gefasst und umfasst nicht nur den vollständigen Anbieterwechsel, sondern auch die parallele Nutzung mehrerer

[210] ABl. L 303, 2018/1807, 28.11.2018, S. 59ff.

Dienste (siehe hierzu insb. Art. 34 DA und Abschnitt 3.14) sowie den (teilweisen) Wechsel auf eigene Systeme.

Ziel ist es, sogenannte »Lock-in-Effekte« zu vermeiden – also Situationen, in denen Kunden durch technische, vertragliche oder organisatorische Hürden an einen Anbieter gebunden bleiben. Um dieses Ziel zu erreichen, verbietet Art. 23 S. 2 DA den Anbietern von Datenverarbeitungsdiensten derartige Wechselhindernisse zu errichten. Die dabei von den Beteiligten zu beachtenden Modalitäten sind in Art. 23 S. 2 DA aufgezählt (siehe dazu unter Abschnitt 3.5.2.3) und weitere Einzelheiten in den Art. 25 ff. DA geregelt.

3.5.2.1 Wechselziele

Ein Wechsel im Sinne von Art. 23 DA kann auf drei verschiedene Arten erfolgen, die jeweils unterschiedliche Wechselziele betreffen:

> Art. 2 Nr. 9 DA definiert »gleiche Dienstart« als »eine Reihe von Datenverarbeitungsdiensten, die dasselbe Hauptziel haben und dasselbe Dienstmodell für die Datenverarbeitung sowie dieselben Hauptfunktionen aufweisen.«

Wechsel zu einem Datenverarbeitungsdienst mit gleicher Dienstart
Eine »gleiche Dienstart« liegt vor, wenn alle folgenden drei Merkmale gleichzeitig erfüllt sind:

- **Hauptziel:** Beide Dienste verfolgen denselben primären Zweck, etwa Speicherung strukturierter Daten.
- **Dienstmodell:** Die Art der Bereitstellung ist identisch, z. B. SaaS zu SaaS. Ein Wechsel zwischen unterschiedlichen Modellen (z. B. SaaS zu PaaS) ist nicht erfasst.[211]
- **Hauptfunktionen:** Die zentralen Funktionen der Dienste stimmen überein, wobei die Bewertung objektiv aus Sicht eines verständigen Dritten erfolgt.[212]

Das Merkmal der »gleichen Dienstart« ist eng auszulegen und setzt eine funktionale Gleichwertigkeit voraus. Ziel ist es, echte Wechselmöglichkeiten zu schaffen, ohne Anbieter zur Interoperabilität völlig unterschiedlicher Dienste zu verpflichten.[213]

Auch wenn Dienste auf den ersten Blick ähnlich erscheinen, können sie sich durch unterschiedliche Datenverarbeitungsmodelle, Vertriebsmodelle oder Anwendungsfälle in Untergruppen unterscheiden. Entscheidend ist, dass die o.g. Kernmerkmale

[211] Pommerening/Nickel, RDi 2024, 289 (293).
[212] BeckOK DatenschutzR/Schmidt-Wudy DA Art. 23 Rn. 33.
[213] HK-DatenR/Linardatos DA Art. 23 Rn. 35.

übereinstimmen; Unterschiede in Leistung, Sicherheit oder Qualität sind dabei unerheblich.[214]

Wechsel zu einer IKT-Infrastruktur in eigenen Räumlichkeiten

> Art. 2 Nr. 33 DA bezeichnet »IKT-Infrastruktur in eigenen Räumlichkeiten« als »IKT-Infrastruktur und Rechenressourcen, die im Eigentum des Kunden stehen oder vom Kunden gemietet oder geleast werden und die sich im Rechenzentrum des Kunden befinden und von ihm oder einem Dritten betrieben wird bzw. werden«.

Auch wenn sich Kunden von Datenverarbeitungsdiensten dazu entscheiden, auf eine eigene IKT-Infrastruktur zu wechseln, gilt dies als Wechsel im Sinne von Art. 23 DA und die Maßnahmen und Verbote der Art. 25 ff. DA finden Anwendung.

Gleichzeitige Inanspruchnahme mehrerer Anbieter von Datenverarbeitungsdiensten
Die dritte von der Vorschrift umfasste Wechselkonstellation betrifft die gleichzeitige Nutzung mehrerer Datenverarbeitungsdienste (sog. Multi-Cloud-Ansatz zur Vermeidung von Abhängigkeiten und zur Steigerung der Betriebsstabilität)[215], auch wenn in diesem Fall kein vollständiger Anbieterwechsel erfolgt. Erfasst werden soll dabei nicht nur die gleichzeitige Nutzung gleicher Dienstarten, sondern auch die parallele Nutzung sich ergänzender Datenverarbeitungsdienste.

3.5.2.3 Verpflichtende Maßnahmen aus Art. 23 S. 1 DA

Art. 23 S. 1 DA bestimmt als Ausgangspunkt, dass Datenverarbeitungsdienste erfolgsbezogen handeln müssen – bloße Bemühungen sind nicht ausreichend[216] – und Datenverarbeitungsdienste die Maßnahmen aus den Art. 25 bis 30 DA umsetzen müssen.

Verbot von Wechselhindernissen und Beseitigungspflicht aus Art. 23 S. 2 DA
Art. 23 S. 2 DA benennt explizit die Art der Hindernisse, die den Kunden nicht aufgezwungen werden dürfen – was abschließend unter diese Art der Hindernisse jeweils fällt, ist noch nicht geklärt:

1. **Vorkommerzielle** – Forschung, Entwicklung und Pilotphasen vor dem kommerziellen Rollout
2. **Gewerbliche** – Geschäftsmodelle, Preissetzung, Wettbewerbsstrategien
3. **Technische** – APIs, Datenformate, Interoperabilität insgesamt

[214] Siehe EG 81 DA.
[215] Siehe EG 99 DA.
[216] Vgl. HK-DatenR/Linardatos DA Art. 23 Rn. 37.

4. **Vertragliche** – AGB-Klauseln, insb. Kündigungsfristen

5. **Organisatorische** – Abläufe, Prozesse, Kommunikation oder auch Ressourcen

Zudem besteht eine Pflicht der Anbieter von Datenverarbeitungsdiensten, Hindernisse der oben genannten Arten zu beseitigen, welche die Kunden an den folgenden Handlungen bzw. Rechten hindern würden:

Art. 23 S. 2 lit. a DA – Kündigung des Vertrags nach maximaler Kündigungsfrist und erfolgreichem Wechsel
Anbieter von Datenverarbeitungsdiensten müssen solche Hindernisse beseitigen, die dem Kunden erschweren würden, den Vertrag über den Datenverarbeitungsdienst nach Ablauf der maximalen Kündigungsfrist von zwei Monaten[217] oder nach einem erfolgreichen Wechsel zu kündigen. Die Kündigung soll nach dem Wechsel ohne zusätzliche Hürden möglich sein.

Art. 23 S. 2 lit. b DA – Abschluss neuer Verträge mit anderen Anbietern
Es dürfen keine Hindernisse bestehen, die Kunden daran hindern, neue Verträge mit anderen Anbietern von Datenverarbeitungsdiensten für die gleiche Dienstart (zum Begriff siehe oben unter Abschnitt 3.5.2.1) abzuschließen. Dies umfasst beispielsweise das Verbot von Exklusivitätsklauseln – letztlich handelt es sich hierbei um eine »privatrechtliche Selbstverständlichkeit«[218].

Art. 23 S. 2 lit. c DA – Übertragung exportierbarer Daten und digitaler Vermögenswerte
Anbieter von Datenverarbeitungsdiensten sind verpflichtet, Kunden die Übertragung ihrer exportierbaren Daten[219] und digitalen Vermögenswerte[220] zu einem anderen Anbieter oder in eine eigene IKT-Infrastruktur zu übertragen. Dies gilt auch dann, wenn der Kunde zuvor ein unentgeltliches Angebot genutzt hat. Technische oder organisatorische Hindernisse, die eine solche Übertragung verhindern oder erschweren könnten, sind zu beseitigen.

Art. 23 S. 2 lit. d DA – Erreichung der Funktionsäquivalenz beim neuen Anbieter
Es dürfen keine Hindernisse bestehen, die verhindern, dass der Kunde nach dem Wechsel bei der Nutzung des neuen Datenverarbeitungsdienstes eine Funktionsäquivalenz[221] erreicht. Das bedeutet, dass die wesentlichen Funktionen, die der Kunde beim bisherigen Anbieter genutzt hat, auch beim neuen Anbieter auf Basis der übertragenen Daten und digitalen Vermögenswerte wiederhergestellt werden können.

Art. 23 S. 2 lit. e DA – Trennung einzelner Dienste
Anbieter von Datenverarbeitungsdiensten dürfen keine Hindernisse schaffen, die es Kunden unmöglich machen, bestimmte Datenverarbeitungsdienste von anderen, im Rahmen eines gemeinsamen Vertrags erbrachten Datenverarbeitungsdiensten zu trennen (sog. Unbundling), sofern dies technisch durchführbar ist. Im Rahmen dieser technischen Durchführbarkeit erscheint es sinnvoll, neben der technischen Möglichkeit

[217] Vgl. Art. 25 Abs. 2 lit. d DA.
[218] Zum Begriff: HK-DatenR/Linardatos DA Art. 23 Rn. 42.
[219] Zum Begriff siehe Art. 2 Nr. 38 DA.
[220] Zum Begriff siehe Art. 2 Nr. 32 DA.
[221] Zum Begriff vergleiche Art. 2 Nr. 37 sowie EG 86 DA.

auch wirtschaftliche Gründe (insbesondere, ob die Trennung mit ökonomisch vertretbarem Aufwand für den Datenverarbeitungsdienst durchzuführen ist) zu berücksichtigen. Kunden müssen also die Möglichkeit haben, einzelne Datenverarbeitungsdienste herauszulösen und zu einem anderen Anbieter zu wechseln, ohne an den gesamten »Dienstverbund« gebunden zu sein. Mittelbar führt dies zu einer Pflicht der Datenverarbeitungsdienste, modulare Dienste anzubieten.

3.5.2.4 Rechtsfolgen bei einer Zuwiderhandlung

Verstößt ein Unternehmen gegen die Vorgaben des Art. 23 DA, kann die zuständige Behörde Sanktionen gem. Art. 40 Abs. 1 DA verhängen. Nach dem aktuellen Entwurf des Durchführungsgesetzes[222] wäre die Bundesnetzagentur die zuständige Behörde, die bei Verstößen gegen Art. 23 S. 2 lit. a bis e DA ein Bußgeld oder eine Verwarnung aussprechen kann. Geldbußen nach DSGVO dürften ausgeschlossen sein, da das Kapitel VI nicht in Art. 40 Abs. 4 DA genannt wird.

3.5.2.5 Auswirkungen einer Zuwiderhandlung auf abgeschlossene Verträge

Der DA regelt nicht ausdrücklich[223], welche Folgen ein Verstoß gegen Art. 23 DA auf die geschlossenen Verträge zwischen Nutzern und Datenverarbeitungsdienste hat. Es ist naheliegend, dass die einzelnen Vertragsklauseln, die gegen Art. 23 DA verstoßen, unwirksam sind. Damit diese einzelne Unwirksamkeit nicht zur Unwirksamkeit des gesamten Vertrages führt (§ 139 BGB), bedarf es einer salvatorischen Klausel im Vertrag. Diese stellt sicher, dass der restliche Vertrag auch dann wirksam bleibt, wenn einzelne Regelungen unwirksam sind.

3.6 Tragweite der technischen Verpflichtungen (Art. 24 DA)

Lukas Mehl, Senior Data Protection Counsel, Telefónica Germany GmbH & Co. OHG

EG 85, 86 DA

3.6.1 Übersicht

Auch wenn der Wortlaut der Überschrift zu Art. 24 DA nur auf technische Verpflichtungen abstellt, so geht der Norminhalt als eine der zentralen Vorschriften

[222] BMWE, »Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG)«, Stand 07.02.2025, https://www.bmwk.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/20250214-entwurf-data-act-durchfuehrungsgesetz.html.
[223] Zum Problem: Heinzke, BB 2024, 1291; Piltz/Zwerschke, CR 2024, 153.

des Kapitel VI über rein technische Verpflichtungen hinaus. Art. 24 DA sieht vor, dass die in den Artikeln

- 23 (= Beseitigung von Hindernissen für einen wirksamen Wechsel),
- 25 (= Vertragsklauseln für den Wechsel),
- 29 (= Schrittweise Abschaffung von Wechselentgelten),
- 30 (= Technische Aspekte des Wechsels) und
- 34 (= Interoperabilität zu Zwecken der parallelen Nutzung von Datenverarbeitungsdiensten)[224]

festgelegten Verantwortlichkeiten für die Anbieter von Datenverarbeitungsdiensten für die Dienste, Dienstleistungen, Verträge oder Geschäftspraktiken gelten, die sie selbst erbringen.[225] Neben technischen Verpflichtungen sind über die Verweisnormen auch explizit vertragliche Vorgaben z. B. in Bezug auf Wechselentgelte oder Sorgfalts- und Informationspflichten umfasst. Demnach ist Art. 24 DA sowohl vor dem Hintergrund technischer als auch vertraglicher Aspekte zu betrachten. Diese Ausweitung deckt sich auch mit dem Zielgedanken der Norm. Vertragliche oder technische Einschränkungen, die einen unkomplizierten Wechsel des Kunden erschweren, sollen ausgeschlossen sein.

3.6.2 Adressaten

Adressaten des Art. 24 DA sind – auch wenn in der Fachliteratur vereinzelt abweichende Ansichten vertreten werden[226] – sowohl der ursprüngliche als auch der neue Anbieter sowie der Kunde selbst. Dies ergibt sich u. a. aus dem Wortlaut der englischen Sprachfassung (»The responsibilities of providers of data processing services …«), welcher klar auf eine Mehrzahl von Verantwortlichen verweist und somit eine ausschließliche Beschränkung auf den ursprünglichen Anbieter ausschließt. Art. 24 DA verfolgt gerade nicht die Zielsetzung, dass ausschließlich der ursprüngliche Anbieter dazu verpflichtet wird, das vertragliche, kommerzielle oder technische Umfeld in einer Weise zu replizieren, dass dessen Leistungsmerkmale oder Vertragsbedingungen mit jenen des übernehmenden Anbieters identisch sind.[227] Vielmehr regelt die Norm die Fortgeltung und Übertragung bestehender Verpflichtungen, die gegenüber dem originären Anbieter begründet wurden, auf den übernehmenden Anbieter im Rahmen des Anbieterwechsels. Nur hierdurch wird ein sachgerechter Wechsel in der Praxis gewährleistet. Eine wirksame, effiziente und gleichzeitig koordinierte Datenübermittlung wird nur durch ein kooperatives Zusammenwirken sämtlicher beteiligten Akteure erreicht. EG 86 S. 2 DA unterstreicht die Erforderlichkeit der Einbindung sämtlicher relevanter Beteiligten, da hiernach von Anbietern von Datenverarbeitungsdiensten lediglich erwartet wird, dass sie die

[224] Art. 34 verweist wieder zurück auf Art. 24 DA. Der rechtliche Mehrwert aus derartigen wechselseitigen Verweisen hat sich dem Verfasser bis zum Redaktionsschluss nicht offenbart.
[225] Lienemann in Hennemann/Ebner/Karsten/Lienemann/Wienroede, Data Act, S. 190f.
[226] z. B. Schmidt-Wudy in Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Art. 24 Rn. 1; Lienemann in Hennemann/Ebner/Karsten/Lienemann/Wienroede, DA, S. 191 und Bomhard, MMR 2024, 109 (110).
[227] vgl. Art. 30 Abs. 6 DA, der regelt, dass der ursprüngliche Anbieter nicht verpflichtet ist, neue Technologien oder Dienste zu entwickeln, um einem Antrag auf Wechsel oder Übertragung gemäß Art. 25 Abs. 2 lit. a DA zu entsprechen.

Funktionsäquivalenz[228] in Bezug auf die Funktionen ermöglichen, die sowohl vom ursprünglichen als auch vom übernehmenden Datenverarbeitungsdienst unabhängig voneinander angeboten werden. Eine derartige Auslegung des Adressatenkreises von Art. 24 DA führt auch nicht zu einer unverhältnismäßigen Benachteiligung der beteiligten Parteien, da die Pflichten aus Art. 24 DA mit Vollzug des Anbieterwechsels auf den übernehmenden Anbieter übergehen. Dieser unterliegt dann im Falle eines weiteren Wechsels denselben Verpflichtungen.

3.6.3 Verantwortungsbereiche der Anbieter

Art. 24 DA definiert für die beteiligten Anbieter und den Kunden eigene Verantwortungsbereiche. Hierbei wird klargestellt, welches Maß an Verantwortung den involvierten Parteien hinsichtlich des konkreten Bearbeitungsstadiums zugewiesen werden kann. Daher muss Art. 24 DA auch im Lichte des Regelungsziels von Art. 23 DA, sprich: der Sicherstellung eines effizienten Anbieterwechsels, betrachtet werden.[229] Die innerhalb von Art. 24 DA referenzierten Artikel umfassen dabei die »technischen« Verpflichtungen des übernehmenden Anbieters. Hierdurch wird verdeutlicht, dass ein daten-übernehmender Anbieter nicht verpflichtet wird, zusätzliche Erweiterungen oder Anpassungen an seinem Dienstleistungsportfolio vorzunehmen.[230] Die zu übernehmenden Leistungen beziehen sich auf Dienste, Verträge oder Geschäftsgepflogenheiten, die im Verhältnis zum ursprünglichen Anbieter bestanden haben. Der übernehmende Anbieter muss Funktionsäquivalenz[231] sicherstellen, er ist jedoch nicht verpflichtet, mit seinem Angebot über seinen gegenwärtigen Ist-Zustand hinauszugehen.[232] Die Entscheidung, einen Wechsel vorzunehmen – auch wenn dieser mit Einschränkungen bei bestimmten Parametern oder Funktionen verbunden ist – liegt ausschließlich im Ermessen des Kunden. Der übernehmende Anbieter ist jedoch nicht allein für die Erreichung der Funktionsäquivalenz verantwortlich. Der ursprüngliche Anbieter ist im Rahmen seiner Möglichkeiten und seines Verantwortungsbereiches für das Zustandekommen der Funktionsäquivalenz mitverantwortlich.

3.7 Vertragsklauseln für den Wechsel (Art. 25 DA)

Lukas Mehl, Senior Data Protection Counsel, Telefónica Germany GmbH & Co. OHG

[228] vgl. Art. 2 Nr. 37 DA; hiernach meint »Funktionsäquivalenz« die Wiederherstellung – auf der Grundlage der exportierbaren Daten und digitalen Vermögenswerte des Kunden – eines Mindestmaßes an Funktionalität in der Umgebung eines neuen Datenverarbeitungsdienstes der gleichen Dienstart nach dem Wechsel, wenn der übernehmende Datenverarbeitungsdienst als Reaktion auf dieselbe Eingabe für gemeinsame Funktionen, die dem Kunden im Rahmen des Vertrags bereitgestellt werden, ein materiell vergleichbares Ergebnis erbringt.
[229] Diese Verpflichtung ergibt sich bereits aus Art. 23 DA.
[230] Vgl. auch Art. 30 Abs. 6 DA. Hiernach ist ein Anbieter von Datenverarbeitungsdiensten nicht verpflichtet, neue Technologien oder Dienste zu entwickeln.
[231] Vgl. EG 86 zum DA.
[232] Linardatos in Specht/Hennemann, Data Act/Data Governance Act, Art. 24 Rn. 1-6.

EG 78, 79, 80, 81, 82, 83, 84, 94 DA – für Art. 23 DA sowie EG 85, 87 DA

3.7.1 Allgemeines

Gemäß Art. 25 Abs. 1 S. 1 DA sind die Rechte des Kunden und Pflichten des Anbieters von Datenverarbeitungsdiensten in Bezug auf einen Wechsel[233] eindeutig und in einem schriftlichen Vertrag festzulegen. Hierdurch sollen die Anforderungen aus Art. 23 DA konkretisiert werden. Dieser Vertrag muss dem Kunden ermöglichen, den Anbieter für die Datenverarbeitungsdienste zu wechseln.[234] Dabei muss sichergestellt sein, dass der Geschäftsbetrieb während des Wechsels weiterläuft.[235] Der Anbieter darf das Herausgeben der Daten nicht verzögern oder unterbrechen. Falls es dennoch zu unvorhergesehenen Unterbrechungen kommt, muss der Anbieter den Kunden darüber informieren.[236]

Bereits aus dem Wortlaut wird ersichtlich, dass die EU-KOM bei Erstellung das Szenario des »unterlegenen« Kunden gegen den verhandlungsstärkeren (Cloud-)Anbieter vor Augen hatte.[237] Die EU-KOM hat versucht, diesem unterstellten Ungleichgewicht dahingehend entgegenzuwirken, dass der Kunde nur Rechte erhält und der Anbieter des Datenverarbeitungsdienstes nur Pflichten. Der von der EU-KOM hierbei verfolgte Zweck liegt offensichtlich in dem Ausgleich des Verhandlungsungleichgewichtes durch eine vertragliche Gewährleistung der technischen Wechseldurchführbarkeit. Art. 25 DA soll dabei die in Kapitel VI angestrebte Wechseleffizienz vertraglich absichern, indem verbindliche Mindestinhalte für Verträge über Anbieterwechsel vorgegeben werden. Hierbei wird jedoch stark in die vertragliche Inhaltsfreiheit eingegriffen, da lediglich auf die Durchführbarkeit des Wechsels für den Kunden geachtet wird. So differenziert Art. 25 DA nicht innerhalb seines Kundenbegriffes.[238] So können sich Unternehmen, die als Datenverarbeitungsdienstleister tätig werden und ihrerseits als Kunde auftreten, ebenfalls von den Vorgaben des Art. 25 DA profitieren.[239] Insofern werden die Kundeninteressen in großem Maße übervorteilt, da der ursprüngliche Anbieter des Datenverarbeitungsdienstes dem jeweiligen Kunden bei dem Wechsel zum neuen Anbieter unterstützen muss. Inwieweit man hier noch von einem sachgerechten Interessensausgleich zwischen Verhinderung von Lock-in-Effekten und vertraglicher Inhaltsfreiheit sprechen kann, ist fraglich. Im Umgang mit Art. 25 DA ist zu beachten, dass dieser dem Kunden keine unmittelbaren Rechte und Ansprüche gegenüber einem Anbieter statuiert. Der Wortlaut des Art. 25 DA verpflichtet die Parteien lediglich dazu, einen »schriftlichen« Vertrag abzuschließen, der einen bestimmten Mindestinhalt zwingend zu regeln hat. Im Lichte des effet utile-Grundsatzes und der Wortlautanforderung, dass der Vertrag speicherbar und reproduzierbar sein muss, wird

[233] Der Begriff «Wechsel« ist in Art. 2 Nr. 34 DA legaldefiniert und bezeichnet den Prozess, »an dem ein Quellenanbieter von Datenverarbeitungsdiensten, ein Kunde eines Datenverarbeitungsdienstes und gegebenenfalls ein übernehmender Anbieter von Datenverarbeitungsdiensten beteiligt sind und bei dem der Kunde eines Datenverarbeitungsdienstes von der Nutzung eines Datenverarbeitungsdienstes zur Nutzung eines anderen Datenverarbeitungsdienstes der gleichen Dienstart oder eines anderen Dienstes, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird oder der einem einer IKT-Infrastruktur in eigenen Räumlichkeiten angeboten wird, auch durch Extraktion, Umwandlung und Hochladen der Daten, wechselt.«
[234] Vgl. Art. 25 Abs. 2 lit. a DA.
[235] Vgl. Art. 25 Abs. 2 lit. a ii DA
[236] Vgl. Art. 25 Abs. 2 lit. a iii DA.
[237] Pommerening/Nickel, RDi 2024, 289; Bomhard, MMR 2024, 109 ff
[238] Linardatos in Specht/Hennemann, Data Act/Data Governance Act, Art. 25 Rn. 6.
[239] Vgl. EG 91 zum DA.

schnell klar, dass hiermit gerade keine Schriftform i. S. d. § 126 BGB gemeint ist. Durch die Anforderung, dass der Vertrag einem Kunden vor der Vertragsunterzeichnung so bereitzustellen ist, dass dieser den Vertrag »speichern und reproduzieren«[240] kann, kann davon ausgegangen werden, dass auch elektronische Formen möglich sein müssen.

