

Einleitung

Ziele des Data Act

Der Data Act (**Datenverordnung**, „DA“)¹ soll eine faire Nutzung der Daten, die beim Verwenden eines Gerätes oder eines verbundenen Dienstes erzeugt werden, ermöglichen. Er wendet sich daher sowohl an die **Nutzer** als auch an die **Hersteller** solcher vernetzten Produkte und an die Nutzer und Anbieter von mit diesen verbundenen Diensten und Datenverarbeitungsdiensten. Die Europäische Kommission spricht davon, dass der DA die Chancen, die Daten in der Europäischen Union bieten, „entfesseln“ soll und regeln soll, wer unter welchen Bedingungen aus Daten Wert schaffen kann.² Da unter die Begriffsdefinition des „**vernetzten Produkts**“ jeglicher Gegenstand fällt, der **Daten – egal, ob personenbezogen oder nicht-personenbezogen** – über seine Nutzung oder Umgebung erlangt, generiert oder erhebt, und der Produktdaten nach außen übermitteln kann, ist der DA nicht nur auf Konsumentenprodukte wie etwa **Smartwatches, Smart-Home-Produkte** oder **Fahrzeuge**, sondern auch auf **landwirtschaftliche oder industrielle Maschinen** und die mit diesen „verbundenen Dienste“ anwendbar. Durch die fortschreitende Digitalisierung wird der Anwendungsbereich des DA faktisch immer größer werden.

Der DA regelt aber nicht nur den **Zugang zu diesen Daten**, sondern auch die **Erleichterung des Wechsels zwischen Datenverarbeitungsdiensten** wie etwa **Cloud-Diensten**, die Einführung von **Schutzmaßnahmen** gegen den unrechtmäßigen Zugang Drit-

1 VO (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), ABl L 2023/2854, 1.

2 <https://digital-strategy.ec.europa.eu/en/policies/data-act>.

Einleitung

ter zu nicht-personenbezogenen Daten und die Entwicklung von **Interoperabilitätsnormen** für Daten, die abgerufen, übertragen und genutzt werden sollen.

Inkrafttreten und Geltungsbeginn

Der DA trat am 11. 1. 2024 in Kraft und gilt ab dem **12. 9. 2025**. Die Pflicht des Art 3 Abs 1 zur Zugänglichmachung von Produktdaten und verbundenen Dienstdaten für den Nutzer gilt für vernetzte Produkte und die mit ihnen verbundenen Dienste, die nach dem 12. 9. 2026 in Verkehr gebracht werden. Eine echte Abgrenzung zu den „ohne Weiteres verfügbaren Daten“ des Art 4 Abs 1, die bereits ab dem 12. 9. 2025 zur Verfügung zu stellen sind, bleibt der DA leider schuldig. Nationale Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen werden, gelten im Hinblick auf die Pflichten der Dateninhaber des Kapitels III, Daten bereitzustellen, erst für solche Vorschriften, die nach dem 12. 9. 2025 in Kraft treten. Das Kapitel IV über missbräuchliche Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen gilt erst für Verträge, die nach dem 12. 9. 2025 geschlossen wurden. Für davor geschlossene Verträge, die unbefristet abgeschlossen wurden, oder deren Geltungsdauer frühestens am 11. 1. 2034 endet, gilt Kapitel IV erst ab dem 12. 9. 2027. Dies bedeutet, dass für befristete Verträge, die vor dem 12. 9. 2025 geschlossen wurden und die vor dem 11. 1. 2034 enden, Kapitel IV bereits ab dem 12. 9. 2025 gilt.

Verhältnis zu anderen Rechtsakten

Der DA setzt andere bestehende Rechtsvorschriften auf EU-Ebene nicht außer Kraft und greift auch nicht in die DSGVO ein. Art 1 Abs 5 DA hält ausdrücklich fest, dass, soweit Nutzer betroffene Personen iSd DSGVO sind, die in Kapitel II des DA festgelegten Rechte das Auskunftsrecht (Art 15 DSGVO) von betroffenen Personen und deren Recht auf Datenübertragbarkeit (Art 20 DSGVO) ergänzen.³ Im Falle eines Widerspruchs zwischen dem

3 Zum Verhältnis und den Unterschieden zwischen Data Act und Art 20 DSGVO siehe *Knyrim/Briegl*, Datenzugangsansprüche im Vergleich: Das Verhältnis zwischen dem Recht auf Datenportabilität (DSGVO) und dem Recht auf Datenzugang (Data Act), *Dako* 2024/49.