3.7.2 Inhaltliche Anforderungen

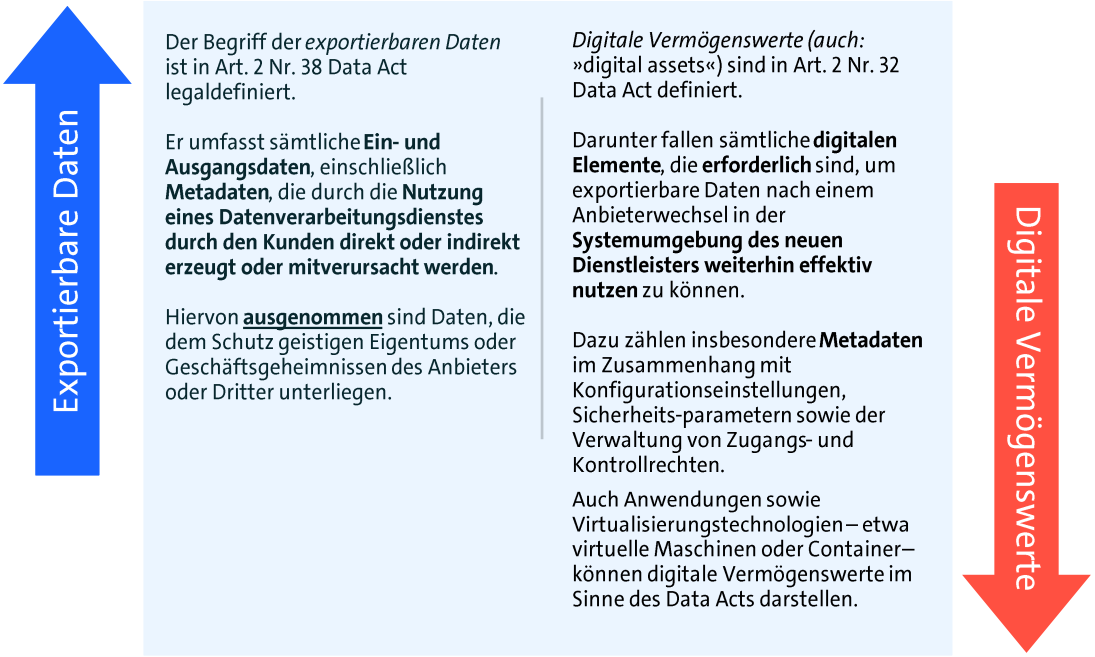
3.7.2.1 Mindestinhalt

Der Vertrag muss gemäß Art. 25 Abs. 2, 3 DA bestimmte Mindestinhalte[241] enthalten, die sicherstellen, dass ein Anbieterwechsel durch den Kunden reibungslos, wirksam, ohne unzumutbare Hürden und unter angemessener Unterstützung erfolgen kann. Das bedeutet, dass der Wechsel unverzüglich bzw. spätestens innerhalb einer vorgegebenen Frist zu erfolgen hat. Der Anbieter des Datenverarbeitungsdienstes muss hierbei dem Kunden innerhalb dieser Frist eine angemessene Unterstützung (auch in Bezug auf die Ausstiegsstrategie) unter Bereitstellung aller einschlägiger Informationen zur Verfügung stellen[242] und gleichzeitig die Kontinuität des Betriebs aufrechterhalten. Ein Formerfordernis für das Verlangen des Kunden gibt es nicht. In der Praxis wird es insbesondere darauf ankommen, dass der Kunde auch eine tatsächliche Unterstützung erhält. Ein bloßes Bemühen der Anbieter wird nicht genügen, da diese zur Herbeiführung eines konkreten (Leistungs-)Erfolgs verpflichtet sind. Flankiert wird diese (Erfolgs-)Pflicht durch den Grundsatz von Treu und Glauben gemäß Art. 27 DA. Diese Verpflichtungen aus Art. 25 DA gehen aber nicht so weit, dass der ursprüngliche Anbieter Leistungen innerhalb von fremder Infrastruktur des neuen Anbieters erbringen muss. Eine diesbezüglich reibungslose und erfolgreiche Migration kann nicht vertreten werden.[243] Ergeben sich im Rahmen des Wechselprozesses Risiken für die unterbrechungsfreie Erbringung der vertraglich geschuldeten Funktionen oder Dienste, ist der Anbieter des Datenverarbeitungsdienstes verpflichtet, den Kunden darüber zu unterrichten. Es dürften hierbei primär technische Risiken gemeint sein, die die Integrität, Verfügbarkeit, Vertraulichkeit oder Resilienz der Daten bedrohen könnten.[244] Daneben hat der Anbieter ein hohes Maß an Sicherheit zu garantieren.[245] Ebenso sind Verpflichtungen zu inkludieren, die den Anbieter zur Zurverfügungstellung zusätzlicher Informationen auffordern, die dem Kunden einen reibungslosen Anbieterwechsel unterstützen sollen. Erfasst sind hiervon insbesondere Angaben zu Kategorien von Daten und digitalen Vermögenswerten, die während des Wechselvollzugs übertragen werden können (einschließlich mindestens aller exportierbaren Daten), Informationen hinsichtlich ausgenommener Datenkategorien, wenn hierdurch die Gefahr einer Verletzung von Geschäftsgeheimnissen des Anbieters bestünde und den Löschzeitpunkt dieser Informationen.[246] Ferner muss der Vertrag potenzielle Wechselentgelte, die der Anbieter gemäß Art. 29 DA geltend machen kann,

[240] Vgl. Art. 25 Abs. 1 S. 2 DA.
[241] Vgl. Art. 25 Abs. 2 lit. a bis i, Abs. 3 DA.
[242] Vgl. Art. 25 Abs. 2 lit. b DA.
[243] Pommerening/Nickel, RDi 2024, 289.
[244] Ebenfalls: Linardatos in Specht/Hennemann, Data Act/Data Governance Act, Art. 25 Rn. 25.
[245] Vgl. Art. 25 Abs. 2 lit. a DA.
[246] Vgl. Art. 25 Abs. 2 lit. b, e, f, Abs. 4 DA.

beinhalten.

3.7.2.2 Was unterscheidet exportierbare Daten von digitalen Vermögenswerten?



Mehl, 2025.

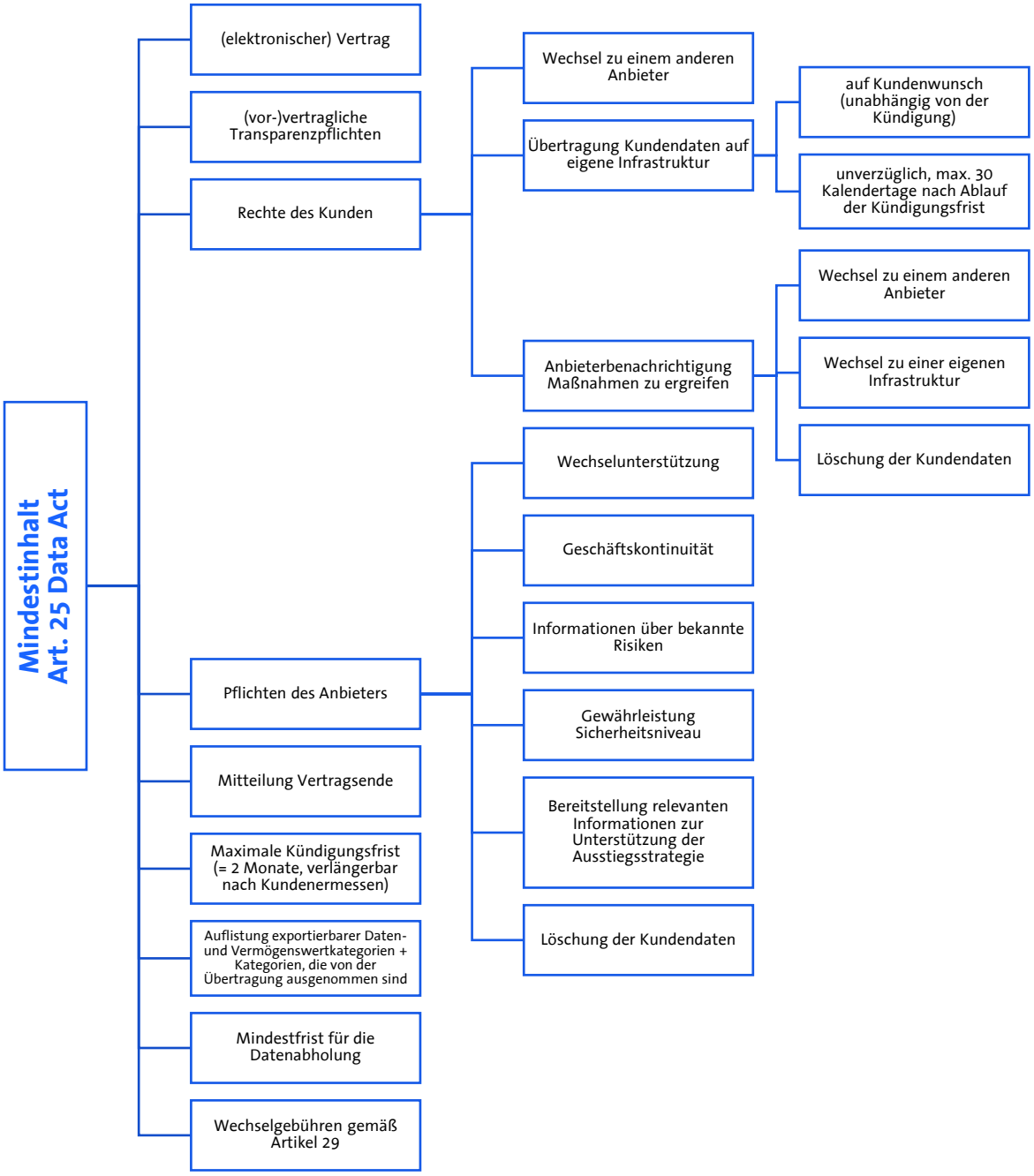
3.7.2.3 Kündigung

Der Vertrag zwischen Anbieter und Kunden muss eine Regelung enthalten, nach der das Vertragsverhältnis als beendet gilt, sobald der Wechsel erfolgreich vollzogen wurde bzw. nachdem der Kunde nach Kündigung des Dienstes die Löschung seiner Daten veranlasst hat und die vereinbarte Kündigungsfrist abgelaufen ist.[247] Zu beachten ist, dass die Einleitung eines Wechselprozesses an sich noch keine Kündigungserklärung des bestehenden Vertragsverhältnisses mit dem ursprünglichen Anbieter darstellt. Gerade dieser Mechanismus wird in der Praxis von besonderer Bedeutung sein, da diese Regelung das allgemeine Vertragsrecht stark verändert. Nach lit. c kann zwischen folgenden beiden Fallkonstellationen unterschieden werden, bei denen es keine zusätzliche Kündigungserklärung bedarf:

- Wenn der Anbieterwechsel erfolgreich abgeschlossen wurde, oder
- Wenn nach Ablauf der maximalen Kündigungsfrist[248] der Kunde seine Daten und digitalen Vermögenswerte löschen möchte.

Gemäß Option 1 gilt der Vertrag bei erfolgreichem Vollzug des Wechsels als beendet[249]. Dieser Anknüpfungspunkt für die Beendigung des Vertrages ist jedoch unvorteilhaft. Sofern das Verständnis zugrunde gelegt wird, die Kündigung erfolge erst mit erfolgreichem Wechsel, würde dies in der Praxis bedeuten, dass man von Aktionen Dritter abhängig ist, die im Zweifel nicht beeinflusst werden können. Option 2 stellt auf den Ablauf der »Kündigungsfrist«[250] ab. Hiernach gilt der Vertrag als beendet, sofern der Kunde nach Ablauf der maximalen Kündigungsfrist keinen Anbieterwechsel wünscht und stattdessen die Löschung seiner exportierbaren Daten bzw. digitalen Vermögenswerte beim bisherigen Anbieter nach Beendigung des Dienstes veranlasst. Das Recht der Vertragsparteien, die Vertragsbeziehung durch eine »ordentliche« Kündigung zu beenden, bleibt unberührt, sofern der Kündigungsgrund weder in einem Anbieterwechsel noch – aufseiten des Kunden – in einer Absicht zur Löschung von Daten liegt. Liegt ein solcher Zweck der Kündigung vor, finden die Regelungen des Art. 25 DA vorrangig Anwendung.

[247] Vgl. Art. 25 Abs. 2 lit. c DA.
[248] Art. 25 Abs. 2 lit. d DA.
[249] Art. 25 Abs. 2 lit. c i DA.
[250] Art. 25 Abs. 2 lit. c ii DA.


Mindestinhalt Art. 25 Data Act
(elektronischer) Vertrag
(vor-)vertragliche Transparenzpflichten
Rechte des Kunden
Wechsel zu einem anderen Anbieter
Übertragung Kundendaten auf eigene Infrastruktur
auf Kundenwunsch (unabhängig von der Kündigung)
unverzüglich, max. 30 Kalendertage nach Ablauf der Kündigungsfrist
Anbieterbenachrichtigung Maßnahmen zu ergreifen
Wechsel zu einem anderen Anbieter
Wechsel zu einer eigenen Infrastruktur
Löschung der Kundendaten
Pflichten des Anbieters
Wechselunterstützung
Geschäftskontinuität
Informationen über bekannte Risiken
Gewährleistung Sicherheitsniveau
Bereitstellung relevanten Informationen zur Unterstützung der Ausstiegsstrategie
Löschung der Kundendaten
Mitteilung Vertragsende
Maximale Kündigungsfrist (= 2 Monate, verlängerbar nach Kundenermessen)
Auflistung exportierbarer Daten- und Vermögenswertkategorien + Kategorien, die von der Übertragung ausgenommen sind
Mindestfrist für die Datenabholung
Wechselgebühren gemäß Artikel 29

Mehl, 2025.

3.7.2.4 Fristen

Art. 25 DA sieht vor, dass der Vertrag eine »maximale Kündigungsfrist für die Einleitung des Wechsels« beinhalten muss, die zwei Monate nicht überschreiten darf.[251] Nach Ablauf dieser Frist beginnt eine Übergangsphase von maximal 30 Kalendertagen, in der alle exportierbaren Daten und digitalen Vermögenswerte unverzüglich an den neuen Datenverarbeitungsdienst oder auf eine eigene Infrastruktur übertragen werden müssen. Mit Ablauf dieser 30 Tage muss der Wechsel zu dem übernehmenden Anbieter vollzogen sein bzw. die vorhandenen Daten auf die on-premise Instanz übertragen worden sein.[252] Da technisch komplexe Wechsel innerhalb von 30 Tagen kaum realisierbar sein dürften, sehen Art. 25 Abs. 4 und Abs. 5 DA diesbezüglich eine Einschränkung vor. Demnach kann der Anbieter des Datenverarbeitungsdienstes im Falle technischer Undurchführbarkeit einen alternativen zeitlichen Rahmen vorschlagen. Diese Information, einschließlich der Gründe für die technische Undurchführbarkeit, muss der Anbieter dem Kunden aber innerhalb von 14 Arbeitstagen nach Beantragung des Wechsels mitteilen. In diesem Fall muss der Anbieter einen alternativen Übergangszeitraum nennen, der sieben Monate nicht überschreiten darf. Die Beweislast für die Begründung der technischen Undurchführbarkeit liegt beim Anbieter.[253] Hingegen darf der Kunde die Wechselfrist gemäß Art. 25 Abs. 5 DA einmalig um einen aus seiner Sicht angemessenen Zeitraum verlängern.[254] Eine Begründungspflicht entsprechend Art. 25 Abs. 4 DA trifft jedoch ausschließlich den Anbieter; dem Kunden obliegt eine solche gerade nicht.

[251] Vgl. Art. 25 Abs. 2 lit. d DA.
[252] Vgl. Art. 25 Abs 2. lit. a DA.
[253] Vgl. EG 87 S. 4 DA.
[254] Vgl. Art. 25 Abs. 4 DA.

Zusammenfassung und Übersicht der Fristen

- Grundsätzliche Möglichkeit für Kunden, innerhalb von **maximal 30 Tagen**[206] ab Ablauf der maximalen Kündigungsfrist Daten und digitale Vermögenswerte zu übertragen
- Die maximale Kündigungsfrist für die Einleitung eines Wechsels darf **zwei Monate**[207] nicht überschreiten
- Nach dem Ablauf des vereinbarten **Übergangszeitraums**[208] ist eine Mindestfrist für den Datenabruf von **mindestens 30 Kalendertagen** zu garantieren.

Daher denkbar:

- Übergangszeit, bestehend aus
  - **2 Monaten Kündigungsfrist** für die Einleitung der Übergangsphase und
  - maximal 30 Tagen für die Datenübertragung
- und das Recht des Kunden, die Übergangsphase **einmalig** um einen für den Kunden angemesseneren Zeitraum zu verlängern

Ausnahme: Ist der o. g. Übergangszeitraum von **maximal 3 Monaten** technisch nicht realisierbar, so kann der Anbieter eine verlängerte Übergangsfrist von **maximal 7 Monaten** geltend machen. Dies muss der Anbieter dem Kunden innerhalb von **14 Arbeitstagen** nach der Beantragung des Wechsels begründen. In der Praxis wird diese verlängerte Übergangsfrist für die Mehrheit **komplexer Projekte** mit **großen Datenmengen** vertreten werden können, wenn die Datenübertragung für den Kunden

- kritisch;
- technisch, betrieblich und rechtlich komplex ist; und
- ein **umfassendes Migrationsprojekt** mit z. B. NDA, IP-Schutz, Lizenzierung/Unterlizenzierung/Übertragung von Softwarelizenzen Dritter usw. sowie vertragliche Verpflichtungen erfordert

Die maximal zulässige Gesamtumstellungszeit beträgt somit **9 Monate plus eine einmalige Verlängerung durch den Kunden** (= max. 2 Monate Kündigungsfrist + max. 7 Monate Verlängerung der Umstellungsfrist auf Antrag des Anbieters des Datenverarbeitungsdienstes und unbekannte zusätzliche Frist auf Antrag des

[255] Vgl. Art. 25 Abs. 2 lit. a DA.
[256] Vgl. Art. 25 Abs. 2 lit. d DA.
[257] Vgl. Art. 25 Abs. 2 lit. a, Abs. 4 DA.

3.7.2.5 Betriebswirtschaftliche Auswirkungen

Zu klären ist, wie genau sich ein durch den Kunden initiierter Wechselprozess auf die Vergütung gegenüber dem Anbieter des Datenverarbeitungsdienstes auswirken soll. EG 89 zum DA sagt diesbezüglich, dass »Standarddienstentgelte für die Erbringung der Datenverarbeitungsdienste selbst [...] keine Wechselentgelte (sind). Diese Standarddienstentgelte sind nicht widerrufsfähig und gelten, bis der Vertrag über die Erbringung des betreffenden Dienstes nicht mehr gilt.« Das kann dahingehend verstanden werden, dass eine Vergütung bis zum regulären Vertragsende zu zahlen ist. Art. 25 Abs. 4 S. 2 DA kann aber auch so verstanden werden, dass ab Beginn des alternativen Übergangszeitraums die originäre Vergütung nicht mehr geschuldet ist. Mithin steht es den Parteien im Sinne des EG 89 i.V.m. Art. 29 Abs. 4 DA frei, die Laufzeit und verhältnismäßige Sanktionen für eine vorzeitige Kündigung des Vertrages zu vereinbaren. Folglich ist ein Kunde grundsätzlich berechtigt, bei einem Vertrag mit fester Laufzeit die Kündigung des Vertrages auszusprechen. In solch einem Falle wäre – unabhängig von etwaigen Vereinbarungen hinsichtlich angemessener Vertragsstrafen – nach erfolgreicher Migration keine weitere Vergütung geschuldet.[258] Hierfür wäre es aber vermutlich notwendig, dass die Kontinuität aus Art. 25 Abs. 4 S. 2 DA eine einseitige Anbieterpflicht darstellt und diese nicht der originären Vergütung entgegenstehen soll.[259]

Zum gegenwärtigen Zeitpunkt steht lediglich fest, dass dieser Aspekt in der Literatur unterschiedlich beurteilt wird.[260]

[258] Pommerening/Nickel, RDi 2024, 289.
[259] Bomhard, MMR 2024, 109.
[260] So z. B. Linardatos in Specht/Hennemann, Data Act/Data Governance Act, Art. 25 Rn. 46; Bomhard, MMR 2024, 109; Schmidt-Wudy in Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Art. 25 Rn. 74.

Ausgewählte Praxistipps

- **(Vor-)Vertragliche Vereinbarungen**
  - Rechte und Pflichten in einem separaten »**Data Provision Annex**« regeln – dieser muss die Rechte und Pflichten der Parteien klar definieren
  - Die Einzelheiten zum Wechsel sollten vorrangig nach den Regelungen des Hauptvertrages gelten (= **Vorrangregelung**)
  - Der Annex sollte (technische) **Flexibilität** für unterschiedliche Anwendungsfälle, Dienste, Konfigurationen und Kunden ermöglichen. Hierdurch können Anpassungen an reale Erfahrungen und Herausforderungen ermöglicht werden
- **Transparente und detaillierte Informationen** über Datenverarbeitungsdienste und Wechsel zur Verfügung stellen bzw. einfordern
- **Verpflichtung zur angemessenen Unterstützung bei einem Wechsel**
  - Aufnahme der **Verpflichtung**, dem Kunden und vom Kunden autorisierten Dritten beim Wechselprozess (und bei der Ausstiegsstrategie des Kunden) **angemessene** Unterstützung zu gewähren
- **Beschränkung der Unterstützungsleistungen und -maßnahmen** auf **angemessene** Hilfe im Rahmen der Kapazitäten und im Verhältnis zu ihren jeweiligen Verpflichtungen, die erforderlich sind, um einen erfolgreichen, wirksamen und sicheren Wechsel zu gewährleisten
- Erwägung der **Festlegung von Bedingungen für eine gemeinsame Zielinfrastruktur**, um die **funktionale Gleichwertigkeit dieser vorab festgelegten Ziele zu erleichtern**
- Erstellen Sie **Standarddokumente** mit Details, Fähigkeiten, Dokumentation, technischem Support und Tools, um die Erreichung der funktionalen Gleichwertigkeit für eine branchenübliche Infrastruktur zu erleichtern

Im Zusammenhang mit den Wechselanforderungen des DA wird die EU-KOM verschiedene Standardvertragsklauseln (»SCC«) veröffentlichen. Die SCC dienen als Vorlage und können erste Rahmenbedingungen bieten. Sie sind klar formuliert und regeln, wer was wann tun muss. Diese Klauseln ergänzen sich größtenteils, können aber auch einzeln genutzt werden. Unternehmen können diese daher an ihre eigenen Bedürfnisse und Wechselprozesse anpassen. Die Nutzung der SCCs ist freiwillig. Im April 2025 hat eine Expertengruppe der EU-KOM einen finalen Entwurf solcher SCCs vorgelegt.[261]

[261] Expert Group on B2B data sharing and cloud computing contracts, «Final Report of the Expert Group on B2B data sharing and cloud computing contracts", 02.04.2025, zuletzt abgerufen am 27.08.2025, https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/116180/download.

3.8 Informationspflicht der Anbieter von Datenverarbeitungsdiensten (Art. 26 DA)

Lukas Mehl, Senior Data Protection Counsel, Telefónica Germany GmbH & Co. OHG

EG 84, 95 DA

Sinn und Zweck des Art. 26 DA ist es, (potenziellen) Kunden ohne Mitwirkung des Anbieters eine informierte Einschätzung der Vor- und Nachteile eines Anbieterwechsels, sowie der damit verbundenen technischen Herausforderungen zu ermöglichen. Der (potenzielle) Kunde soll somit in die Lage versetzt werden, verschiedene Anbieter von Datenverarbeitungsdiensten anhand transparenter Kriterien miteinander zu vergleichen, um auf dieser Grundlage eine fundierte Entscheidung treffen zu können. Der Adressatenkreis des Art. 26 DA ist hingegen nicht klar geregelt. In der Literatur ist streitig, ob sich die Informationspflichten des Art. 26 DA auf den bisherigen, den künftig übernehmenden oder beide Anbieter beziehen. Da Anbieter sowohl als ursprünglicher als auch als übernehmender Anbieter auftreten können, empfiehlt es sich aus Gründen der Rechtssicherheit und Risikominimierung, die Informationspflichten des Art. 26 DA beidseitig zu erfüllen – jedenfalls so lange, bis eine zuständige Behörde hierzu eine verbindliche Positionierung veröffentlicht. Die hierfür bereitgestellten Informationen müssen dabei nicht zwingend Bestandteil des Vertrags werden. Insbesondere die in EG 95 S. 1 DA genannten Angaben, sowie die Ausstiegsstrategie des Kunden, dienen der Unterstützung dieses Entscheidungsprozesses. Hierzu sollen dem (potenziellen) Kunden insbesondere folgende Informationen zur Verfügung gestellt werden:

- verfügbare Wechsel- und Übertragungsverfahren der Inhalte der Datenverarbeitungsdienste (z. B. Informationen hinsichtlich der Einleitung des Wechsels)
- verfügbare Wechsel- und Übertragungsmethoden und -formate (z. B. Informationen über offene Schnittstellen)
- technische Be- und Einschränkungen (z. B. Informationen über geschätzte Zeit, die für den Wechsel anfallen)

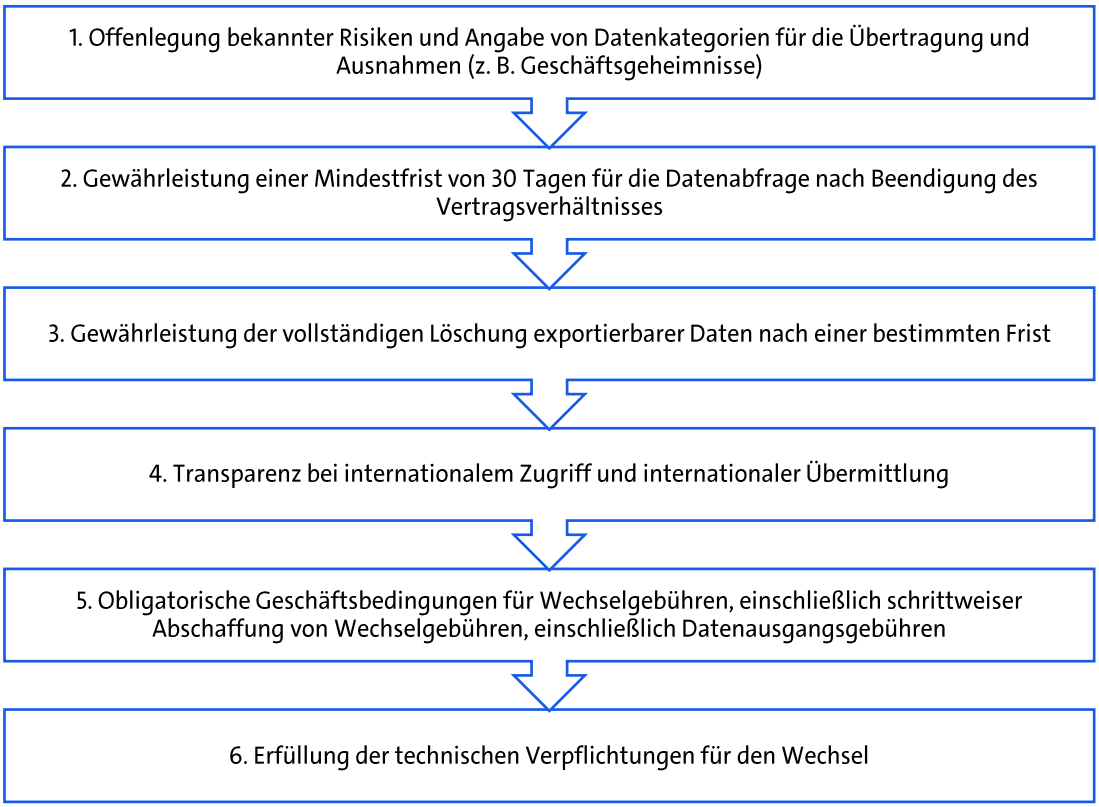
Hierdurch soll der (potenzielle) Kunde vorab in die Lage versetzt werden, vorkommerzielle, gewerbliche, technische, vertragliche und/oder organisatorische Hindernisse antizipieren zu können, um diesen im Rahmen des faktischen Wechsels zwischen den Datenverarbeitungsdiensten bzw. der Entscheidung über einen Wechsel effektiver entgegenwirken zu können. Welche Informationen für diesen Zweck bereitzustellen sind, unterliegt der autonomen Entscheidung des Anbieters. Eine Orientierungshilfe bietet insoweit lediglich EG 95 DA, dem zufolge insbesondere Informationen zur Einleitung des Anbieterwechsels, zu offenen Schnittstellen sowie zur voraussichtlichen Dauer des Wechsels bereitzustellen sind. Eine Prüfung

hinsichtlich der Vollständigkeit dieser Informationen wird für Dritte kaum möglich sein.

Daneben ist durch den Anbieter ein Online-Register mit Einzelheiten zu den Datenstrukturen bzw. Datenformaten und Hinweisen bezüglich offener Interoperabilitätsspezifikationen, in denen die exportierbaren Daten verfügbar sind, vorzuhalten. Was mit Online-Register konkret gemeint ist und welche Anforderungen ein solches Online-Register zu erfüllen hat, wird nicht näher spezifiziert. Dies wird auch mehr eine dogmatische Fragestellung bleiben. In der Praxis wird es darauf ankommen, dass eine systematische Darstellung der Informationen zur Verfügung gestellt wird. Ob dies dann im Rahmen eines Online-Registers erfolgt oder durch eine selbst verwaltete Internetdomain, bleibt dem Anbieter überlassen.

Es bleibt abzuwarten, inwiefern man mit Art. 26 DA eine »Marketing-Norm« geschaffen hat. Die Art und Weise, wie Informationen durch die Anbieter der Datenverarbeitungsdienste zur Verfügung zu stellen sind, werden nicht näher spezifiziert, Art. 26 DA verpflichtet lediglich, die Informationen bereitzustellen. Es wird nicht vorausgesetzt, dass eine aktive Übermittlung der Informationen erfolgen muss.

3.8.1 Vorschlag für einen Prozess zur Festlegung verbindlicher Vertragsbedingungen beim Wechsel (Art. 24 – 26 DA)



Mehl, 2025.

3.9 Verpflichtung zum Handeln nach Treu und Glauben (Art. 27 DA)

Lukas Mehl, Senior Data Protection Counsel, Telefónica Germany GmbH & Co. OHG

EG 85, 97 DA

Art. 27 DA definiert einen Grundsatz von Treu und Glauben, wonach Beteiligte »in good faith« bzw. nach Treu und Glauben zusammenarbeiten müssen. Dieser Grundsatz umfasst sämtliche Beteiligten und ist nicht nur auf die Parteien des Vertragsverhältnisses beschränkt. Ob ein Vertragsverhältnis vorliegt, ist für den Art. 27 DA irrelevant. Es wird lediglich darauf abgestellt, ob die Partei an dem Vorgehen beteiligt ist. Ist dies gegeben, greifen die Vorgaben hinsichtlich Treu und Glauben. Regelmäßig werden in der Praxis hierdurch der ursprüngliche und der übernehmende Anbieter des Datenverarbeitungsdienstes zusammen mit dem Kunden verpflichtet. Durch den weiten Wortlaut des Art. 27 DA können aber auch Dritte gemäß Art. 27 DA verpflichtet werden.[262] Insofern nennt EG 89 S. 1 DA ein Beispiel. Hiernach kann nach Ansicht des Gesetzgebers ein Dritter vom ursprünglichen Anbieter des Datenverarbeitungsdienstes eingeschaltet werden, damit dieser den Anbieter bei der Erfüllung der DA-Verpflichtungen unterstützt. Da Art. 27 DA nicht auf ein konkretes Vertragsverhältnis abstellt, ist davon auszugehen, dass in solch einer Konstellation auch ein mindestens mittelbares Gebot von Treu und Glauben zwischen Dritten und Kunde erwächst. Dies soll die Effektivität und Schnelligkeit im Rahmen eines Wechsels bei Beachtung einer gewissen »Mindestfairness« garantieren. EG 97 DA konkretisiert dies, indem eine »… sichere und fristgemäße Übertragung der erforderlichen Daten in einem gängigen, maschinenlesbaren Format über eine offene Schnittstelle« sicherzustellen ist.

Einen greifbaren Mehrwert durch diese Norm wird man in der Praxis aber frühestens in mehreren Jahren erleben können. Aufgrund fehlender Bestimmtheit des Wortlauts und der Notwendigkeit, Treu und Glauben europarechtskonform autonom[263] und nicht nur nach Vorgabe des § 242 BGB auszulegen, wird die Auslegung einige Rechtsunsicherheit mit sich bringen. Erst im Zusammenhang mit Urteilen des EuGH werden faktische Kriterien eine gewisse Hilfestellung liefern können.

Art. 27 DA dient im Verhältnis zu den übrigen Verordnungsnormen als Ausgleichsmechanismus zur Annäherung der (Verhandlungs-)Positionen der beteiligten Parteien. Ziel ist eine sachdienliche Zusammenarbeit, die den Anbieterwechsel möglichst effizient gestaltet und eine Verhandlungsführung auf Augenhöhe gewährleistet. Denklogisch folgt hieraus, dass eine einseitige Bevorzugung einzelner Parteien ausgeschlossen sein muss. Bei der Auslegung der Art. 23 ff. DA ist

[262] Vgl. EG 85 S.3 DA.
[263] So auch Pommerening/Nickel, RDi 2024, 289.

Art. 27 DA stets als leitende Orientierung heranzuziehen.[264] Gleichwohl erscheint es wenig realistisch, auf Grundlage von Art. 27 DA konkrete technische Maßnahmen oder vertragliche Zusagen einseitig durchsetzen zu können.

3.10 Vertragliche Transparenzpflichten in Bezug auf den Zugang und die Übermittlung im internationalen Umfeld (Art. 28 DA)

Lukas Mehl, Senior Data Protection Counsel, Telefónica Germany GmbH & Co. OHG

EG 101, 102 DA

Art. 28 Abs. 1 DA erweitert die bereits bestehenden Informationspflichten um zusätzliche vertragliche Transparenzpflichten in Bezug auf den Zugang und die Übermittlung im Zusammenhang mit internationalen Kontaktpunkten. Gemäß Art. 28 Abs. 1 lit. a und b DA sind Anbieter verpflichtet, folgende Informationen auf ihren Webseiten zur Verfügung zu stellen und aktuell zu halten:

- lit. a: die Gerichtsbarkeit, der die IKT-Infrastruktur unterliegt, die für die Datenverarbeitung der einzelnen Dienste der Anbieter errichtet wurde und
- lit. b: eine allgemeine Beschreibung der technischen, organisatorischen und vertraglichen Maßnahmen, die einen staatlichen Zugriff auf die nicht-personenbezogenen Informationen verhindern sollen, wenn dieser im Widerspruch mit dem Unionsrecht stünde.

Art. 28 DA zielt gerade nicht auf die on-premise Infrastrukturen der Kunden ab, sondern auf die Infrastruktur der Anbieter. So sind Datenverarbeitungsdienste großer Anbieter regelmäßig auf unterschiedliche Infrastrukturen aufgeteilt, was zu einer Sequenzierung der Gerichtsbarkeiten führen kann.[265] Vor diesem Hintergrund soll der Kunden zusätzliche Transparenz hinsichtlich der einschlägigen Jurisdiktionen erhalten.[266] Der Begriff der »Gerichtsbarkeit« ist dabei weit auszulegen. Eine sachgerechte Auslegung erfordert die Berücksichtigung sämtlicher staatlicher Maßnahmen und Zugriffsmöglichkeiten ausländischer Hoheitsträger – einschließlich einschlägiger Rechtsakte, Verwaltungsvorschriften, gerichtlicher Praktiken, verwaltungsbehördlicher Maßnahmen sowie Befugnismaßnahmen der Strafverfolgung.

[264] Vgl. z. B. Art. 30 Abs. 1 DA, der eine ähnliche Konstellation vorsieht.
[265] So z. B. bei Cloud-Regionen, die abhängig von der jeweiligen Einstellung und dem jeweiligen Kontinent des Kunden sind.
[266] Linardatos in Specht/Hennemann, Data Act/Data Governance Act, Art. 28 Rn. 7,8.

Praxishinweis

Nach Auffassung der EU-KOM ist das Bundesamt für Justiz die zentrale Anlaufstelle, an die sich Anbieter wenden können, wenn sie ein behördliches Ersuchen aus einem Drittstaat erhalten. Das Bundesamt soll die Anbieter dabei unterstützen, vor einer etwaigen Gewährung des Zugangs oder Übermittlung personenbezogener Daten eine rechtliche Bewertung vorzunehmen. Im Zweifelsfall kann sich ein Adressat auch an den Datenkoordinator des Mitgliedstaats wenden.[217]

Durch diese neue Transparenz wird die Nachprüfbarkeit der einzelnen Maßnahmen gemäß Art. 32 DA unterstützt. Daher sind die in Art. 28 Abs. 1 lit. a und b DA genannten Informationen aktuell zu halten. Damit diese Informationen nicht »versteckt« werden können, sind Anbieter von Datenverarbeitungsdiensten verpflichtet, die Website mit den entsprechenden Informationen in den Vertrag aufzunehmen.

Art. 28 DA liest sich wie das nicht-personenbezogene Pendant zu den datenschutzrechtlichen Vorgaben des Kapitel V der DSGVO und den Anforderungen zu Schrems-II[268]. Vor diesem Hintergrund ist auch die Einschränkung des sachlichen Anwendungsbereichs von Art. 25 Abs. 2 lit. b DA zu verstehen: Soweit personenbezogene Daten betroffen sind, müssen die eingesetzten technischen und organisatorischen Maßnahmen den Anforderungen der DSGVO entsprechen. Im Ergebnis dürften die angestrebten Schutzziele jedoch – ungeachtet der Anwendbarkeit des DA oder der DSGVO – weitgehend deckungsgleich sein. EG 101 S.3 und EG 102 S.2 DA verdeutlichen diesen Schutzgedanken gegenüber nichteuropäischen Sicherheitsbehörden. Im Sinne des EG 101 S. 5 DA sollten Anbieter – wenn möglich – den Kunden darüber in Kenntnis setzen, wenn dessen Daten von einer nichteuropäischen Behörde herausverlangt werden. Die Idee scheint darin zu liegen, dass der Kunde dann prüfen können soll, ob möglicherweise ein Rechtsverstoß gegen europäisches oder nationales Recht vorliegt.[269] Wann aber davon auszugehen ist, dass ein Begehren ausländischer (Sicherheits-) Behörden im Widerspruch mit dem Unionsrecht oder dem nationalen Recht des betreffenden Mitgliedstaats stattfindet, lässt Art. 28 DA offen. Der allgemeine Sinn und Zweck des Art. 28 DA scheint darin zu liegen, Transparenz zu schaffen, aus welchen nicht-europäischen Ländern Zugriffe auf die nicht-personenbezogenen Daten stattfinden könnten. Problematisch wird hierbei sein, dass ähnlich wie bei den personenbezogenen Daten und den Anforderungen, die aus dem Schrems-II-Urteil erwachsen sind, Unternehmen regelmäßig nicht in der Lage sein werden, die Rechtslage und eine Rechtmäßigkeitskontrolle im Drittland detailliert prüfen zu können. Zwar kann über Art. 32 Abs. 3 DA eine Quasi-Einschätzung durch die zuständige nationale Stelle oder der für die internationale Zusammenarbeit in Rechtssachen zuständigen Behörde eingeholt werden, inwieweit man einen solchen

[267] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 33, https://ec.europa.eu/newsroom/dae/redirection/document/108144.
[268] Vgl. EuGH, Urteil vom 16. Juli 2020, C-311/18.
[269] Siehe auch Art. 32 Abs. 5 DA.

Aufwand aber als gewinnorientiertes Unternehmen in Kauf nimmt, bleibt fraglich. Für die Praxis scheint es sinnvoll, die Beurteilung der Rechtsstaatlichkeit im Sinne des DA kohärent mit datenschutzrechtlichen Bewertungen nach der DSGVO zu verzahnen, um widersprüchliche Einschätzungen zur Rechtsstaatlichkeit von Drittländern zu vermeiden und damit eine weitere Verschärfung des bereits bestehenden Spannungsverhältnisses zwischen DSGVO und DA zu verhindern. Auf behördlicher Seite ist wichtig, dass empfohlene technische und organisatorische Maßnahmen zum Schutz der Inhalte im Rahmen des DA nicht von den nach der DSGVO vorgesehenen Schutzmaßnahmen abweichen.

Praxistipp

Zur Verhinderung unzulässiger Datenzugriffe durch (Aufsichts-)Behörden in Drittstaaten kann auf die allgemeinen Schutzziele der Informationssicherheit sowie auf die vom EDSA entwickelten datenschutzrechtlichen Grundsätze zu »Supplementary Measures« zurückgegriffen werden.[220] Um die Schutzgüter der (i.) Vertraulichkeit, (ii.) Verfügbarkeit und (iii.) Integrität zu gewährleisten, können insbesondere folgende Maßnahmen in Betracht gezogen werden:

- Zutrittskontrolle: Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Daten verarbeitet oder genutzt werden, zu verwehren,
- Zugangskontrolle: Verhinderung, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können
- Zugriffskontrolle: Gewährleistung, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können
- Weitergabekontrolle: Gewährleistung, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung der Daten durch Einrichtungen zur Datenübertragung vorgesehen ist,
- Eingabekontrolle: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
- Auftragskontrolle: Gewährleistung, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können,

Technische Maßnahmen umfassen sowohl software- als auch hardwarebasierte Sicherheitsvorkehrungen. In der Praxis bestehen zentrale Schutzmaßnahmen regelmäßig in der Anwendung geeigneter kryptografischer Verschlüsselungsverfahren, dem Einsatz externer Key-Management-Systeme sowie in der Implementierung wirksamer Firewall-Lösungen. Organisatorische Maßnahmen betreffen insbesondere die Durchführung interner und externer Audits, die Dokumentation von Prozessabläufen, die Schulung von Beschäftigten sowie die Ausgabe verbindlicher Arbeitsanweisungen.

3.11 Schrittweise Abschaffung von Wechselentgelten (Art. 29 DA)

Oliver Zigan, Director Contract Management, Member of the Executive Board, ITENOS GmbH

EG 88, 89 DA

[270] Vgl. EDSA, »Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", Stand 01/2020, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

3.11.1 Definitionen

> Art. 2 Nr. 36 DA: »Wechselentgelte« andere Entgelte als Standarddienstentgelte oder Sanktionen bei vorzeitiger Kündigung, die ein Anbieter von Datenverarbeitungsdiensten bei einem Kunden für die Handlungen erhebt, die in dieser Verordnung für den Wechsel zu den Systemen eines anderen Anbieters oder IKT-Infrastruktur in eigenen Räumlichkeiten vorgeschrieben sind, einschließlich Datenextraktionsentgelten;

> Art. 2 Nr. 35 DA: »Datenextraktionsentgelte« Datenübertragungsentgelte, die den Kunden dafür in Rechnung gestellt werden, dass ihre Daten über das Netz aus der IKT-Infrastruktur eines Anbieters von Datenverarbeitungsdiensten in die Systeme anderer Anbieter oder in IKT-Infrastruktur in eigenen Räumlichkeiten extrahiert werden;

Ziel der Vorschrift ist die Abschaffung von Wechselentgelten bei Datenverarbeitungsdiensten, damit ein Anbieterwechsel und der freie Datenfluss nicht behindert werden. Zudem sollen Lock-in-Effekte vermieden werden.[271]

[271] Siehe hierzu auch Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 29 Rn.2.

3.11.2 Verbot von Wechselentgelten (Art. 29 Abs. 1 DA)

(1) Ab dem 12. Januar 2027 dürfen Anbieter von Datenverarbeitungsdiensten für den Vollzug des Anbieterwechsels keine Wechselentgelte mehr erheben.