DA und dem Unionsrecht in Bezug auf den Schutz personenbezogener Daten bzw die Privatsphäre oder den im Einklang mit dem Unionsrecht erlassenen nationalen Rechtsvorschriften haben das Unionsrecht und/oder das nationale **Recht zum Schutz personenbezogener Daten bzw der Privatsphäre Vorrang**.

Regelungsadressaten

Der DA richtet sich an **Hersteller** vernetzter Produkte, die in der Union in Verkehr gebracht werden und **Anbieter** verbundener Dienste, unabhängig vom Ort der Niederlassung dieser Hersteller oder Anbieter. Bei einem „**vernetzten Produkt**“ handelt sich um jeglichen Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und diese Daten dann über Kommunikationsdienste oder einen physischen oder einen geräteeigenen Zugang übermitteln kann, wobei dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist. Ein „**verbundener Dienst**“ ist ein digitaler Dienst, bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt – einschließlich Software –, der zum Zeitpunkt des Kaufs, der Miete oder des Leasings so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen.

Weiters gilt die Verordnung für die **Nutzer** solcher vernetzten Produkte oder verbundenen Dienste, und ebenso für **Dateninhaber**, die Datenempfängern in der Union Daten bereitstellen, und zwar unabhängig vom Ort ihrer Niederlassung. Sowohl Nutzer als auch Dateninhaber können **natürliche oder juristische Personen** sein, was eine bedeutende Erweiterung des Anwendungsbereichs des DA im Vergleich zur DSGVO bewirkt, denn die DSGVO schützt nur natürliche Personen (das österreichische DSG hingegen nach wie vor auch juristische Personen). Auch der sachliche Anwendungsbereich des DA ist im Vergleich zur DSGVO viel größer, da die Definition von „**Daten**“ **jede digitale Darstellung**

Einleitung

von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen, auch in Form von Ton-, Bild- oder audiovisuellen Material, umfasst und sich somit nicht auf personenbezogene Daten beschränkt, sondern **auch nicht-personenbezogenen Daten umfasst**. Die Daten sind dabei auf Produktdaten und verbundene Dienstdaten beschränkt, die **nach dem Inkrafttreten des DA generiert wurden**. **Hoch angereicherte** Daten, das sind Daten, die aus Informationen gefolgert oder abgeleitet werden – insbesondere mittels komplexer proprietärer Algorithmen – fallen hingegen nicht darunter (siehe Erwägungsgrund 15).

Da der DA nicht nur den Begriff des Dateninhabers, sondern auch des **Datenempfängers** schafft, sind auch die Rollen gegenüber der DSGVO erweitert. Geht es dort nur um den Verantwortlichen, die betroffene Person und Auftragsverarbeiter, so kann ein Dateninhaber berechtigt oder verpflichtet sein, Daten (soweit vertraglich vereinbart auch Produktdaten und verbundene Dienstdaten) zu nutzen und bereitzustellen, die er während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat, und kann diese an Datenempfänger weitergeben, die natürliche oder juristische Personen sein können. Die Datenempfänger können diese Daten – ohne selbst Nutzer eines vernetzten Produkts oder verbundenen Dienstes zu sein – zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit verwenden. Datenempfänger können Dritte sein, denen der Dateninhaber auf Verlangen des Nutzers oder in Einklang mit einer rechtlichen Verpflichtung aus anderem Unionsrecht oder aus nationalen Rechtsvorschriften Daten bereitstellt.

Der DA gilt auch für **Anbieter von Datenverarbeitungsdiensten**, die unabhängig vom Ort ihrer Niederlassung Kunden in der Union solche Dienste anbieten, weiters für **Teilnehmer an Datenräumen** und **Anbieter von Anwendungen**, die **intelligente Verträge** (englisch „Smart Contracts“) verwenden oder Personen, deren berufliche Tätigkeit die Einführung intelligenter Verträge umfasst. Schließlich gilt er auch für die Europäische Kommission, die Europäischen Zentralbank und Einrichtungen der Union sowie öffentliche Stellen, die von Dateninhabern die Herausgabe

von Daten verlangen können, soweit eine außergewöhnliche Notwendigkeit der Nutzung dieser Daten zur Wahrnehmung einer speziellen Aufgabe im öffentlichen Interesse besteht.