Gemäß Art. 2 Nr. 8 DA sind »Datenverarbeitungsdienste« im Sinne dieser Vorschrift »eine digitale Dienstleistung, die einem Kunden bereitgestellt wird und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen zentralisierter, verteilter oder hochgradig verteilter Art ermöglicht, die mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können.« Damit gehören insbesondere Cloud-Umgebungen zum Regelungsgegenstand (siehe insb. Abschnitt 3.1).

Unter »Anbieterwechsel« ist gem. Art 2 Nr. 34 DA letztlich der Wechsel des jetzigen Anbieters von Datenverarbeitungsdiensten zu einem anderen Anbieter gemeint, wobei es sich auch um einen Wechsel zu einer anderen Dienstart handeln kann. Im Fokus steht dabei stets die Herausgabe der Daten des Kunden.

Gem. Art. 2 Nr. 36 DA sind »Wechselentgelte« solche Entgelte, die für den vorgenannten Anbieterwechsel von dem aktuellen Anbieter berechnet werden, einschließlich »Datenextraktionsentgelte« gem. Art. 2 Nr. 35 DA. Unter letzterem sind die Entgelte zu verstehen, die ein Anbieter für die Extraktion und Übertragung der Daten des Kunden in ein System eines anderen Anbieters in Rechnung stellt.

Standarddienstentgelte selbst sind keine Wechselentgelte[272].

Nach EG 88 DA würden unangemessen hohe Wechselentgelte u. a. den Datenfluss und den Wettbewerb einschränken. Zudem wäre die freie Entscheidungsfindung des Kunden in Bezug auf einen Anbieterwechsel durch solche hohen Wechselentgelte beeinträchtigt. Aus diesem Grund »[...] sollten Wechselentgelte nach drei Jahren nach dem Tag des Inkrafttretens dieser Verordnung abgeschafft werden.«

Der Kunde soll durch diese Vorschrift allerdings gem. EG 89 DA nicht daran gehindert werden, Dritte kostenpflichtig zur Unterstützung bei Migrationsleistungen zu beauftragen.

[272] Vgl. EG 89 DA.

Außerdem kann der Kunde weitere Dienste vom Anbieter verlangen, die über solche im Zusammenhang mit dem Wechsel hinausgehen. Diese weiteren Dienste kann der Anbieter gegenüber dem Kunden abrechnen.[273]

Allerdings ist eine Abgrenzung zu Wechselentgelten beispielsweise für den Aufwand, der möglicherweise durch notwendige Datenaufbereitungsschritte oder Zwischenspeicherungen bei einem Wechsel entsteht, schwierig.[274]

Der schrittweise Entfall von Wechselentgelten gilt gem. Art. 31 Abs. 1 DA nicht für Verträge über Datenverarbeitungsdienste, bei denen die Funktionen oder Komponenten auf die spezifischen Anforderungen eines Kunden zugeschnitten werden, z. B. für dedizierte Private-Cloud-Systeme, soweit diese die Tatbestandsmerkmale des Art. 2 Nr. 8 DA erfüllen (z.B. Skalierbarkeit, s. auch Abschnitt 3.1.4; soweit eine Private-Cloud auf dedizierter Hardware bereitgestellt wird, dürfte der Anwendungsbereich des DA nicht eröffnet sein[275]). Dies sind Systeme, die auf Kundenwunsch mit aufwendig abgestimmten Parametern exklusiv und maßgeschneidert für den jeweiligen Kunden aufgebaut werden. Siehe hierzu auch Abschnitt 3.13.1.

Diese Verträge werden in der Regel mit langen Laufzeiten abgeschlossen, damit der Anbieter dieses Modell wirtschaftlich sinnvoll anbieten kann (Amortisation der Investitionen). Art. 25 DA räumt dem Kunden allerdings auch für diesen Fall eine zu jedem Zeitpunkt – unabhängig von der Vertragslaufzeit – kurze Kündigungsmöglichkeit ein. In EG 89 DA wird in diesem Zusammenhang darauf hingewiesen, dass die Verordnung die Parteien nicht daran hindern solle, Verträge mit fester Laufzeit zu vereinbaren, einschließlich verhältnismäßiger Sanktionen bei vorzeitiger Kündigung. Der Verweis auf die sog. »Sanktionen« ist in Art. 29 Abs. 4 DA zu finden. »Sanktionen« stellen hierbei kein Wechselentgelt i.S.v. Art. 29 Abs. 1 DA dar. Art. 29 Abs. 4 DA gilt direkt für Cloud-Systeme, die nicht überwiegend auf die spezifischen Belange eines Kunden zugeschnitten werden. Die Vorschrift dürfte sachlogisch analog anzuwenden sein, wenn es sich um dedizierte Systeme handelt.

Der unglückliche Rückgriff auf »Sanktionsmöglichkeit« überzeugt jedoch nicht. Die vorgegebene, jederzeitige Kündigungsmöglichkeit des Kunden stellt einen Eingriff in die Vertragsfreiheit dar, welcher insbesondere den Anbieter von dedizierten Systemen (»Private-Cloud«, s.o.) vor Herausforderungen stellt. Letzterer kann seine Investitionen im Kontext der kurzen Kündigungsmöglichkeit mittels »Sanktionen« absichern, wobei diese »Sanktionen« gem. EG 89 DA »verhältnismäßig« sein müssen. Der Anbieter trägt hierbei somit ein erhebliches Kalkulationsrisiko.

[273] Vgl. Ehlen/Fritz/Blum, Cloud-Switching unter dem Data Act: Kostenloser Wechsel in jedem Fall?, CR 3/2025, S. 141ff.
[274] Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 29 Rn. 14f.
[275] Pommerening/Nickel, RDI 2024, 289 Rn. 12f.

3.11.3 Übergangszeitraum (Art. 29 Abs. 2 DA)

(2) Vom 11. Januar 2024 bis zum 12. Januar 2027 dürfen Anbieter von Datenverarbeitungsdiensten bei den Kunden für den Vollzug des Wechsels ermäßigte Wechselentgelte erheben.

(3) Die in Absatz 2 genannten ermäßigten Wechselentgelte dürfen die Kosten, die dem Anbieter von Datenverarbeitungsdiensten im unmittelbaren Zusammenhang mit dem betreffenden Wechsel entstehen, nicht übersteigen.

Im Übergangszeitraum bis zum 12.01.2027 dürfen Anbieter ermäßigte Wechselentgelte erheben, soweit sie gem. Art 29 Abs. 3 DA nicht die tatsächlichen Wechselkosten des Anbieters überschreiten. Dies sollte vom Gesetzgeber ein Entgegenkommen gegenüber KMU sein, um sich auf die neuen Modelle auch kalkulatorisch einzustellen.

3.11.4 Informationspflichten (Art. 29 Abs. 4 – 6 DA)

(4) Vor dem Abschluss eines Vertrags mit einem Kunden unterrichten Anbieter von Datenverarbeitungsdiensten den potenziellen Kunden eindeutig über die möglicherweise erhobenen Standarddienstentgelte und die bei vorzeitiger Kündigung möglicherweise auferlegten Sanktionen sowie über die ermäßigten Wechselentgelte, die während des in Absatz 2 genannten Zeitrahmens erhoben werden könnten.

Dem Anbieter werden mit dieser Regelung Informationspflichten hinsichtlich der erhobenen Standarddienstentgelte, Sanktionen bei vorzeitiger Kündigung und Wechselentgelte für den Übergangszeitraum auferlegt. Diese Regelung impliziert, dass bei einer vorzeitigen Kündigung »Sanktionen« erhoben werden dürfen. Verträge mit fester Laufzeit sollen von der Verordnung eben nicht verhindert werden (EG 89, s.o.). Eine vorzeitige Kündigung kann dann mit verhältnismäßigen »Sanktionen« belegt werden.

Diese (analoge Anwendung der) Regelung ist insbesondere für Anbieter bedeutsam, die z. B. eine dedizierte Private-Cloud-Umgebung für Kunden anbieten, welches in der Regel mit erheblichen Investitionen verbunden ist (s.o.). Um hier Planungssicherheit hinsichtlich der aufgewandten Investitionen zu erlangen, kann eine Laufzeitsicherheit bzw. eine Absicherung mittels »Sanktionen« notwendig sein.

Die Informationen über die in Art. 29 Abs. 4 DA aufgeführten Punkte sind dem potenziellen Kunden vor Vertragsschluss aktiv in eindeutiger Form zu übermitteln. Es handelt sich somit um vorvertragliche Pflichten des Anbieters.[276]

(5) Gegebenenfalls stellen Anbieter von Datenverarbeitungsdiensten einem Kunden Informationen über Datenverarbeitungsdienste bereit, durch die der Wechsel sehr kompliziert oder kostspielig wird oder ohne nennenswerte Eingriffe in die Daten, digitalen Vermögenswerte oder die Dienstarchitektur unmöglich ist.

Anlass- bzw. anbieterbezogen soll der Anbieter dem Kunden Informationen über Dienste bereitstellen, soweit durch diese Dienste ein Wechsel sehr kompliziert oder kostspielig wird. Gleiches gilt, wenn bei einem Wechsel nennenswerte Eingriffe in die Daten, digitalen Vermögenswerte oder die Dienstarchitektur notwendig werden. Diese Regelung dürfte bei Standard-Cloud-Leistungen regelmäßig nicht einschlägig sein.

(6) Anbieter von Datenverarbeitungsdiensten veröffentlichen die in den Absätzen 4 und 5 genannten Informationen für Kunden gegebenenfalls auf einem gesonderten Abschnitt ihrer Website oder auf eine andere leicht zugängliche Weise.

[276] Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 29 Rn. 24f.

Hierbei handelt es sich um keine zwingende Vorgabe. Anbieter könnten allerdings gerade allgemeingültige Informationen auf diese (für den Anbieter einfacheren) Weise zugänglich machen.

3.11.5 Marktüberwachung (Art. 29 Abs. 7 DA)

Rainer Duda, Lead of Competence Center Data & AI, M&M Software GmbH

> (7) Der Kommission wird die Befugnis übertragen, gemäß Artikel 45 delegierte Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, indem ein Überwachungsmechanismus eingerichtet wird, mit dem die Kommission die von Anbietern von Datenverarbeitungsdiensten auf dem Markt verlangten Wechselentgelte überwachen kann, um sicherzustellen, dass die Wechselentgelte gemäß den Absätzen 1 und 2 des vorliegenden Artikels innerhalb der in diesen Absätzen festgelegten Fristen abgeschafft und verringert werden.

Die EU-KOM ist gemäß Art. 29 Abs. 7 DA dazu befugt, zusätzliche detaillierte Regelungen in Form von delegierten Rechtsakten zu erlassen, um ein formelles Kontrollsystem einzuführen.

Dieser Überwachungsmechanismus würde wohl regelmäßig Daten darüber sammeln, welche Wechselentgelte Anbieter tatsächlich verlangen, prüfen, ob diese Entgelte den gesetzlichen Vorgaben entsprechen (Reduktion nur auf tatsächliche Kosten im Übergangszeitraum, vollständige Abschaffung ab 12. Januar 2027), Abweichungen oder Verstöße identifizieren und so eine Grundlage für rechtliche oder regulatorische Maßnahmen schaffen.

Das bedeutet, dass Anbieter damit rechnen müssen, dass ihre Preisgestaltung für den Anbieterwechsel von der EU überwacht wird. Bei zu hohen oder nicht fristgerecht reduzierten Entgelten müssen sie mit Sanktionen rechnen. Art. 29 DA enthält keine eigenen Bestimmungen zu Strafen oder Bußgeldern bei Nichteinhaltung seiner Vorgaben. Die Durchsetzung erfolgt auf Grundlage von Art. 40 DA, der die EU-Mitgliedstaaten verpflichtet, wirksame, verhältnismäßige und abschreckende Sanktionen für Verstöße gegen den DA festzulegen. Sollte die EU-KOM im Rahmen des vorgesehenen Überwachungsmechanismus Verstöße feststellen, könnten zuständige nationale Behörden des jeweiligen EU-Mitgliedstaats geeignete Maßnahmen ergreifen.

3.12 Technische Aspekte des Wechsels (Art. 30 DA)

Luisa Nissen, Rechtsreferendarin, Bitkom e.V.

EG 86, 90, 92 DA

Art. 30 DA gewährleistet die Schnelligkeit und Leichtigkeit eines Wechsels. Indem dessen technische Anforderungen definiert werden, werden die Hürden zwischen den jeweiligen Anbietern abgebaut und die technischen Gegebenheiten so weit wie möglich harmonisiert, wobei die Pflichten abhängig vom jeweiligen Leistungsumfang variieren.[277] Ziel ist es, beim übernehmenden Anbieter einen (möglichst) äquivalenten Betrieb der bereits vorhandenen Datenverarbeitung zu gewährleisten.

Während sich Art. 30 Abs. 1 DA an den Anbieter von IaaS richtet, legen Art. 30 Abs. 2–4 DA die technischen Bedingungen für alle übrigen Anbieter von Datenverarbeitungsdiensten, insbesondere PaaS, SaaS und XaaS fest. Bringt eine Bereitstellung der Daten Gefahren für die Sicherheit des Systems oder den Schutz der Kundendaten mit sich, kann der Anbieter die Bereitstellung verweigern, Art. 30 Abs. 6 DA.

Sofern die Anbieter ihren Pflichten nach Art. 30 DA nicht nachkommen, kommen neben vertraglichen Durchsetzungsansprüchen auch Schadensersatzansprüche nach §§ 280 ff. BGB in Betracht, sofern dem Kunden ein kausaler Schaden entstanden ist.

3.12.1 IaaS (Art. 30 Abs. 1 DA)

Art. 30 Abs. 1 DA richtet sich an den Anbieter von IaaS und legt für diesen die strengsten Anforderungen fest. Denn dieser hat proaktiv für die Herstellung von sog. Funktionsäquivalenz zu sorgen.

3.12.2 PaaS/SaaS/XaaS (Art. 30 Abs. 2 ff. DA)

Die Anbieter von Datenverarbeitungsdiensten, die nicht bereits unter Art. 30 Abs. 1 DA fallen – insbesondere namentlich die Anbieter von PaaS, SaaS und XaaS – müssen nur offene Schnittstellen zum Datenexport und -transfer bereitstellen (APIs).

Die Web-APIs müssen nur für die Kunden, Entwickler und den übernehmenden Anbieter öffentlich zugänglich sein, jedoch nicht für die Allgemeinheit.[278]

[277] So auch Linardatos in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 30 Rn. 5f.
[278] Linardatos in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 30 Rn. 25; kritisch: Leistner/Antoine, IPR and the use of open data and data sharing initiative by public and private actors, 2022, S. 114.

Datensicherheit sollte durch Authentifizierung und Autorisierung sichergestellt werden. Die Schnittstellen müssen ausreichende Informationen über den Dienst beinhalten, damit die erforderlichen technischen Maßnahmen (z. B. Softwareentwicklung) getroffen werden können, um die Datenübertragung und Interoperabilität zu gewährleisten, Art. 30 Abs. 2 DA.[279] Eine Entwicklungspflicht trifft dabei jedoch nur die übernehmenden Anbieter.[280] Die Schnittstellen müssen unentgeltlich zur Verfügung gestellt werden.

Nach Art. 30 Abs. 3 DA muss der ursprüngliche Anbieter die Kompatibilität mit gemeinsamen Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen[281] oder harmonisierter Interoperabilitätsnormen[282] gewährleisten. Solange diese Spezifikationen und Normen nach Art. 35 Abs. 8 DA noch nicht veröffentlicht sind, muss der ursprüngliche Anbieter die Daten nach Art. 35 Abs. 5 DA in einem strukturierten, gängigen und maschinenlesbaren Format bereitstellen, Art. 30 Abs. 5 DA.

Art. 35 Abs. 4 DA verpflichtet den ursprünglichen Anbieter darüber hinaus, das nach Art. 26 lit. b DA zu führende Online-Register stetig zu aktualisieren.

3.12.3 Funktionsäquivalenz

Kernelement des Art. 30 Abs. 1 DA ist die sog. Funktionsäquivalenz. Diese hat der Anbieter von IaaS bei der Nutzung des übernehmenden Datenverarbeitungsdienstes nach Wechsel des Kunden sicherzustellen, indem er alle ihm zur Verfügung stehenden angemessenen Maßnahmen ergreift. Eine Definition der Funktionsäquivalenz findet sich in Art. 2 Nr. 37 DA. Gemeint ist »die Wiederherstellung [...] eines Mindestmaßes an Funktionalität in der Umgebung eines neuen Datenverarbeitungsdienstes gleicher Dienstart nach dem Wechsel«. Wann das Mindestmaß an Funktionsäquivalenz erreicht wird, bleibt hingegen offen. Allerdings stellt EG 86 klar, dass von Anbietern von Datenverarbeitungsdiensten nur erwartet werden kann, dass sie die Funktionsäquivalenz in Bezug auf die Funktionen ermöglichen, die sowohl vom ursprünglichen als auch vom übernehmenden Datenverarbeitungsdienst unabhängig voneinander angeboten werden. Die Eingabe der Kundendaten soll deshalb beim übernehmenden Anbieter zum gleichen Ergebnis führen, wie die Eingabe beim ursprünglichen Anbieter.

Die vom ursprünglichen Anbieter geschuldeten Unterstützungsmaßnahmen umfassen insbesondere technische und personelle Kapazitäten sowie das Bereitstellen von Informationen und Dokumentationsmaterial.[283]

Berechtigter ist der Kunde selbst, wobei es wohl zulässig sein dürfte, dass dieser dem ursprünglichen Anbieter eine Weisung erteilt, die exportierten Daten unmittelbar an den übernehmenden Anbieter weiterzuleiten.

[279] Pommerening/Nickel, RDi 2024, 289 Rn. 26.
[280] Linardatos in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 30 Rn. 25.
[281] Art. 2 Nr. 42 DA.
[282] Art. 2 Nr. 41, 43 DA.
[283] Im Einzelnen: Linardatos in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 30 Rn. 16ff.

3.12.4 Zumutbarkeitsgrenze (Art. 30 Abs. 6 DA)

Die den Anbietern von Datenverarbeitungsdiensten in Art. 30 Abs. 1–5 DA auferlegten Pflichten stehen nach Art. 30 Abs. 6 DA stets unter dem Vorbehalt der Zumutbarkeit. Anbieter von Datenverarbeitungsdiensten sind deshalb nicht verpflichtet, neue Technologien oder Dienste zu entwickeln. Auch digitale Vermögenswerte[284], die durch Rechte des geistigen Eigentums geschützt sind oder ein Geschäftsgeheimnis darstellen, müssen nicht gegenüber Kunden oder dem übernehmenden Anbieter offengelegt werden. Wenn die Offenlegung die Sicherheit und Integrität des ursprünglichen Anbieters des Datenverarbeitungsdienstes oder des Kunden beeinträchtigen würde, darf der ursprüngliche Anbieter auch die Offenbarung dieser digitalen Vermögenswerte verweigern.

Dabei kann sich der ursprüngliche Anbieter aber nicht mit einem pauschalen Hinweis auf Sicherheitsbedenken seinen Pflichten zur Unterstützung des Wechsels entziehen. Im Hinblick auf die von Art. 23 ff. DA gewährleistete Wechseleffektivität kommt dieser im Rahmen einer Interessenabwägung erhebliches Gewicht zu. In dem Herrschaftsbereich des ursprünglichen Anbieters obliegt es diesem deshalb, alle erforderlichen Schutzmaßnahmen zu ergreifen, um die Sicherheit und Integrität seines Systems zu gewährleisten und einen Wechsel zu ermöglichen.[285]

Daneben sind auch die Sicherheitsinteressen des Kunden zu berücksichtigen. Insbesondere dürfen beim Wechselvorgang keine Daten des Kunden gefährdet werden.

Sofern der Kunde Durchsetzungs- oder Schadensersatzansprüche geltend macht, stellt Art. 30 Abs. 6 DA eine Einwendung dar.

3.13 Ausnahmen für bestimmte DVD (Art. 31 DA)

Rainer Duda, Lead of Competence Center Data & AI, M&M Software GmbH | David Schönwerth, Bereichsleiter Data Economy, Bitkom e.V.

> EG 98 DA

In Art. 31 DA werden für einzelne DVDs Ausnahmen von Verpflichtungen festgelegt.

[284] Art. 2 Nr. 32 DA.
[285] Schmit-Wudy in: BeckOK DatenschutzR, 52. Edition, Stand 01.05.2025; DA Art. 30 Rn. 40; Linardatos in: Specht/Hennemann, Data Act/Data Governance Act, 2. Auflage 2025, Art. 30 Rn. 38.

3.13.1 Ausnahmen für maßgeschneiderte DVDs (Art. 31 Abs. 1 DA)

Gemäß Art. 31 Abs. 1 DA sind »für Datenverarbeitungsdienste, bei denen [A] die meisten zentralen Funktionen auf die spezifischen Bedürfnisse eines einzelnen Kunden zugeschnitten wurden, oder [B] wenn alle Komponenten für die Zwecke eines einzelnen Kunden entwickelt wurden und [C] wenn diese Datenverarbeitungsdienste nicht im größeren kommerziellen Maßstab über den Dienstleistungskatalog der Anbieter von Datenverarbeitungsdiensten angeboten werden« die Pflichten aus Art. 23 lit. d, Art. 29, Art. 30 Abs. 1, 3 DA nicht anwendbar.

Die Wiederholung von Datenverarbeitungsdiensten an der Stelle [C] »wenn diese Datenverarbeitungsdienste nicht im kommerziellen Maßstab« deutet darauf hin, dass die Tatbestandsmerkmale [A] und [B] alternativ und das Tatbestandsmerkmal [C] kumulativ vorliegen müssen, folglich ([A] und/oder [B]) und [C].

Hilfreich ist hierbei auch ein Blick auf die englische Sprachversion von Art. 31 Abs. 1 DA: »[...] shall not apply to data processing services of which the majority of main features has been custom-built to accommodate the specific needs of an individual customer or where all components have been developed for the purposes of an individual customer, and where those data processing services are not offered at broad commercial scale via the service catalogue of the provider of data processing services.«

3.13.2 Vollausnahme für zeitlich begrenzt bereitgestellte DVDs für Test- und Bewertungszwecke (Art. 31 Abs. 2 DA)

Art. 31 Abs. 2 DA nimmt DVDs aus den Pflichten aus Kapitel 6 aus, »die nicht als Vollversion, sondern zu Test- und Bewertungszwecken und für einen begrenzten Zeitraum bereitgestellt werden«.

3.13.3 Vorvertragliche Informationspflicht (Art. 31 Abs. 3 DA)

Sowohl in den Fällen von Art. 31 Abs. 1 als auch Abs. 2 DA muss der Anbieter den Kunden vor Vertragsabschluss über die nicht anwendbaren Pflichten informieren.

3.14 Parallele Nutzung von DVDs (Art. 34 DA)

EG 99 DA

Artikel 34 legt dar, dass einzelne Anforderungen aus den Art. 23 ff. DA für den Zweck der parallelen Nutzung von DVDs anwendbar sind und welche Datenextraktions-entgelte im Fall der parallelen Nutzung von DVDs erhoben werden dürfen.

3.14.1 Anwendbare Pflichten

Folgende Pflichten sind gemäß Art. 34 Abs. 1 DA nicht nur für einen Wechsel zwischen DVDs (siehe Abschnitt 3.5.2), sondern auch zum Zweck der parallelen Nutzung von DVDs anwendbar:

Norm	Grobe Beschreibung	Abschnitt im Leitfaden
Art. 23 DA	Generalklausel	3.5
Art. 24 DA	Tragweite der technischen Verpflichtungen	3.6
Art. 25 Abs. 2 lit. a ii) DA	Sorgfaltspflicht, Kontinuität des Geschäftsbetriebs, Fortsetzung der Erbringung der vertraglichen Leistungen	3.7.2
Art. 25 Abs. 2 lit. a iv) DA	Sicherheitsanforderungen	
Art. 25 Abs. 2 lit. e DA	Auflistung aller Kategorien von Daten und digitalen Vermögenswerten	
Art. 25 Abs. 2 lit. f DA	Liste aller Datenkategorien, die nicht exportiert werden	
Art. 30 Abs. 2 DA	Bereitstellung offener Schnittstellen (PaaS/SaaS/XaaS) mit ausreichenden Informationen	3.12.2
Art. 30 Abs. 3 DA	Verpflichtung zur Kompatibilität mit hEN und gemeinsamen Spezifikationen auf Basis von Art. 35 DA (PaaS/SaaS/XaaS)	
Art. 30 Abs. 4 DA	Aktualisierung des Online-Registers gemäß Art. 26 lit. b DA (PaaS/SaaS/XaaS)	
Art. 30 Abs. 5 DA	Export aller exportierbaren Daten falls keine hEN oder	

Norm	Grobe Beschreibung	Abschnitt im Leitfaden
	gemeinsamen Spezifikationen veröffentlicht wurden	

3.14.2 Kostenweitergabe

Gemäß Art. 34 Abs. 2 DA dürfen bei der parallelen Nutzung von DVDs seitens der Anbieter Datenextraktionsentgelte verlangt werden, die jedoch auf die Höhe der entstandenen Extraktionskosten limitiert sind.

3.15 Interoperabilität von Datenverarbeitungsdiensten (Art. 35 DA)

Volker Smoljko, Technical Relations Executive, IBM Deutschland Research & Development GmbH | David Schönwerth, Bereichsleiter Data Economy, Bitkom e.V.

EG 100 DA

Art. 2 Nr. 41 DA: »offene Interoperabilitätsspezifikationen« eine technische Spezifikation im Bereich der Informations- und Kommunikationstechnologie, die leistungsbezogen darauf ausgerichtet sind, die Interoperabilität zwischen Datenverarbeitungsdiensten herzustellen;

Art. 2 Nr. 42 DA: »gemeinsame Spezifikationen« ein Dokument, bei dem es sich nicht um eine Norm handelt und das technische Lösungen enthält, die es ermöglichen, bestimmte Anforderungen und Pflichten, die im Rahmen dieser Verordnung festgelegt worden sind, zu erfüllen;

Art. 2. Nr. 43 DA: »harmonisierte Norm« eine harmonisierte Norm im Sinne des Artikels 2 Nummer 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012;

3.15.1 Wesentliche Anforderungen (Art. 35 Abs. 1, 2 DA)

Die wesentlichen gesetzlichen Anforderungen an offene Interoperabilitätsspezifikationen und harmonisierte Normen, so wie sie in Art. 30 DA beschrieben sind, finden sich in Art. 35 Abs. 1 sowie 2 DA.

Hervorzuheben ist die leicht abgeschwächte Formulierung für die Umsetzung der Anforderungen in der englischen Sprachfassung: Art. 35 Abs. 1 DA nutzt »...shall...« während Art. 35 Abs. 2 DA »shall adequately address« nutzt.

In der deutschen Sprachfassung wiederum werden in Art. 35 Abs. 1 DA imperative Formulierungen verwendet (...bewirken...; ...erleichtern...), während Art. 35 Abs. 2 DA

eine abgeschwächte Formulierung dessen nutzt (... müssen Folgendes angemessen regeln...).

»(1) Offene Interoperabilitätsspezifikationen und harmonisierte Normen für die Interoperabilität von Datenverarbeitungsdiensten

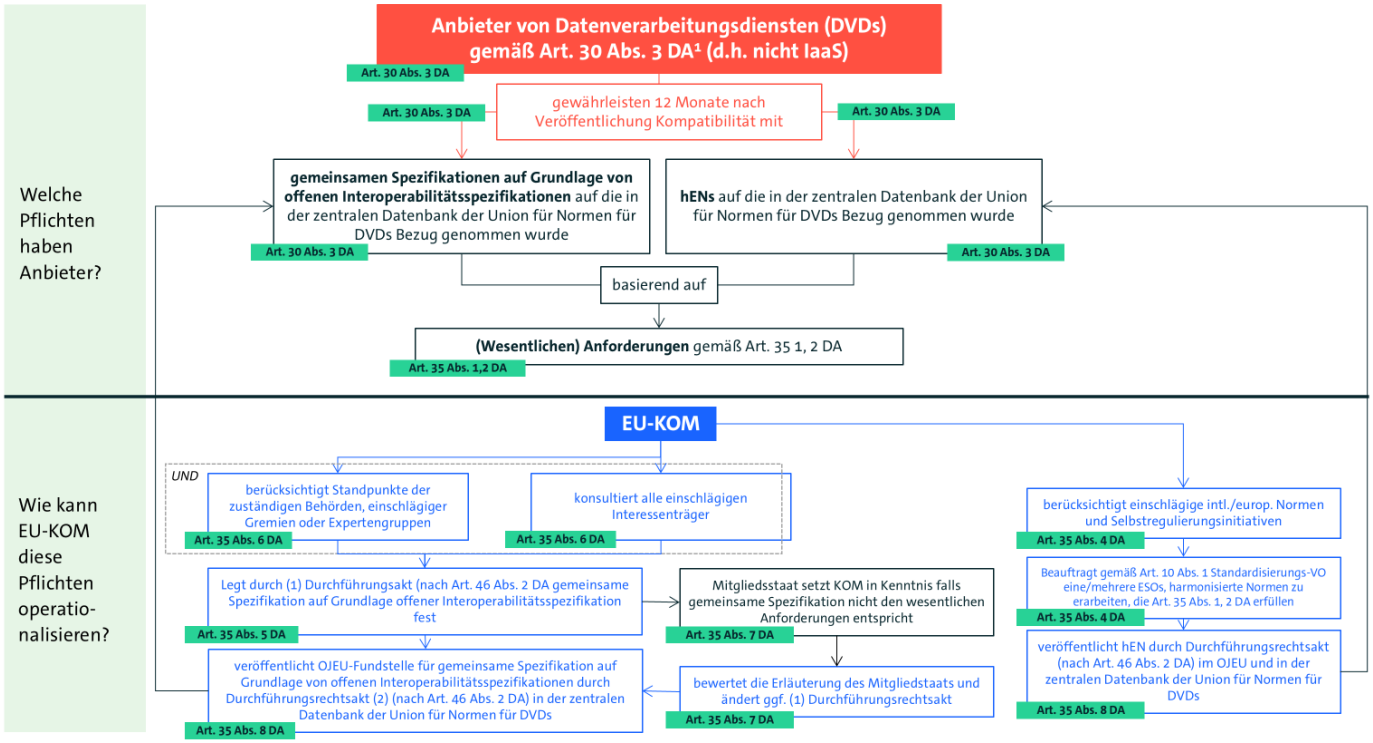
a) bewirken, soweit dies technisch machbar ist, die Interoperabilität zwischen verschiedenen Datenverarbeitungsdiensten, die die gleiche Dienstart abdecken;

b) verbessern die Übertragbarkeit digitaler Vermögenswerte zwischen verschiedenen Datenverarbeitungsdiensten, die die gleiche Dienstart abdecken;

c) erleichtern, soweit dies technisch machbar ist, die Funktionsäquivalenz zwischen den in Artikel 30 Absatz 1 genannten Datenverarbeitungsdiensten, die die gleiche Dienstart abdecken;

d) beeinträchtigen Sicherheit und Integrität der Datenverarbeitungsdienste und Daten nicht;

e) sind für die Möglichkeit einer technischen Aufrüstung und die Einbindung neuer Funktionen und Innovationen in Datenverarbeitungsdiensten ausgelegt.«



[1] » Bei anderen als den in Absatz 1 des vorliegenden Artikels genannten Datenverarbeitungsdiensten [Abs. 1: » Was Datenverarbeitungsdienste für skalierbare und elastische Rechenressourcen betrifft, die auf Infrastrukturelemente wie Server, Netze und die für den Betrieb der Infrastruktur erforderlichen virtuellen Ressourcen beschränkt sind, aber keinen Zugang zu den Betriebsdiensten, zur Software und zu den Anwendungen gewähren, die auf diesen Infrastrukturelementen gespeichert sind, anderweitig verarbeitet oder eingesetzt werden […] «], gewährleisten Anbieter von Datenverarbeitungsdiensten die Kompatibilität mit […] « (Art. 30 Abs. 3 DA).

Bitkom, 2025.

3.15.2 Möglichkeit 1: hEN via SSOs

Gemäß Art. 35 Abs. 4 DA kann die EU-KOM nach Berücksichtigung relevanter internationaler und Europäischer Normen und ‚selbstregulierender' Initiativen, nach Art. 10 Abs. 1 Standardisierungs-Verordnung (**Standardisierungs-VO**)[286] eine oder mehrere Europäische Standardisierungs-Organisationen (ESOs) mittels eines Standardisation Request den Auftrag zur Erstellung einer ‚Draft' harmonisierten Norm erteilen, die die aufgeführten ‚essential requirements', die in Art. 35 Abs. 1, 2 DA beschrieben sind, erfüllen.

Gemäß Art. 35 Abs. 8 DA müssen die Fundstellen solcher hENs wiederum nach Fertigstellung der hEN, um dann unter Art. 30 Abs. 3 DA anwendbar zu sein, per Durchführungsrechtsakt veröffentlicht werden.

Gemäß Art. 35 Abs. 9 DA ist für den Erlass eines solchen Durchführungsrechteakts ein sog. Komitologieverfahren nach Art. 46 Abs. 2 DA i.V.m. Art. 5 der Ausschussverfahrensverordnung[287] durchzuführen, welches unter Umständen die Möglichkeit der Ablehnung des Durchführungsrechtsaktes vorsieht.

[286] ABl. L 316, 1025/2012, 14.11.2012, S. 12ff.
[287] ABl. L 55, 182/2011, 28.2.2011, S. 13ff.

3.15.3 Möglichkeit 2: Gemeinsame Spezifikationen außerhalb SSOs (Art. 35 Abs. 5 ff. DA)

Gemäß Art. 35 Abs. 5 DA kann die EU-KOM neben dem Pfad über die formale Standardisierung über einen Durchführungsrechtsakt[288] gemeinsame Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen erlassen, die die Anforderungen aus Art. 35 Abs. 1, 2 DA abdecken[289].

3.15.4 Anforderungen

Gemäß Art. 35 Abs. 3 DA müssen offene Interoperabilitätsspezifikationen für eine Anerkennung alle Anforderungen des Annex II der Standardisierungs-VO erfüllen. Dazu zählt insbesondere, dass diese

- Marktakzeptanz erreicht haben (Annex II Abs. 1 Standardisierungs-VO)
- Nicht im Widerspruch zu europäischen Normen stehen (Annex II Abs. 2 Standardisierungs-VO)
- Von einer gemeinnützigen Organisation erarbeitet wurden (Annex II Abs. 3 Standardisierungs-VO)
- in Verfahren entwickelt wurden, die (Annex II Abs. 3 Standardisierungs-VO)
  - offen,
  - konsensbasiert und
  - transparent sind
- folgende Anforderungen erfüllen bzgl. (Annex II Abs. 4 Standardisierungs-VO)
  - Pflege
  - Verfügbarkeit
  - Lizenzierung
  - Relevanz
  - Neutralität und Stabilität
  - Qualität.

[288] Vgl. Erklärung von Delegierten Rechtsakten und Durchführungsrechtsakten, EU-KOM, »Durchführungsrechtsakte und delegierte Rechtsakte«, zuletzt abgerufen am, 27.07.2025, https://commission.europa.eu/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts_de.
[289] Art. 35 Abs. 5 DA.

3.15.5 Verabschiedung

Dabei sind gemäß Art. 35 Abs. 6 DA u.a. die unter Art. 37 Abs. 5 lit. h DA genannten einschlägigen zuständigen Behörden sowie bestimmte andere Stakeholder zu beteiligen, was denen jedoch keine Vetorechte oder Vergleichbares zubilligt.

EU-Mitgliedsstaaten können dahingehend gemäß Art. 35 Abs. 7 DA gegenüber der EU-KOM äußern, dass die gesetzlichen Anforderungen in Art. 35 Abs. 1, 2 DA mit den angezeigten Spezifikationen und hENs nicht ausreichend abgedeckt würden. In diesem Fall muss die EU-KOM die Details zu Erläuterung entsprechend untersuchen und kann den betroffenen Durchführungsrechtsakt entsprechend anpassen.

Für den Erlass eines solchen Durchführungsrechteakts ist gemäß Art. 35 Abs. 8 DA ein sog. Komitologieverfahren nach Art. 46 Abs. 2 DA i.V.m. Art. 5 der Ausschussverfahrensverordnung[290] durchführen, welches unter Umständen die Möglichkeit der Ablehnung des Durchführungsrechtsaktes vorsieht.

3.15.6 Central Union Repository (Art. 35 Abs. 8)

Sowohl harmonisierte Normen (Möglichkeit 1) als auch gemeinsame Spezifikationen (Möglichkeit 2) sind in einer sog. zentralen Datenbank der Union für die Interoperabilität von Datenverarbeitungsdiensten (‚Union Standards Repository') zu veröffentlichen. Ab Veröffentlichung haben Normadressaten von Art. 30 Abs. 3 DA 12 Monate Zeit, die Kompatibilität ihrer Dienste entsprechend der veröffentlichten hEN/Spezifikationen nachzuweisen.

Das Union Standards Repository soll planmäßig im September 2025 online gehen. Es wird erwartet, dass sich das Central Union Standards Repository dadurch auszeichnet, dass es:

- Als ‚One-Stop-Shop' für Anbieter, Kunden und Systemintegratoren fungiert
- Eine Online-Plattform darstellt, die in die Website der EU-KOM integriert ist, mit entsprechenden Funktionen, z. B. Filtern
- Harmonisierte Normen (hENs), gemeinsame Spezifikationen, sowie anerkannte Industrie-Standards enthält.

[290] ABl. L 55, 182/2011, 28.2.2011, S. 13ff.

4 Internationale Datentransfers (Kapitel VII DA)

Tahir Mughal, MBA, Senior Consultant,
Enterprise Transformation, Materna SE

EG 101, 102 DA

4.1 Zielsetzung

Art. 32 DA regelt den Schutz nicht-personenbezogener Daten vor unrechtmäßigen Zugriffen durch staatliche Stellen aus Drittstaaten. Ziel ist es, die digitale Souveränität Europas zu stärken und sicherzustellen, dass Daten, die in der EU gespeichert werden, nicht ohne rechtlich saubere Grundlage an ausländische Behörden übermittelt oder durch diese abgerufen werden.

Diese Vorschriften betreffen insbesondere Anbieter von Datenverarbeitungsdiensten wie Cloud-Anbieter, Plattform-betreiber oder IoT-Dienstleister. Sie müssen geeignete Maßnahmen ergreifen, um die Anforderungen des Art. 32 DA umzusetzen. Die EG 101 und 102 DA verdeutlichen dabei die politische Zielsetzung: Der Schutz europäischer Datenräume vor ausländischen Zugriffen bedarf klarer rechtlicher Grenzen und technischer sowie organisatorischer Absicherungen.

4.1.1 Maßnahmen

Anbieter von Datenverarbeitungsdiensten müssen Maßnahmen ergreifen, um unrechtmäßigen staatlichen Zugriff auf in der EU gespeicherte, nicht-personenbezogene Daten zu verhindern, wenn dies im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats steht. Der DA sieht hierfür vier zentrale Maßnahmenkategorien vor:

4.1.1.1 Technisch

Technische Schutzmaßnahmen dienen der Absicherung der Systeme selbst. Dazu gehören etwa:

- Verschlüsselung sensibler Daten,
- Zugriffs- und Nutzerverwaltung (z. B. Multi-Faktor-Authentifizierung),
- Protokollierungen (Monitoring und Nachvollziehbarkeit von Zugriffen).

Diese Maßnahmen sollen den direkten Zugriff durch ausländische Stellen technisch unterbinden oder nachvollziehbar machen.

4.1.1.2 Organisatorisch

Hierunter fallen betriebsinterne Regeln, Prozesse und Zuständigkeiten, mit denen der Umgang mit Datenzugriffs-anfragen strukturiert wird:

- interne Freigabeprozesse und Eskalationsstufen,
- klare Verantwortlichkeiten im Unternehmen,
- Prüfmechanismen bei Anfragen aus Drittstaaten.

Ziel ist es, den operativen Umgang mit internationalen Datenanforderungen rechtskonform, kontrollierbar und wiederholbar zu gestalten.

4.1.1.3 Rechtlich

Rechtliche Absicherungen sollen durch Verträge und Vereinbarungen sicherstellen, dass Daten nicht ohne rechtmäßige Grundlage weitergegeben werden. Dies kann beispielsweise durch die Einfügung von Standardvertragsklauseln erreicht werden, die eine Weitergabe nur bei rechtmäßigen Anfragen erlauben. Zudem sollen Anbieter in der Lage sein, sich auf vertragliche Regelungen zu berufen, wenn rechtswidrige Anforderungen gestellt werden.

4.1.1.4 Angemessenheit

Alle Maßnahmen müssen verhältnismäßig und wirksam im Verhältnis zum Risiko sein. Das bedeutet, je sensibler oder wirtschaftlich bedeutender die Daten sind, desto strenger müssen die Schutzvorkehrungen sein. Eingehende Anfragen müssen auf ihre Rechtsgrundlage, Verhältnismäßigkeit und Konkretheit hin geprüft werden. Anbieter müssen dokumentieren und nachweisen können, dass ihre Maßnahmen geeignet sind, die Daten effektiv zu schützen.

4.1.2 Staatlicher Zugang

Staatlicher Zugang liegt vor, wenn Behörden aus Drittstaaten direkten Zugriff auf in der EU gespeicherte Daten verlangen, ohne dass die Daten physisch übermittelt werden. Dies kann beispielsweise durch digitale Schnittstellen oder Fernzugriffe erfolgen. Ein solcher Zugriff ist nur zulässig, wenn er auf einer gültigen internationalen Vereinbarung basiert (z. B. einem Rechtshilfeabkommen) und mit EU-Recht sowie nationalem Recht vereinbar ist. Fehlt diese Grundlage, muss der Anbieter den Zugriff verweigern.

4.1.3 Staatliche Übermittlung

Im Gegensatz zum staatlichen Zugang bezieht sich die staatliche Übermittlung auf Fälle, in denen ein Anbieter aktiv Daten an eine Behörde in einem Drittstaat übermittelt, z. B. als Reaktion auf eine behördliche Anordnung oder ein Gerichtsurteil. Eine solche Übermittlung ist nur erlaubt, wenn eine rechtskräftige internationale Übereinkunft besteht oder in Ausnahmefällen folgende Bedingungen erfüllt sind:

- Die Anordnung muss begründet, verhältnismäßig und konkret sein.

- Der Anbieter muss die Möglichkeit haben, vor einem Gericht im Drittstaat rechtlich dagegen vorzugehen.
- Das ausländische Gericht muss die Interessen und Rechte des EU-Anbieters berücksichtigen.
- Der Anbieter darf sich von nationalen Behörden beraten lassen und muss das Prinzip der Datenminimierung beachten.

Falls die Entscheidung die nationale Sicherheit oder Verteidigungsinteressen der Union oder ihrer Mitgliedstaaten beeinträchtigen könnte, muss der Anbieter die Stellungnahme der nationalen Stellen einholen. Bei fehlender Antwort innerhalb eines Monats oder negativer Stellungnahme kann der Anbieter die Aufforderung ablehnen.

Der Anbieter muss Kunden informieren, wenn Daten an ausländische Behörden übermittelt werden, außer bei Strafverfolgung, wenn dies Ermittlungen gefährden würde.

4.1.4 Rechtskräftige internationale Übereinkunft

Ein zentraler Baustein für die Rechtmäßigkeit staatlicher Zugriffe oder Übermittlungen ist das Vorliegen einer rechtskräftigen internationalen Übereinkunft. Hierzu zählen:

- bilaterale oder multilaterale Rechtshilfeabkommen,
- internationale Kooperationsabkommen zwischen der EU und Drittstaaten,
- spezifische Vereinbarungen zwischen einzelnen Mitgliedstaaten und Drittstaaten.

Solche Vereinbarungen schaffen eine gemeinsame Rechtsgrundlage für die grenzüberschreitende Zusammenarbeit. Nur wenn sie bestehen, kann ein Zugriff oder eine Übermittlung grundsätzlich als rechtmäßig anerkannt werden. Fehlt eine solche Übereinkunft, greifen die strengen Schutzvorschriften des Art. 32 Abs. 3 DA, die eine Übermittlung faktisch stark einschränken.

5 Missbräuchliche Vertragsklauseln (Art. 13 DA)

Valentino Halim, Rechtsanwalt Tech, Data & AI, Junior Partner, Oppenhoff & Partner Rechtsanwälte Steuerberater mbB |
Nancy Ngân Piechota, Rechtsanwältin, Taylor Wessing Partnerschaftsgesellschaft mbB |
Paul Brings, Rechtsanwalt, Taylor Wessing Partnerschaftsgesellschaft mbB

EG 58, 60, 61, 62 DA

Ein weiteres zentrales Ziel des DA besteht darin, faire und transparente Vertragsbedingungen über Datenzugang und Datennutzung zu gewährleisten.

Art. 13 DA legt hierzu – ähnlich Art. 3 Richtlinie 93/13/EWG (im Folgenden **Klausel-RL** und §§ 305 ff. BGB (im Folgenden **deutsches AGB-Recht**) – Regeln für eine inhaltliche Kontrolle und rechtskonforme Gestaltung von Vertragsklauseln fest, um missbräuchliche Vertragsbedingungen in datenbezogenen Verträgen zwischen Unternehmen zu verhindern. Einseitige und unangemessene Vertragsbedingungen, die ein erhebliches Ungleichgewicht in Geschäftsbeziehungen zwischen den jeweiligen Vertragsparteien schaffen, sind danach nicht bindend. Die Missbrauchskontrolle schützt vor allem kleine und mittlere Unternehmen (KMU), die aufgrund ihrer Verhandlungsposition gegenüber größeren Unternehmen im Rechtsverkehr häufig benachteiligt werden.

5.1 Anwendungsbereich der Missbrauchskontrolle

Nicht alle vertraglichen Regelungen unterliegen der Missbrauchskontrolle. Diese greift gemäß Art. 13 Abs. 1 DA bei Vertragsklauseln über die Bereitstellung von Daten, d. h. den Datenzugang und die Datennutzung, und die Haftung oder Rechtsbehelfe bei Verletzung und Beendigung datenbezogener Pflichten. Die Regelung schränkt andere Regelungen desselben Vertrags nicht weiter ein (EG 60 DA). Die Missbrauchskontrolle findet sowohl auf das Vertragsverhältnis zwischen Dateninhaber und Nutzer (Datengenerierungsverhältnis) als auch zwischen Dateninhaber und Drittem (Datenweitergabeverhältnis) Anwendung.

Die Missbrauchskontrolle greift nur bei Vertragsbedingungen, die einem Unternehmen einseitig auferlegt werden. Dies betrifft sog. Take-It-or-Leave-It-Situationen, in denen

keine echte Verhandlungsmöglichkeit besteht. Ein einseitiges Auferlegen liegt vor, wenn eine Vertragsbedingung von einem Unternehmen als Verwender eingebracht wird und die andere Vertragspartei erfolglos versucht, über den Inhalt der Vertragsbedingung zu verhandeln. Dies unterscheidet sich von der Anforderung an eine Verhandlung von Vertragsbedingungen nach deutschem AGB-Recht, wo keine solchen Verhandlungsversuche notwendig sind.

Der DA stellt keine Anforderungen dahingehend, in welcher Form eine Vertragsverhandlung versucht worden sein muss. Jedoch schreibt Art. 13 Abs. 6 S. 2 DA vor, dass das einbringende Unternehmen nachweisen muss, dass keine Verhandlung stattgefunden hat. Da eine solche negative Tatsache im Einzelfall nicht belegbar sein wird, kann sich das einbringende Unternehmen darauf berufen, dass der Vertragspartner den Verhandlungsversuch beweisen muss.

Unternehmen können die Vorgaben der Missbrauchskontrolle vermeiden, wenn sie einen »strategischen« erfolglosen Verhandlungsversuch unternommen haben. Ein solcher Versuch sollte zu Nachweiszwecken dokumentiert werden.

5.2 Feststellung der Missbräuchlichkeit im Detail

Um zu bestimmen, ob eine Vertragsklausel missbräuchlich ist, sieht Art. 13 DA ein mehrstufiges Prüfschema vor. Dabei gilt, dass Klauseln, die zwingendem EU-Recht entsprechen, gemäß Art. 13 Abs. 2 DA niemals missbräuchlich sind. Im Übrigen sollten Unternehmen die folgenden Schritte untersuchen:

5.2.1 Blacklist

In einem ersten Schritt ist die sog. Blacklist[291] zu prüfen. Diese abschließende Liste enthält Klauseln, die stets als missbräuchlich gelten (EG 62 DA). Die Klauseln der Blacklist sind ohne weitere Prüfung unwirksam und dürfen in Verträgen nicht verwendet werden. Die Verbote schaffen Rechtssicherheit und bieten Unternehmen eine klare Orientierungshilfe für die Vertragsprüfung und -gestaltung.

Zur Blacklist gehören insbesondere Vertragsbedingungen, die entweder die Haftung für vorsätzliches oder grob fahrlässiges Verhalten ausschließen oder beschränken[292], der benachteiligten Partei bei Nichterfüllung vertraglicher Pflichten Rechtsbehelfe vorenthalten[293] oder die Auslegung von Vertragsbedingungen sowie die Beurteilung der Vertragserfüllung ausschließlich der einbringenden Partei vorbehalten[294].

Verstöße gegen die Blacklist führen automatisch zur Unverbindlichkeit (Unwirksamkeit) der Klausel(n) und potenzieller Sanktionen.

[291] Art. 13 Abs. 4 DA.
[292] Art. 13 Abs. 4 lit. a DA.
[293] Art. 13 Abs. 4 lit. b DA.
[294] Art. 13 Abs. 4 lit. c DA.

5.2.1 Greylist

Der zweite Prüfschritt betrifft die sog. Greylist[295]. Sie beinhaltet Vertragsbedingungen, von denen vermutet wird, dass ihre Inhalte missbräuchlich sind. Anders als bei der Blacklist ist diese Vermutung indes widerlegbar. Die Vertragsbedingungen der Greylist sind einer besonderen Prüfung zur Beurteilung im Einzelfall zugänglich, um die Angemessenheit der fraglichen Vertragsbedingungen zu beurteilen. Dies umfasst Vertragsbedingungen,

- die einseitig auferlegt wurden und eine unangemessene Beschränkung der Rechtsmittel oder Haftung bei Nichterfüllung vorsehen oder die Haftung der benachteiligten Partei unangemessen erweitern[296],
- dem einbringenden Unternehmen Zugriff auf Daten gewähren, deren Nutzung die berechtigten Interessen des anderen Unternehmens erheblich schädigt, insbesondere bei sensiblen oder geschützten Geschäftsdaten[297],
- die Nutzung, Kontrolle oder Verwertung der von dem Unternehmen, dem die Klausel einseitig auferlegt wurde, bereitgestellten oder erzeugten Daten während der Vertragslaufzeit unangemessen einschränken[298],
- die Kündigung des Vertrags innerhalb einer angemessenen Frist durch das Unternehmen, dem die Klausel einseitig auferlegt wurde, verhindern[299],
- den Erhalt einer Kopie der bereitgestellten oder generierten Daten nach Vertragsende unangemessen verhindern[300],
- dem einbringenden Unternehmen eine Kündigung mit unangemessen kurzer Frist erlauben, ohne Rücksicht auf den Wechsel zu einem anderen vergleichbaren Dienst und den wirtschaftlichen Schaden[301],
- oder wesentliche Vertragsbedingungen wie Format, Art, Qualität oder Menge der Daten ohne triftigen Grund ändern, ohne dem anderen Unternehmen, dem die Klausel einseitig auferlegt wurde, ein Kündigungsrecht einzuräumen[302].

Verstöße führen ebenfalls zur Unverbindlichkeit der betroffenen Vertragsbedingung, wobei die Beweislast für eine etwaige Widerlegung beim Verwender der jeweiligen Klausel liegt. Unternehmen sollten die Greylist sorgfältig prüfen und die Ergebnisse dieser Prüfung dokumentieren, um diesbezügliche rechtliche Risiken zu minimieren.

5.2.3 Generalklausel

Im dritten und letzten Schritt ist die Generalklausel[303] zu prüfen. Danach sind Vertragsklauseln missbräuchlich, wenn sie eine grobe Abweichung von der guten

[295] Art. 13 Abs. 5 DA.
[296] Art. 13 Abs. 5 lit. a DA.
[297] Art. 13 Abs. 5 lit. b DA.
[298] Art. 13 Abs. 5 lit. c DA.
[299] Art. 13 Abs. 5 lit. d DA.
[300] Art. 13 Abs. 5 lit. e DA.
[301] Art. 13 Abs. 5 lit. f DA.
[302] Art. 13 Abs. 5 lit. g DA.
[303] Art. 13 Abs. 3 DA.

Geschäftspraxis darstellen oder gegen das Gebot von Treu und Glauben verstoßen. Dies betrifft Klauseln, die ein erhebliches Ungleichgewicht zwischen den Vertragsparteien schaffen und daher nicht bindend sind. Die Generalklausel dient als Auffangregelung für Fälle, die nicht durch die Blacklist[304] oder Greylist[305] abgedeckt sind.

Die Generalklausel ist besonders praxisrelevant, da sie auf die Umstände des Einzelfalls abstellt und daher eine flexible Bewertung ermöglicht.

Eine genaue Festlegung der Bewertungskriterien ist derzeit noch nicht möglich, insbesondere da bislang noch keine dispositiven Rechtsvorschriften für den Datenzugang und die Datennutzung existieren. Allerdings hat eine Expertengruppe der EU-KOM einen finalen Entwurf standardisierter Mustervertragsbedingungen vorgelegt.[306] Obwohl die offizielle, endgültige Fassung der Mustervertragsbedingungen der EU KOM erst bis zum 12. September 2025 erwartet wird, bietet der finale Entwurf Anhaltspunkte, welche Vertragsklauseln Gerichte voraussichtlich als faire und ausgewogene Geschäftspraxis ansehen werden.

Unternehmen, die sich verhältnismäßig eng an den Mustervertragsbedingungen orientieren, dürften die Anforderungen der Generalklausel nach Art. 13 Abs. 3 DA erfüllen. Allerdings enthalten die Mustervertragsbedingungen keine allgemeingültigen Leitlinien dazu, was als gute Geschäftspraxis gilt. Bei Abweichungen von den Mustervertragsbedingungen fehlt für Unternehmen damit vorerst eine klare Orientierung, wann die Einhaltung einer guten Geschäftspraxis gewährleistet ist.

Das Merkmal von Treu und Glauben ist bereits aus Art. 3 Abs. 1 Klausel-RL[307] bekannt. Hiernach ist unter Berücksichtigung von höchstrichterlicher Rechtsprechung[308] davon auszugehen, dass Treu und Glauben das Verhalten umfasst, das ein Vertragspartner nach loyalem und billigem Verhalten vernünftigerweise erwarten durfte. Auch dieser Maßstab wird sich mit der Zeit weiter konkretisieren.

Die Generalklausel ähnelt in nicht wenigen Punkten den nach deutschem AGB-Recht bestehenden Regelungen z.B. der §§ 309 Nr. 7 ,8 BGB und bietet so eine in der Praxis bewährte Grundlage für die Bewertung von Missbräuchlichkeit.

5.3 Geltungsbeginn

Gemäß Art. 50 DA gilt Art. 13 DA für Verträge, die ab dem 12. September 2025 geschlossen wurden.

5.4 Durchsetzung und Rechtsfolgen

[304] Art. 13 Abs. 4 DA.
[305] Art. 13 Abs. 5 DA.
[306] Expert Group on B2B data sharing and cloud computing contracts, «Final Report of the Expert Group on B2B data sharing and cloud computing contracts", 02.04.2025, zuletzt abgerufen am 27.08.2025, https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/116180/download.
[307] ABl. L 95, 93/13/EWG, 5.4.1993, S. 29ff.
[308] Vgl. EuGH, Urteil vom 14.03.2013 – C-415/11.

Missbräuchliche Klauseln sind nicht bindend[309]. Das heißt, die entsprechenden Klauseln können von dem Verwender nicht durchgesetzt werden und müssen von der benachteiligten Vertragspartei nicht beachtet werden. Dies ist zwingend. Die Parteien können die rechtliche Folge nicht ausschließen oder davon abweichen[310].

Im Übrigen könnten Wettbewerber oder berechtigte Verbände das die missbräuchliche Klausel verwendende Unternehmen abmahnen und auf Unterlassung in Anspruch nehmen. Bei den Bestimmungen des DA zu missbräuchlichen Vertragsklauseln dürfte es sich um Marktverhaltensregeln im Sinne des § 3a des Gesetzes gegen den unlauteren Wettbewerb (UWG) handeln.

In Fällen, in denen das verwendende Unternehmen zugleich gegen weitere Bestimmungen des DA verstößt, können auch die Verhängung von Bußgeldern drohen.

5.5 Fazit und Ausblick

Die Regelungen aus Art. 13 DA betreffen sowohl Dateninhaber und Nutzer als auch Datenempfänger. Unabhängig davon, welche Rolle ein Unternehmen im Kontext von Datennutzungen einnimmt, ist genau zu prüfen, ob die Vertragsbedingungen das Unternehmen in seinen Rechten nach dem DA benachteiligen.

Unternehmen ist zu raten, die vorstehend beschriebenen Prüfschritte im Einzelfall durchzuführen, um sicherzustellen, dass die verwendeten Vertragsbedingungen rechtlich durchsetzbar sind.

Unter welchen Voraussetzungen eine Vertragsklausel gegen die Grundsätze der guten Geschäftspraxis oder gegen Treu und Glauben verstößt, wird eine entscheidende Frage für die praktische Anwendung des DA sein. Die Bewertung erfordert eine sorgfältige Einzelfallprüfung und wird künftig maßgeblich durch die Rechtsprechung nationaler Gerichte sowie durch die Vorgaben und Leitlinien zuständiger Behörden sowie die Mustervertragsbedingungen der EU-KOM konkretisiert werden. Bis dahin bleibt für Unternehmen eine gewisse Rechtsunsicherheit, welche Vertragsklauseln als missbräuchlich einzustufen sind.

[309] Art. 13 Abs. 1 DA.
[310] Art. 13 Abs. 9 DA.

6 Implementierung

6.1 Umsetzung des Datenzugangs (Art. 4, 5 DA)

Lukas Klein, Manager, Digetiers GmbH | Anne Untermann, Consultant, Digetiers GmbH

6.1.1 Identifikation und Beschreibung relevanter Daten

Die folgenden Abschnitte befassen sich mit der praktischen Umsetzung zur Identifikation, Klassifizierung und Beschreibung der für den DA relevanten Daten in betroffenen Unternehmen. Entwickler und Hersteller vernetzter Produkte müssen dabei nicht nur klären, welche Daten überhaupt ausgeleitet werden, sondern auch sicherstellen, dass berechtigte Empfänger diese eigenständig verstehen und interpretieren können. Dies erfordert neben der physischen Ausleitung der Daten auch die Bereitstellung klarer, verständlicher Beschreibungen bzw. Metadaten für Nutzer oder beauftragte Dritte.[311]

Der Grundstein zur Identifikation und Klassifizierung der vom DA betroffenen Daten ist die vollständige Transparenz über die im eigenen Unternehmen verfügbaren Daten. Idealerweise existiert bereits eine vollständige Dokumentation über vorhandenen Daten im Unternehmen – beispielsweise in Form eines unternehmensweiten Datenkatalogs. Folglich kann dieser Datenkatalog als Absprungbasis für alle weiteren Schritte dienen. Für den Fall, dass bislang noch keine bzw. noch keine durchgängig etablierte Lösung zur Dokumentation der eigenen Daten existiert, muss diese im Rahmen der Erfüllung des DA konzeptioniert und ausgerollt werden. Ferner ist eine sowohl menschen- als auch maschinenlesbare Ausleitung der erforderlichen Metadaten über beispielsweise eine zentral zugängliche Datenbank essenziell für die Erfüllung des DA.[312]

Als Ausgangspunkt für die Identifikation relevanter Produkt- und zugehöriger Dienstdaten empfiehlt sich eine umfassende Analyse der im vernetzten Produkt sowie in dessen Umfeld entstehenden Daten und Datenflüsse. Dabei sollte untersucht werden, welche Informationen zu Leistung, Nutzung und Umgebung generiert und beispielsweise über elektronische Kommunikationsdienste weitergeleitet werden.[313] Die Zerlegung der Produkte in logisch abgrenzbare Einheiten wie Sub-Systeme, Komponenten, Funktionen oder vergleichbare Cluster kann die Komplexität der initialen Analyse reduzieren. Im Fokus steht dabei nicht allein das Produkt selbst, sondern ebenso die damit verbundenen Dienste, die dessen Funktionalität erweitern und beeinflussen – beispielsweise durch zusätzliche digitale Features oder

[311] Vgl. Art. 3 Abs. 2, 3, Art. 4 Abs. 1, Art. 5 Abs. 1 DA, EG 24 DA sowie Abschnitte 2.3.5, 2.4.1, 2.5.1.
[312] Für eine Einleitung bzgl. Datenkatalogen und Datenmarktplätzen vgl. Bitkom, »Leitfaden Best Practices zur Entwicklung von Datenprodukten«, 2023, S. 19ff, https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Best-Practices-Entwicklung-von-Datenprodukten.
[313] Vgl. EG 14, Art. 2 Nr. 5 DA sowie Abschnitte 2.1.1, 2.1.2.

cloudbasierte Interaktionen.[314] Ziel ist es, nachzuvollziehen, wie sich die interne Produktarchitektur zusammensetzt, welche Systemkomponenten miteinander interagieren und an welchen Stellen konkret Daten bei der Nutzung durch den jeweiligen Nutzer entstehen. Systeme, Steuergeräte, Sensoren, Aktoren oder Gateways sind typische Quellen, an denen Produktdaten erzeugt, weitergeleitet oder verarbeitet werden. Darüber hinaus ist eine genaue Betrachtung der schon heute bestehenden Datenflüsse (z. B. via Kabel, Bluetooth, etc.) aus dem Produkt heraus erforderlich. Die Analyse sollte nicht bei der reinen Datenübertragung enden, sondern von Beginn an auch berücksichtigen, in welchen Systemen (z.B. Cloud-Datenbanken) die physischen Daten anschließend abgelegt und gespeichert werden und in welchem Format sie dort vorliegen. Darüber hinaus ist zu klären, ob die Verantwortlichkeit für die betroffenen Systeme unternehmensintern und/oder bei externen Dienstleistern liegt. Für all diese teilweise sehr komplexen Analysen empfiehlt es sich, die entsprechenden Experten und verantwortlichen Personen der Daten aus den Entwicklungsbereichen frühzeitig zu involvieren. Insbesondere bei der Identifikation betroffener Backendsysteme können ggf. bereits vorhanden Enterprise-Architekturbilder und Datenflussdiagramme helfen.

Auf Basis der so identifizierten Produkt- und Dienstdaten kann anschließend die Bewertung und Klassifizierung der DA Relevanz erfolgen. Voraussetzung hierfür ist ein klar definiertes Regelwerk, dass durch eine spezialisierte Rechtsberatung oder die unternehmensinterne Rechtsabteilung definiert wird. In der Praxis haben sich Werkzeuge wie Entscheidungsbäume und einfach verständliche und pragmatisch anwendbare Fragebögen bewährt. Es empfiehlt sich, die Klassifizierung dezentral durch die verantwortlichen Fachbereiche bzw. Dateneigner vornehmen zu lassen, da sie in der Regel über die größte inhaltliche, technische und fachliche Expertise hinsichtlich der Daten verfügen. Im Zuge dessen sollten weitere Klassifizierungsmerkmale definiert und bewertet werden. Dazu zählen Überlegungen im Hinblick auf potenzielle Geschäftsgeheimnisse, kartellrechtliche Implikationen, relevante Veredelungs- bzw. Verarbeitungsstufen von Daten sowie der Schutz von proprietären Inhalten. Weiterhin lassen sich personenbezogene (Produkt-/Dienst-) Daten ggf. über das Verzeichnis von Verarbeitungstätigkeiten[315] ermitteln.

Idealerweise erfolgt der Bewertungsprozess toolgestützt und parallel zur Beschreibung bzw. Inventarisierung der identifizierten Daten. Gemeinsam mit der Rechtsabteilung sind hierfür spezifische Anforderungen an die Dokumentation und Nachverfolgbarkeit der Bewertungsschritte zu definieren und umzusetzen, um Revisionssicherheit sowie die Erfüllung von Prüfpflichten gegenüber Aufsichtsbehörden sicherzustellen.

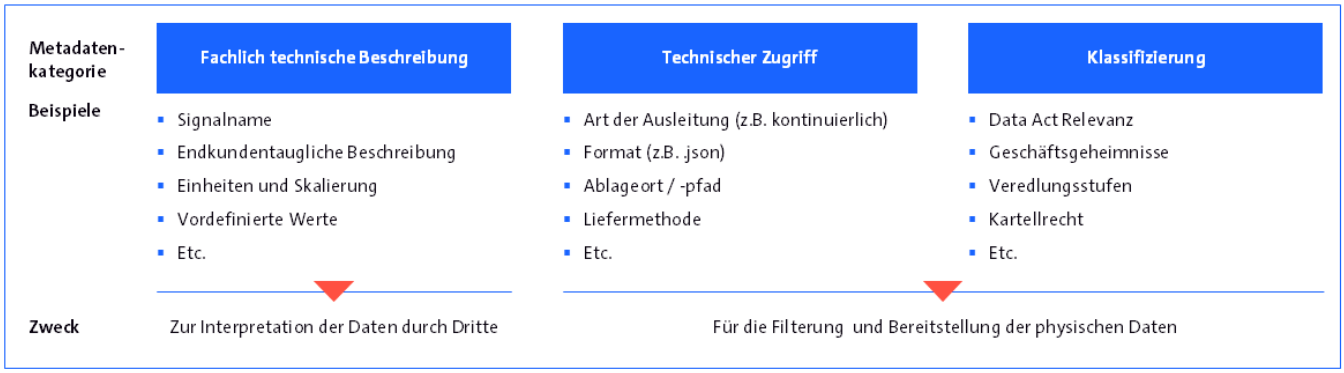
Auch wenn im Optimalfall alle betroffenen Daten bereits vor dem Inkrafttreten des DA im Rahmen einer generellen Datenstrategie[316] inventarisiert und beschrieben wurden, stellt der DA erweiterte Anforderungen an die Metadatenbereitstellung. Hersteller sind hierdurch verpflichtet, eine Beschreibung zu liefern, die »[...] eine strukturierte Beschreibung der Inhalte oder der Nutzung von Daten, die das Auffinden eben jener Daten bzw. deren Verwendung erleichtert«[317].

[314] EG 24 DA; vgl. Art. 4 Abs. 1, Art. 5 Abs. 1, Art. 2 Nr. 6, Nr. 16 DA sowie insb. Abschnitte 2.4.1, 2.5.1.
[315] Art. 30 DSGVO.
[316] Für eine Einleitung bzgl. Datenstrategien vgl.: Bitkom, »Datenstrategien: Bestandsaufnahme, Einführung & Zukunft«, 2024, zuletzt abgerufen am 27.08.2025, https://www.bitkom.org/Bitkom/Publikationen/Datenstrategien-Bestandsaufnahme-Einfuehrung-Zukunft.
[317] Art. 2 Nr. 2 DA.

Erforderliche Metadaten sind hierbei durch den Hersteller

- **gemäß Art. 4 Abs. 1 DA:** »[...] unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit [...]« bzw.
- **gemäß Art. 5 Abs. 1 DA:** »[...] unverzüglich, für den Nutzer unentgeltlich, in derselben Qualität, die dem Dateninhaber zur Verfügung steht, einfach, sicher, für den Nutzer unentgeltlich, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, kontinuierlich und in Echtzeit [...]« bereitzustellen, was gleichermaßen die Leitplanken zur Dokumentation dieser darstellt.

Darüber hinaus sollten Metadaten so beschrieben werden, dass sie auch ohne tiefes Fach- oder Domänenwissen für Nutzer und fachfremde Dritte verständlich, interpretierbar und effizient nutzbar sind. Ergänzend ist die Dokumentation der technischen Metadaten erforderlich, um die Lokalisierung der physischen Daten und damit deren spätere Ausleitung sicherzustellen. Auch im Hinblick auf die erforderlichen Metadaten gilt, dass bereits vor der Inventarisierung eine enge Abstimmung mit designierten Rechtsvertretern und fachlichen und IT-seitigen Experten erfolgen sollte, um das konkrete fachliche, sowie technisch notwendige Mindestmetadatenset zu definieren. Eine Option für eine mögliche Metadatenstruktur inkl. entsprechender Beispiele ist in der folgenden Grafik aufgezeigt.



Klein, Untermann, 2025.

Zusammenfassend lässt sich sagen, dass Unternehmen, die bereits über ein etabliertes und zentral zugängliches Dateninventar verfügen einen gewissen Vorteil bei der Identifikation, Klassifikation und Beschreibung der relevanten Daten haben. Nichtsdestotrotz stellt der DA zusätzliche Anforderungen, die vermutlich in jedem Unternehmen eine qualitative Nacharbeit erfordern. Essenziell für den Erfolg und die Effizienz der zuvor beschriebenen Schritte bleibt ein pragmatisches und technisch abbildbares Konzept. Da die manuelle Erstellung beschreibender Metadaten ohne Nutzung von Automatisierungspotenzialen in den Fachbereichen häufig mit erheblichem Aufwand verbunden ist, sollten unterstützende Maßnahmen – wie etwa initial durch KI-generierte und anschließend durch die Verantwortlichen verifizierte

Beschreibungen – sorgfältig geprüft und gezielt und rechtskonform eingesetzt werden. Neben dem zusätzlichen Aufwand eröffnet der DA Unternehmen, die bislang mit der Definition und Umsetzung einer übergreifenden Datenstrategie gerungen haben, zugleich eine klare – nun verpflichtende – Chance: der gezielte Aufbau und die nachhaltige Verankerung notwendiger Strukturen für Data Governance und Datenmanagement.

6.1.2 Konzeptionelle Ansätze zur technischen Umsetzung von Art. 4, 5 DA

Im Folgenden sollen erste Impulse und Konzepte für die initiale Umsetzung der Anforderungen aus Art. 4 und 5 DA für »ohne Weiteres verfügbarer Daten« (»readily available«) an Nutzer und / oder beauftragte Dritte gegeben werden[318]. Die Umsetzung des direkten Zugriffs gemäß Art. 3 Abs. 1 DA erfordert – sofern noch keine entsprechende Produktschnittstelle besteht – tiefgreifende Anpassungen der Produktarchitektur und ist daher separat, mit Blick auf bestehende Entwicklungsprozesse und ausreichenden Planungsvorlauf, zu berücksichtigen. Allerdings sind die im vorherigen Abschnitt zur Identifikation, Beschreibung und Klassifizierung der vom DA betroffenen Produkt- und verbundenen Dienstdaten ausgeführten Anforderung und Schritte unabhängig der umzusetzenden Artikel gültig.

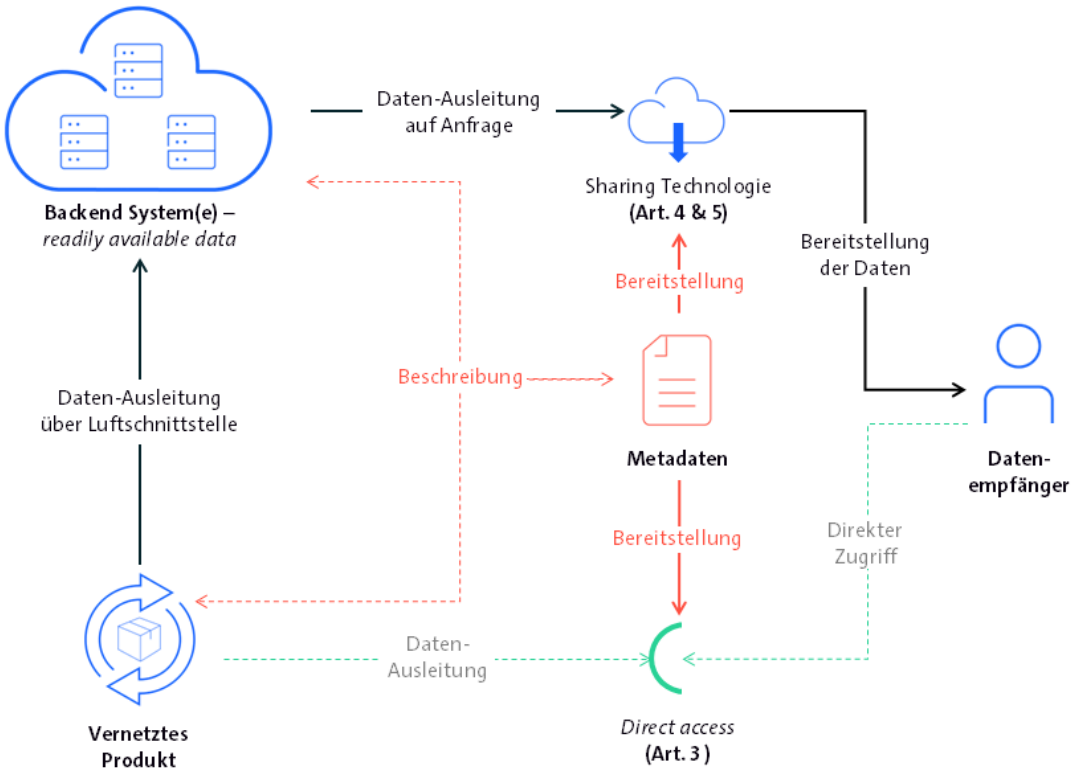
Im Hinblick auf die ab September 2025 geltenden Anforderungen aus Art. 4 Abs. 1 und 5 Abs. 1 DA sind – mit Fokus auf die erforderlichen Elemente und Fähigkeiten der Enterprise-Backend-Architektur – drei grundlegende Komponenten zu betrachten:

- **Ablageort der physischen Daten (z.B. Data Lake):** Der Ort bzw. Orte in den jeweiligen Backends in denen die physischen Daten bereits verfügbar und entweder temporär oder auch persistiert abliegen. Je nach Komplexität kann es mehrere dieser Orte geben. Für die spätere Ausleitung ist insbesondere relevant, auf welche Weise (in Echtzeit oder als historische Datensätze), in welcher Form (z. B. gefilterte Dateien oder Payloads) und nach welchem Schema die Daten bereitgestellt werden.
- **Metadaten Speicher (Dateninventar):** Der zentrale Speicherort an dem die erforderlichen und beschreibenden Metadaten inkl. der gesetzten Klassifizierungen sowohl maschinen- als auch menschenlesbar abliegen. Dazu gehört auch die genaue Angabe des entsprechenden physischen Ablageortes und des technischen Zugangs zum jeweiligen Datenpunkt, um die Daten für eine Ausleitung auffindbar zu machen.
- **Sharing Technologie:** Für die Ausleitung an den Nutzer oder beauftragte Dritte braucht es sowohl eine geeignete Schnittstelle bzw. Frontend inkl. User-Flow, um eingehende Anfragen verarbeiten zu können als auch die entsprechenden technischen Integrationen zur Anzeige und tatsächlichen Ausleitung der angefragten Daten. Gleichermaßen sollte die Ausleitung der für die Verwendung erforderlichen Metadaten an Nutzer und Dritte technisch sichergestellt und prozessual eingebettet werden. Zur Wahrung der Datenintegrität und Vertraulichkeit sollten zwingend übergreifende Schutzmechanismen integriert

[318] Art. 4 Abs. 1, Art. 5 Abs. 1 DA.

werden. Dies betrifft insbesondere Aspekte wie Verschlüsselung und sichere Übertragungswege, die als technologische Mindeststandards etabliert werden sollten.

Soweit im Falle der Umsetzung von Art. 3 DA die erzeugten Daten über eine direkte Schnittstelle an den Nutzer ausgeleitet werden, fallen die Sharing Technologie Komponente als auch die Datenbanken im Backend weg. In der folgenden Abbildung sind die Zusammenhänge und Komponenten nochmals schematisch aufgezeigt:



Klein, Untermann, 2025.

6.1.3 Impulse zur Entwicklung eines langfristigen Betriebskonzeptes

Die Erfüllung des DA ist keine einmalige Aufgabe, sondern verlangt eine durchgängige Integration der Anforderungen in Entwicklungs-, Datenmanagement- und Governance-Prozesse, um die kontinuierliche Umsetzung des DA sicherzustellen. Entsprechend sollten die Vorgaben zur Dateninventarisierung und -klassifizierung dauerhaft in den Produktentstehungsprozess eingebettet werden, um langfristig manuelle Nacharbeiten zu vermeiden. Jedes neue vernetzte Produkt, verbundener Dienst oder Feature sollte diesen Prozess künftig von Beginn an durchlaufen – idealerweise als inhärenter Bestandteil der technischen und regulatorischen Anforderungsdefinition. So wird sichergestellt, dass regulatorische Anforderungen nicht nachgelagert, sondern vorausschauend und effizient berücksichtigt werden. Gleichzeitig schafft dies Raum für eine kontinuierliche Weiterentwicklung der Prozesse, etwa bei sich ändernden regulatorischen Rahmenbedingungen oder

technologischen Neuerungen. Parallel dazu ist eine eindeutige Regelung der Zuständigkeiten für die Pflege und Aktualisierung der Daten erforderlich – wer für welche Daten, dazugehörigen Metadaten und deren Bewertung zuständig ist, sollte dabei nachvollziehbar dokumentiert und allen beteiligten Akteuren zugänglich sein. Erst dadurch kann gewährleistet werden, dass Entscheidungen über die Datenverwendung, -freigabe oder -verantwortung auch unter regulatorischem Druck belastbar sind.

Mit Hinblick auf die zu erzielende Außenwirkung – insbesondere gegenüber Nutzern oder Dritten – kann es sinnvoll sein, eine dedizierte Clearing-Stelle zu etablieren, die die bereitgestellten Metadaten und Beschreibungen zentral überprüft. Die dezentrale Inventarisierung durch z.B. Mitarbeiter der technischen Entwicklung kann ggf. zu Diskrepanzen und Qualitätsunterschieden führen. Eine zweite jetzt nun zentrale Instanz kann dazu beitragen, die inhaltliche Konsistenz, Verständlichkeit und rechtliche Konformität der ausgeleiteten Informationen sicherzustellen und so Risiken in der externen Kommunikation wirksam zu minimieren.

Abschließend bleibt zu sagen, dass die aufgebauten Schnittstellen, Dokumentationen und Beschreibungen nicht nur für die Erfüllung des DA vorbehalten sind, sondern auch für interne Anwendungsfälle wie beispielweise Nutzungsanalysen (wo rechtlich möglich) genutzt werden sollten. Das Wissen und die Transparenz über die eigenen Daten und deren Verfügbarkeit ist einer der ersten und wichtigsten Schritte auf dem Weg zu einem datengetriebenen Unternehmen.

6.2 B2B und B2B Non-Realtime Data Sharing (Kap. II DA)

Lisa Böhler, Managing Consultant, NTT DATA Deutschland SE

6.2.1 Non Real Time Datenbereitstellung

Die Vielzahl der vom DA betroffenen Daten bringt verschiedene Herausforderungen in der Bereitstellung dieser mit sich. Die Unterscheidung zwischen RealTime- und Non-Real-Time-Daten bedeutet, dass davon auszugehen ist, dass einige Daten ausschließlich in Real Time zur Verfügung stehen und daher (technologisch) anders bereitgestellt werden müssen als Non Real Time-Daten, welche langfristig auf den Servern der Dateninhaber gespeichert werden.

Während reine Echtzeitdaten über eine API direkt abgegriffen werden können und somit eine technisch versierte Nutzergruppe ansprechen, sind gespeicherte Non-Real--Time-Daten für die breite Masse geeignet – vorausgesetzt, die Bereitstellung ist entsprechend aufbereitet.

6.2.2 Wie kann ein Nutzer seine Daten anfragen?

Die Erfahrung hat gezeigt, dass Unternehmen die Bereitstellung ihrer Daten auf unterschiedliche Weise ermöglichen – mit entsprechenden Vor- und Nachteilen. Während einige Unternehmen für eine bessere Nutzerinteraktion ihr bestehendes

Datenportal durch entsprechende Nutzerkonten ausbauen oder gar neu implementieren, setzen andere auf Serviceformulare. In beiden Fällen gilt es im ersten Schritt zu klären, um welches Produkt es sich handelt und welche Daten konkret angefordert werden. Ein Datenportal bietet die Möglichkeit einer integrierten Filterung: registrierte Nutzer sehen nur ihre eigenen Produkte und dazu passende Datenkategorien. Je nach Umsetzung können dabei sowohl Real-Time- als auch Non-Real-Time-Daten berücksichtigt werden.

Auch der Zeitraum kann bei der Datenabfrage eine Rolle spielen, etwa um Datenmengen zu reduzieren, aber auch um dem Anspruch der kontinuierlichen Datenbereitstellung[319] gerecht zu werden.

6.2.3 Datenschutz im DA – was gilt für die Datenbereitstellung?

Während in vielen Fällen lediglich sichergestellt werden muss, dass die angefragte Produkt- und Datenkonstellation dem Anfragenden zuzuweisen ist, kann es bestimmte Fälle geben, in denen von Nebennutzern erzeugte Daten personenbezogene Daten darstellen und nicht ohne explizite Zustimmung herausgegeben werden dürfen[320]. Das kann beispielsweise bei vernetzten Fahrzeugen der Fall sein, wenn zwei oder mehrere Fahrerprofile mit demselben Fahrzeug verbunden sind. Fragt beispielsweise der Hauptnutzer (i.d.R. Fahrzeughalter) Daten an, muss im Hintergrund geprüft werden, ob die angefragten Daten ausschließlich von ihm erzeugt wurden und sein Anspruch somit gültig ist, oder ob potenzielle Nebennutzer berücksichtigt werden müssen. Daten lassen sich dabei in drei Kategorien aufteilen:

- Fahrzeugbezogene Daten – erfordern Zustimmung von Hauptnutzern sowie ggf. im Anfragezeitraum aktiven Nebennutzern
- Hauptnutzerbezogene Daten – erfordern keine zusätzliche Zustimmung
- Nebennutzer-erzeugte Daten – erfordern Zustimmung der entsprechenden Nebennutzer

Um datenschutzkonform zu agieren und die Nachweispflicht des DA zu erfüllen, muss die Zustimmung der Nebennutzer genauso eindeutig und belegbar sein, wie die Anfrage des Hauptnutzers auf Datenzugang. Andersherum müssen Nebennutzer die Möglichkeit haben, der Datenausleitung – insbesondere bei regelmäßiger Bereitstellung – jederzeit zu widersprechen. Die Anforderung der Zustimmung von Nebennutzern gilt ebenso bei der Bereitstellung der Daten an Dritte, auch wenn lediglich der Hauptnutzer Vertragspartner ist (vgl. Art. 5 Abs. 7 DA, vgl. hierzu Abschnitt 2.5.6).

6.2.4 Wie werden die Daten bereitgestellt?

Die Speicherung von Non-Real-Time-Daten erfolgt in der Regel über entsprechende Backendsysteme, die nach der erfolgten Datenanfrage voll- oder halbautomatisch

[319] Art. 4 Abs. 1 DA.
[320] Siehe Art. 4, 5 DA.

kontaktiert werden, um die Daten abzurufen. Ob die Anfrage komplett oder in mehrere Einzelanfragen aufgesplittet werden muss, hängt neben der unternehmensspezifischen Datenhaltung (zentrale oder verteilte Serverarchitektur, Anzahl der Datensammlersysteme, etc.) auch von der Art der Anfrage (ein oder mehrere Geräte, welche Datenkategorien, nur Haupt- oder auch Nebennutzer, etc.) ab.

Die Bereitstellung der Daten kann dann über verschiedene Wege erfolgen, abhängig davon, wie die Daten abgefragt wurden. So können Formularanfragen beispielsweise über eine per E-Mail versendeten Downloadlink, oder Zugriff auf ein interaktives Datendashboard mit Downloadfunktion beantwortet werden. Datenportale hingegen stellen meist auch einen Downloadbereich zur Verfügung, in dem die Anfragen nachvollzogen werden und die bereitgestellten Datenpakete heruntergeladen werden können.

Eine weitere Variable ist das Datenformat. Der DA schreibt vor, dass Daten in einem strukturierten, gängigen und maschinenlesbaren Format[321] bereitzustellen sind, das eine einfache Weiterverarbeitung ermöglicht, wodurch viele industriespezifische Formate nicht als alleinige Option geeignet sind.

Gängige Formate für die Non-Real-Time-Datenbereitstellung sind:

- CSV / Excel (XLSX) – für tabellarische Daten, leicht zugänglich für Endnutzer
- XML – weit verbreitet in der Industrie, gut strukturiert
- JSON – maschinenlesbar, ideal für Webanwendungen
- Protocol Buffers (Protobuf) – effizient und plattformneutral, besonders für große Datenmengen geeignet

Die Auswahl des Formats sollte sich an der Zielgruppe und dem Verwendungszweck orientieren – unter Berücksichtigung der Interoperabilitätsanforderungen des DA.

6.3 Cybersicherheit & Missbrauchsprävention (Art. 4, 5 DA)

Dr. Lucas Blum, Rechtsanwalt, Counsel, DLA Piper UK LLP | Dr. Richard Falk, LL.M. (King's College), Rechtsanwalt, Senior Associate, DLA Piper UK LLP

Die Pflicht zur »sicheren« Datenbereitstellung nach Art. 4 Abs. 1 und Art. 5 Abs. 1 DA macht deutlich, dass die IT- und Cybersicherheit (nachfolgend: IT-Sicherheit) im Rahmen der Datenbereitstellung sicherzustellen sind.[322] Übergeordnetes Ziel der sicheren Datenbereitstellung ist die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der **Daten** aber auch der **vernetzten Produkte und verbundenen Dienste.** Da sich im DA keine Konkretisierungen finden, wie die IT-Sicherheit sicherzustellen ist,

[321] Art. 4 Abs. 1, Art. 33 Abs. 1 DA.
[322] Frison/Katko/Schels in Rockstroh/Katko/Meyer (Hrsg.), »Compliance Handbuch EU Data Act«, 1. Aufl. 2025, Kap. 2 E Rn. 510-511.

können die Anforderungen aus anderen Regelwerken wie der DSGVO oder dem Cyber Resilience Act sowie Leitlinien und Industriestandards als Orientierung dienen. Die Sicherstellung der IT-Sicherheit lässt sich im Zusammenhang mit der Datenbereitstellung in drei Bereiche gliedern: die **Systemsicherheit**, die **Datensicherheit** und die **Übertragungssicherheit**.[323] Diese Bereiche müssen, auch mit Blick auf **Missbrauchsprävention**, in einer gemeinsamen **Risikoanalyse** bewertet werden, um eine tragfähige Sicherheitsarchitektur erstellen zu können.

6.3.1 Systemsicherheit

Im Rahmen der Systemsicherheit ist insbesondere sicherzustellen, dass die Bereitstellung der Daten keine **Sicherheitslücken im Produkt** verursacht. Der Dateninhaber muss gewährleisten, dass sowohl der Pflicht der Datenbereitstellung entsprochen wird aber auch weiterhin sämtliche notwendigen Sicherheitsstandards erfüllt werden.[324] Als Maßnahmen zur Sicherstellung der IT-Sicherheit sind beispielsweise Virenschutz und Firewalls zu nennen, aber auch hardwarebezogene Maßnahmen, etwa im Rahmen des Produktdesigns. Hervorzuheben sind in diesem Zusammenhang auch die Anforderungen des **Cyber Resilience Acts**, die ab 11. Dezember 2027 vollständig Anwendung finden.

6.3.2 Datensicherheit

In den Bereich der Datensicherheit fällt die **Authentifizierung** des anfragenden Nutzers, siehe hierzu auch unter Abschnitt 2.4.4. Der Dateninhaber muss sicherstellen, dass nur den natürlichen und juristischen Personen Daten bereitgestellt werden, die die berechtigten Nutzer im Sinne des DA sind, um einen unrechtmäßigen Datenabfluss zu verhindern. Werden Daten anderen Personen als dem berechtigten Nutzer bereitgestellt, so kann es sich gegebenenfalls um einen Verstoß gegen den DA und im Fall von personenbezogenen Daten (auch) um einen Verstoß gegen das Datenschutzrecht handeln. Zu den möglichen Maßnahmen, um die Eigenschaft als berechtigten Nutzer sicherzustellen, wird auf Abschnitt 2.4.4 verwiesen. Sicherzustellen ist neben der Authentifizierung auch die **Autorisierung**. So dürfen einem berechtigten Nutzer nur die seiner Nutzung eines vernetzten Produkts oder verbundenen Diensts zugeordneten Daten bereitgestellt werden. In Bezug auf die Datensicherheit sind daneben bei personenbezogenen Daten insbesondere die Anforderungen des Art. 32 DSGVO zu beachten. So muss die Sicherheit der Verarbeitung der Daten durch **geeignete technische und organisatorische Maßnahmen** gewährleistet werden, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Die in Bezug auf personenbezogene Daten entwickelten Maßstäbe und Maßnahmen können grundsätzlich als Ausgangspunkt auch für die Sicherheit von nicht-personenbezogenen Daten herangezogen werden.

6.3.3 Übertragungssicherheit

[323] Übersicht in Rockstroh/Katko/Meyer (Hrsg.), »Compliance Handbuch EU Data Act«, 1. Aufl. 2025, Kap. 2 D Rn. 333.
[324] Rockstroh/Katko/Meyer (Hrsg.), »Compliance Handbuch EU Data Act«, 1. Aufl. 2025, Kap. 2 D Rn. 511.

Die dritte Säule der Sicherheit ist die **Übertragungssicherheit**. Daten müssen während der Übermittlung an den Nutzer oder Dritten geschützt werden. Zu nennen ist in dieser Hinsicht insbesondere eine starke Transportverschlüsselung, wie beispielsweise via HTTPS/TLS.[325]

6.3.4 Beschränkung der Datenbereitstellung wegen Sicherheitsbedenken

Schließlich soll darauf hingewiesen werden, dass nach Art. 4 Abs. 2 DA die Bereitstellung von Daten vertraglich beschränkt werden kann, wenn hierdurch die im Unionsrecht oder im Recht der Mitgliedstaaten festgelegten Sicherheitsanforderungen des vernetzten Produkts beeinträchtigt werden könnten und dies zu schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen führen könnte. Diese Möglichkeit wird auch in den FAQ der EU-KOM zum DA auch als »safety and security handbrake« bezeichnet.[326]

6.3.4.1 Missbrauchsprävention

Neben der technischen Absicherung müssen auch Maßnahmen gegen missbräuchliche Praktiken erwogen und ergriffen werden. Solche Praktiken umfassen beispielsweise Irreführungen des Dateninhabers durch Bereitstellung falscher Informationen in der Absicht, die Daten für unrechtmäßige Zwecke zu nutzen. Die Motivation hierfür kann beispielsweise in einer Schädigungsabsicht oder gar Industriespionage bestehen.

Missbrauchsprävention knüpft hier auf zwei Ebenen an: Zunächst müssen bei der Authentifizierung der die Datenbereitstellung verlangenden Person alle für ihre Authentifizierung relevanten Informationen angefordert werden (Abschnitt 2.4.4). Für zentrale Informationen wie die Nutzereigenschaft für das konkrete Produkt können Nachweise gefordert werden (bspw. Nutzerkonto verbunden mit einer Produkt-ID, Kopie der Vertragsunterlagen). Zudem braucht es effektive Gegenmaßnahmen bei Verdacht auf erfolgten Missbrauch. Diese sollten u. a. umfassen: Möglichkeit zur sofortigen Beendigung der Datenbereitstellung, Sammlung geeigneter Beweismaterialien sowie ein internes Fraud-Playbook. Informationen der Strafverfolgungsbehörden sowie Lessons Learned sollten ergänzend genutzt werden, um einen weiteren Missbrauch zu verhindern.

6.3.5 Risikoanalyse und weitere Maßnahmen

Im Rahmen der praktischen Umsetzung empfiehlt es sich, mit einer **Risikoanalyse** zu starten – diese sollte die **Systemsicherheit**, die **Datensicherheit** und **Übertragungssicherhei**t sowie Missbrauchsprävention umfassen. Zu fragen ist also beispielsweise: Wie sensibel sind die Daten, die generiert werden? Wer sind die berechtigten Nutzer und wie kann ich diese wirksam authentifizieren und welche Risiken gehen von der Bereitstellung der Daten aus? Darauf aufbauend können die

[325] Frison/Katko/Schels in Rockstroh/Katko/Meyer (Hrsg.), »Compliance Handbuch EU Data Act«, 1. Aufl. 2025, Kap. 2 E Rn. 510-511
[326] EU-KOM, »FAQ Data Act«, Stand 03.02.2025, Version 1.2, S. 18f.
https://ec.europa.eu/newsroom/dae/redirection/document/108144.

konkreten technischen und organisatorischen Maßnahmen definiert werden, wobei die Orientierung an Standards wie dem IT-Grundschutz des BSI oder der ISO/IEC 27001 aber auch den im Datenschutzrecht etablierten technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO Anhaltspunkte bieten.

6.4 Technische Schutzmaßnahmen über die unbefugte Nutzung oder Offenlegung von Daten (Art. 11 DA)

Rainer Duda, Lead of Competence Center Data & AI, M&M Software GmbH | Dr. Richard Falk, LL.M. (King's College), Rechtsanwalt, Senior Associate, DLA Piper UK LLP

6.4.1 Begriff, Einsatz und Grenzen

Laut Art. 11 können Dateninhaber geeignete technische Schutzmaßnahmen (**TPM**) einsetzen, um die unbefugte Nutzung oder Offenlegung von Daten – einschließlich Metadaten – zu verhindern. Ziel des Dateninhabers ist eine Sicherheitsarchitektur, die Angriffe sowohl präventiv erschwert als auch im laufenden Betrieb aktiv erkennt und begrenzt.

Es besteht jedoch keine generelle Pflicht zur Umsetzung von TPM, und sie sind auch nicht genehmigungspflichtig. Der Kern von Art. 11 DA liegt stattdessen in der Einschränkung der angemessenen Ausgestaltung und Nutzung von TPM.

Der Begriff der TPM ist technikneutral zu verstehen; Beispiele sind u. a. Smart Contracts, Verschlüsselung, Firewalls, Zertifikate oder Access-Tokens.

6.4.2 Nicht-Diskriminierung & Nutzerzugang: Prüfmaßstab und Verhältnismäßigkeit

Entscheiden sich die Dateninhaber für die Anwendung von TPM, verlangt Art. 11 Abs. 1 DA, dass diese nicht-diskriminierend gestaltet sein dürfen. Zudem dürfen die Rechte der Nutzer gemäß Art. 4 DA (Berechtigung zu Datenzugang und -nutzung), Art. 5 (Weitergaberecht), Art. 6 DA (Bedingungen für die Datenbereitstellung), Art. 8 (Fairness und Nichtdiskriminierung) und Art. 9 DA (vertragliche Bedingungen für die Datenweitergabe) nicht eingeschränkt werden. Außerdem müssen die TPM mit den vertraglichen Regelungen übereinstimmen, die zwischen den Parteien vereinbart wurden. Diese Regelungen können auf den erwarteten unverbindlichen Mustervertragsklauseln der EU-KOM beruhen, müssen es jedoch nicht. Die Mustervertragsklauseln dienen als Orientierung ohne rechtliche Bindungswirkung. Im

April 2025 hat eine Expertengruppe der EU-KOM einen finalen Entwurf standardisierter Mustervertragsbedingungen vorgelegt.[327]

Unzulässig sind Gestaltungen, die zu einer faktischen Benachteiligung von Datenempfängern führen oder den Nutzerzugang behindern. Das ist aus Sicht eines durchschnittlichen Nutzers mit üblichen Fähigkeiten ohne individuelle Spezialkenntnisse zu bewerten. Dafür genügt bereits die Geeignetheit, den Zugang unzulässig zu beeinträchtigen. Auf den tatsächlichen Schadenseintritt kommt es nicht an.[328]

Für die Zulässigkeit von TPM im Produkt selbst gilt Art. 3 Abs. 1 DA, während Art. 11 Abs. 1 DA die im Backend des Dateninhabers wirkenden TPM adressiert.[329] Beide sind so auszugestalten, dass der im DA angelegte Zweck eines einfachen, sicheren und verwendbaren Datenzugangs nicht unterlaufen wird.

6.4.3 Konkrete Anwendung der TPM

Zur Erkennung und Verhinderung von Manipulationen kommen bei Cloud-Plattformen verschiedene »geeignete Schutzmaßnahmen« zum Einsatz, die oft in Kombination genutzt werden. Dazu zählen

Cloud Security Posture Management (CSPM) zur automatisierten Überwachung von Konfigurationen, Cloud Workload Protection Platforms (CWPP) zur Sicherung laufender Anwendungen sowie Data Loss Prevention (DLP), um unbefugte Datenveränderungen oder -abflüsse zu verhindern.

Ergänzend werden starke Verschlüsselung (sowohl im Ruhezustand – At Rest – als auch während der Übertragung – In Transit), konsequentes Identity- & Access-Management mit Multi-Faktor-Authentifizierung, differenzierte Zugriffssteuerungen wie RBAC (rollenbasierte Entscheidungen) oder ABAC (attributbasierte Entscheidungen), API-Gateways mit Authentifizierung und Rate-Limiting sowie regelmäßige Schwachstellen- und Compliance-Scans eingesetzt[330].

Spezialisierte Tamper-Detection-Mechanismen wie digitale Wasserzeichen[331] zur Herkunftsverfolgung, manipulationssichere Audit-Logs[332], intelligente Verträge (Smart Contracts)[333] und KI-gestützte Anomalieerkennung[334] tragen zusätzlich dazu bei, Manipulationen frühzeitig zu erkennen und deren Auswirkungen zu minimieren. Diese TPM müssen risikoorientiert gewählt werden und dürfen das legitime Nutzungsrecht

[327] Expert Group on B2B data sharing and cloud computing contracts, «Final Report of the Expert Group on B2B data sharing and cloud computing contracts«, 02.04.2025, zuletzt abgerufen am 27.08.2025, https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/116180/download.
[328] HK-DatenR/Denga, Art. 11 Rn. 7, 8.
[329] HK-DatenR/Denga, Art. 11 Rn. 5, 6.
[330] Siehe zum Thema Zero Trust Architecture bspw. PaloAltoNetworks, »What is Zero Trust Architecture (ZTA)?», zuletzt abgerufen am 21.08.2025, https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-security-posture-management oder IBM, »What is zero trust?«, zuletzt abgerufen am 21.08.2025, https://www.ibm.com/think/topics/zero-trust
[331] NIST, »Reducing Risks Posed by Synthetic Content, An Overview of Technical Approaches to Digital Content Transparency«, Stand 04/2024, https://airc.nist.gov/docs/NIST.AI.100-4.SyntheticContent.ipd.pdf
[332] Ahmad et. al, « Towards Blockchain-Driven, Secure and Transparent Audit Logs«, Stand 25.11.2018, https://arxiv.org/abs/1811.09944
[333] Agarwal et al., « Smart Contracts for Ensuring Data Integrity in Cloud Storage with Blockchain«, Stand 04/2024, http://dx.doi.org/10.4108/eetsis.5633
[334] Vervaet, « MoniLog: An Automated Log-Based Anomaly Detection System for Cloud Computing Infrastructures «, Stand 24.04.2023, https://arxiv.org/abs/2304.11940

nicht leerlaufen lassen. Eine zumutbare Erschwernis – etwa Token- oder Passwortschutz – ist akzeptabel, sofern der Zugang insgesamt nutzbar bleibt.

6.4.4 Security-by-Design und Zero-Trust

Gemäß dem Prinzip »Security by Design« sollten Schutzmechanismen von Beginn an in die Architektur und Implementierung eines Systems integriert werden, anstatt sie nachträglich hinzuzufügen. Im Vordergrund stehen dabei die Grundsätze »Least Privilege« (Zugriffe auf das absolut notwendige Maß beschränken) und »Defense in Depth« (mehrere, unabhängige Sicherheitsschichten). Zu den Zielen zählen die frühzeitige Minimierung von Risiken, eine nachhaltige Sicherheitsarchitektur und eine bessere Auditierbarkeit[335].

Die Zero-Trust-Architektur (ZTA) ergänzt dieses Konzept im laufenden Betrieb. Sie basiert auf der Annahme »Never trust, always verify«. Jeder Benutzer, jedes Gerät und jeder Dienst muss sich bei jeder Anfrage authentifizieren und autorisieren – unabhängig davon, ob er sich innerhalb oder außerhalb des Netzwerks befindet. Die Stärke der ZTA ist die Minimierung der Angriffsfläche und Reduktion des Risikos durch kompromittierte Konten oder Insider-Bedrohungen[336].

Technisch bedeutet die Kombination beider Ansätze, dass Systeme dazu befähigt sein müssen, Zugriffsrechte, API-Keys und Zertifikate unverzüglich zu entziehen, betroffene Datenbestände zu sperren und – sofern rechtlich und vertraglich zulässig – Funktionen gezielt zu deaktivieren. Ein optionaler »Remote-Kill-Switch« kann dabei als ergänzendes Instrument dienen, sofern er verhältnismäßig ist, vertraglich vereinbart wurde und keine Rechtsvorschriften verletzt.

6.4.5 Umgehungsverbot

Gemäß Art. 11 Abs. 1 letzter Satz DA dürfen Nutzer, Dritte oder Datenempfänger TPM nur dann verändern oder aufheben, wenn der Dateninhaber – und, falls abweichend, auch der Inhaber des Geschäftsgeheimnisses – ausdrücklich zugestimmt hat. Auch unzulässige TPM dürfen nicht ohne Zustimmung umgangen werden – es gibt also kein »Right to Hack«.

6.4.6 Reaktionspflichten bei Missbrauch (Art. 11 Abs. 2 – 4 DA)

Begeht ein Datenempfänger oder ein Dritter eine der in Art. 11 Abs. 3 DA beschriebenen Missbrauchshandlungen, ist er durch Art. 11 Abs. 2 DA verpflichtet, unverzüglich mehrere Maßnahmen zu ergreifen:

[335] Microsoft, «Microsoft Azure Well-Architected Framework – Security Design Principles«, Stand 15.11.2023, https://learn.microsoft.com/en-us/azure/well-architected/security/principles

[336] Siehe zum Thema Zero Trust Architecture bspw. PaloAltoNetworks, »What is Zero Trust Architecture (ZTA)?«, zuletzt abgerufen am 21.08.2025, https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-security-posture-management oder IBM, »What is zero trust?«, zuletzt abgerufen am 21.08.2025, https://www.ibm.com/think/topics/zero-trust

- Dazu gehört erstens, bereitgestellte Daten sowie sämtliche Kopien davon zu löschen[337].
- Zweitens muss er die Herstellung, das Angebot, die Vermarktung oder die Nutzung rechtsverletzender Waren, abgeleiteter Daten oder Dienste einstellen und, sofern verhältnismäßig, diese Waren auch vernichten[338].
- Drittens ist der betroffene Nutzer über die unbefugte Nutzung oder Offenlegung und über die ergriffenen Gegenmaßnahmen zu informieren[339].
- Schließlich hat der Datenempfänger oder Dritte die geschädigte Partei gegebenenfalls zu entschädigen[340].

Folgende in Abs. 3 genannte Missbrauchshandlungen lösen die Abhilfepflichten nach Art. 11 Abs. 2 DA aus:

- Der Datenempfänger oder Dritte haben zum Zweck der Datenerlangung falsche Informationen bereitgestellt, Täuschungs- oder Zwangsmittel eingesetzt oder Schwachstellen in der technischen Infrastruktur zum Schutz der Daten ausgenutzt[341].
- Er hat die bereitgestellten Daten für nicht genehmigte Zwecke genutzt, etwa zur Entwicklung eines konkurrierenden vernetzten Produkts im Sinne von Art. 6 Abs. 2 lit. e (lit. b) DA.
- Er hat Daten unrechtmäßig an eine andere Partei weitergegeben[342].
- Er hat die vereinbarten technischen und organisatorischen Maßnahmen gemäß Art. 5 Abs. 9 DA nicht aufrechterhalten[343].
- Oder er hat ohne Zustimmung des Dateninhabers die in Art. 11 Abs. 1 beschriebenen TPM verändert oder aufgehoben[344].

Laut Art. 11 Abs. 4 DA gelten diese Pflichten auch für Nutzer, wenn sie selbst TPM unbefugt ändern oder aufheben oder vereinbarte Maßnahmen zum Schutz von Geschäftsgeheimnissen nicht einhalten. Art. 11 Abs. 5 DA regelt zudem, dass Nutzer bei bestimmten Verstößen des Datenempfängers gegen Art. 6 Abs. 2 lit. a oder b DA dieselben Rechte wie Dateninhaber haben, um die in Art. 11 Abs. 2 DA vorgesehenen Maßnahmen durchzusetzen.

6.4.7 Rechtssichere Dokumentation

Darüber hinaus ist die Auditfähigkeit der gesamten Infrastruktur zu gewährleisten, um sämtliche Zugriffe, Änderungen und Schutzmaßnahmen lückenlos und manipulationssicher zu dokumentieren.

[337] Art. 11 Abs. 2 lit. a DA.
[338] Art. 11 Abs. 2 lit. b DA.
[339] Art. 11 Abs. 2 lit. c DA.
[340] Art. 11 Abs. 2 lit. d DA.
[341] Art. 11 Abs. 3 lit. a DA.
[342] Art. 11 Abs. 3 lit. c DA.
[343] Art. 11 Abs. 2 lit. d DA.
[344] Art. 11 Abs. 2 lit. e DA.

6.5 Interne Kommunikation & Governance

Jonas von Dall'Armi, Leiter Datenschutzrecht, Rechtsanwalt (Syndikusrechtsanwalt), CIPP/E, CIPM, FIP, Giesecke+Devrient GmbH

6.5.1 Zielsetzung

Ziel der internen Kommunikation ist es zunächst, das Bewusstsein für die Existenz des DA und seinen Regelungen im gesamten Unternehmen zu schärfen. Es ist essenziell, dass zumindest eine gewisse Grund-Awareness bei den Abteilungen vorhanden ist, die von den Auswirkungen des DA betroffen sein könnten. Die Kommunikation sollte dabei nicht nur auf die reine Informationsweitergabe beschränkt sein, sondern auch die Bedeutung des Themas für das Unternehmen hervorheben. Hierbei empfiehlt es sich, den DA nicht nur als »Herausforderung« im Sinne eines Compliance-Regelwerks, sondern auch als »Chance« zu verstehen. Schließlich dient der DA nach den Vorstellungen der EU-KOM auch der Stärkung der Wettbewerbsfähigkeit europäischer Unternehmen, indem Datensilos aufgebrochen und Verbrauchern wie Unternehmen der Zugriff auf jene Daten ermöglicht wird, deren Nutzung bislang nur den jeweiligen Herstellern vernetzter Produkte und wenigen Dateninhabern vorbehalten war. Ein umfassendes Verständnis vom DA und eine offene Kommunikationskultur fördern zudem die Akzeptanz und die Bereitschaft zur aktiven Mitwirkung im Rahmen eines sich etwaig anschließenden Implementierungsprojekts.

6.5.2 Interdisziplinäres Team

Für größere Unternehmen kann es sich anbieten, ein interdisziplinäres Team zu bilden, das die Federführung für die Aufbereitung von Informationen und die interne Kommunikation zum DA übernimmt. In diesem Team sollten Mitglieder der Abteilungen vertreten sein, die fähig sind, sowohl den DA inhaltlich als auch dessen Relevanz für das Unternehmen zu beurteilen. Darunter zählen insbesondere Rechtsabteilung, Compliance- und Datenschutzabteilung sowie ggf. Produktentwicklung, Forschungs- und Technologieabteilungen. In kleineren Unternehmen wird man häufig nicht umhinkommen, eine dezidierte Person oder gar ein Mitglied der Geschäftsführung mit der Koordination zu betrauen, da hier oft weniger spezialisierte Ressourcen zur Verfügung stehen. Primäre Aufgabe des interdisziplinären Teams oder eines/r Koordinators/in ist die Aufbereitung der DA-Informationen für die relevanten Zielgruppen und Durchführung entsprechender Informationskampagnen.

6.5.3 Relevante Stakeholder/Zielgruppe(n)

Ein zentraler Faktor für den Erfolg der Informationskampagne ist die Identifikation der Stakeholder und Zielgruppe(n) im Unternehmen. Neben der Geschäftsführung ist hier vor allem an die Unternehmensbereiche zu denken, die vom DA vorrangig betroffen sind, wie Produktentwicklung, Produktion, Forschung & Entwicklung, Einkauf und Vertrieb, Rechtsabteilung, Datenschutz, ggf. Head of Data o.ä.

Es ist ratsam, möglichst frühzeitig einen Stakeholder-Kreis zu definieren und die Aufbereitung der Informationen auf diesen Kreis auszurichten. Die Geschäftsführung sollte das Thema DA idealerweise als Priorität kommunizieren, um die notwendige Rückendeckung und Aufmerksamkeit zu gewährleisten.

6.5.4 Ausgestaltung der Informationskampagne

Zunächst kann ein initiales Kick-off-Meeting mit der Geschäftsführung ein klares Signal für die Bedeutung des Themas setzen und die Beteiligten entsprechend motivieren. Um das Thema DA für alle identifizieren Stakeholder verständlich und greifbar zu machen, empfiehlt sich ein mehrstufiger Kommunikationsansatz. Die Informationskampagne selbst sollte an der Unternehmensgröße, Anzahl der Stakeholder und ggf. am Grad der Betroffenheit ausgerichtet werden. Als erste Awareness-Maßnahme können kurze Informationsveranstaltungen, sei es in Form von Präsenz- oder Videokonferenzen, dienen, bei denen über die Zielsetzung des DA und die wesentlichen Regelungsinhalte aufgeklärt wird. Je nach Unternehmensgröße kann dies mit der Aufforderung verbunden werden, einen Ansprechpartner für die jeweilige Abteilung oder den Bereich zu benennen, der für Folgeaktivitäten zur Verfügung steht. Als Folgeaktivitäten kommen gezielte Workshops in Betracht, im Rahmen derer dezidierte Anwendungsfälle identifiziert, Hintergrundwissen vertieft und Fragen zum DA geklärt werden können. Ergänzend sind FAQ-Dokumente, Intranet-Artikel und zielgruppenspezifische Informationsmaterialien hilfreich, um die unterschiedlichen Bedürfnisse der Abteilungen zu adressieren. Die Kommunikation sollte stets transparent, verständlich und praxisnah gestaltet sein, um die Akzeptanz und das Engagement der Mitarbeitenden zu fördern.

6.5.5 Anwendungsbereich klären

Die Klärung des Anwendungsbereichs des DA ist ein zentraler Schritt bei der Implementierung. Hierzu bietet sich die Entwicklung von Checklisten an, anhand derer die jeweiligen Abteilungen bzw. Stakeholder prüfen können, ob und in welchem Umfang sie vom DA betroffen sind. Auch Entscheidungsbäume haben sich diesbezüglich in der Praxis bewährt. Die Herausforderung besteht darin, solche Checklisten so zu gestalten, dass sie allgemein verständlich und möglichst einfach vom Adressaten ausgefüllt werden können. Auch eine schrittweise Vorgehensweise kann hierfür sinnvoll sein, indem man beispielsweise zunächst die DA-relevanten Produkte und anschließend für das jeweilige Produkt die entsprechenden Produktdaten identifiziert.

Beispiel: Checkliste zur Identifikation vernetzter Produkte:

Produkt (= physisches Gerät)	Werden Daten über Nutzung oder Umgebung generiert oder erlangt?	Übertragung über elektr. Kommunikations-dienst möglich?	Übertragung über physische Verbindung möglich?	Übertragung über geräteinternen Zugang möglich?	Ausschlusskriterium: Datenspeicherung, -verarbeitung oder -übertragung für Dritte als Hauptfunktion?
Produkt 1					
Produkt 2					

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

David Schönwerth | Bereichsleiter Data Economy
T 030 27576-179 | d.schoenwerth@bitkom.org

Verantwortliches Bitkom-Gremium

AK Datenpolitik & Datenräume

Autorinnen und Autoren

Bernd Daamen, BusinessCode GmbH | Ferdinand Schwarz, Dr. Daniel Meßmer, Jan-Dierk Schaal & Franziska Wulf, SKW Schwarz Rechtsanwälte Steuerberater Partnerschaft mbB | Valentino Halim, Oppenhoff & Partner Rechtsanwälte Steuerberater mbB | Matthias Treude (YPOG GmbH & Co. KG) im Auftrag der DKE-Data GmbH und Co. KG | Filipp Revinzon, LL.M., Vay Technology GmbH | Dr. Lukas Semmelmayer, LL.B. Digital Law, ADAC e.V. | Dr. Robert Wilkens & Stina Neuenfeldt, LL.M., KPMG AG Wirtschaftsprüfungsgesellschaft | Swen Hildebrandt, Volkswagen AG | Dr. Viola Bensinger (Anwältin), Jana Rudt (Anwältin), Dr. Jannis Dietrich-Webb (Anwalt), Dr. Paul Dürr (Anwalt) & Dr. Ricarda Seifert (Anwältin), Greenberg Traurig | Florian Schwind, Tim Sauerhammer & Lukas Willecke, Reed Smith LLP | Volker Smoljko, IBM | Lukas Mehl, Telefónica Germany GmbH & Co. OHG | Oliver Zigan, ITENOS GmbH | Rainer Duda, M&M Software GmbH | David Schönwerth & Luisa Nissen, Bitkom e.V. | Tahir Mughal, MBA, Materna SE | Nancy Ngân Piechota & Paul Brings, Taylor Wessing Partnerschaftsgesellschaft mbB | Lukas Klein & Anne Untermann, Digetiers GmbH | Lisa Böhler, NTT DATA Deutschland SE | Dr. Lucas Blum & Dr. Richard Falk, LL.M. (King's College), DLA Piper UK LLP | Jonas von Dall'Armi, Giesecke+Devrient GmbH