Der DA enthält verschiedene **Ausnahmen für Klein- und Kleinstunternehmen**.

Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

Der DA schreibt vor, dass vernetzte Produkte und mit ihnen verbundene Dienste, die nach dem 12. 9. 2026 in Verkehr gebracht werden, so konzipiert und hergestellt werden müssen, dass die Produkt- und verbundenen Dienstdaten einschließlich der relevanten Metadaten standardmäßig für den Nutzer **einfach, sicher, unentgeltlich** in einem umfassenden, strukturierten, **gängigen und maschinenlesbaren Format** und, **soweit relevant und technisch durchführbar, direkt zugänglich gemacht werden müssen** (Art 3 iVm Art 50, „**Accessibility by Design**“). Wie bereits gesagt, umfasst der Begriff Produkte hier sämtliche, das heißt – im Gegensatz zur DSGVO – auch nicht-personenbezogene Daten. Bis 12. 9. 2025 müssen Hersteller entscheiden, ob sie einen **direkten oder indirekten Datenzugang** generieren.⁴ Direkt bedeutet, dass User die Daten selbst, dh ohne Involvierung des Dateninhabers, entweder aus dem Gerät oder einem Server herunterladen oder streamen können. Indirekt bedeutet, dass er den Dateninhaber um Zugang bitten muss, also ein Genehmigungsprozess eingerichtet ist.

Der bereits ab 12. 9. 2025 anwendbare Art 4 Abs 1 bestimmt, dass die **Dateninhaber** dem Nutzer, soweit er nicht direkt vom vernetzten Produkt oder verbundenen Dienst auf die Daten zugreifen kann, die ohne Weiteres verfügbaren Daten (einschließlich Metadaten) auf sein einfaches Verlangen hin unverzüglich, **einfach, sicher, unentgeltlich** in einem umfassenden, gängigen und **maschinenlesbaren Format** und – falls relevant und technisch verfügbar – in der gleichen Qualität wie für den Dateninha-

4 Europäische Kommission, Frequently Asked Questions, Data Act, Version 10 v. 6. 9. 2024, Punkt 19.

Einleitung

ber **kontinuierlich und in Echtzeit** bereitstellen muss („**Accessibility by Request**“).

Zusätzlich kommt mit dieser technischen Verpflichtung auch eine **Informationspflicht**. Vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein vernetztes Produkt oder eines Vertrags für die Erbringung eines verbundenen Dienstes muss der Verkäufer, Vermieter oder Leasinggeber – wobei es sich auch um den Hersteller handeln kann – bzw der Anbieter des verbundenen Dienstes dem Nutzer zahlreiche Informationen in klarer und verständlicher Weise bereitstellen. Diese Informationen umfassen ua **Art, Format und geschätzten Umfang der Daten, die das Produkt generieren kann**, die Angabe, ob die Daten **kontinuierlich und in Echtzeit** generiert werden und ob die Daten auf einem **Gerät oder einem entfernten Server gespeichert werden**, inklusive der vorgesehenen **Speicherdauer**; weiters Angaben dazu, wie der Nutzer auf die Daten **zugreifen**, sie abrufen oder gegebenenfalls löschen kann, einschließlich der technischen Mittel, die dafür notwendig sind, sowie die betreffenden Nutzungsbedingungen und die betreffende Dienstqualität.

Bei verbundenen Diensten muss ebenfalls über Art, Umfang und Häufigkeit der Erhebung der Produktdaten und ebenso der zu generierenden verbundenen Dienstdaten sowie die Modalitäten für Zugriff und Abruf und zahlreiche weitere Details informiert werden.

Der **Datenzugang** kann vom Nutzer und Dateninhaber **beschränkt werden**, wenn dieser die im Unionsrecht oder im nationalen Recht festgelegten Sicherheitsanforderungen des vernetzten Produkts beeinträchtigen und damit zu schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen führen könnte (sogenannte „**Sicherheits-Handbremse**“). Die Mitgliedsstaaten müssen eine Behörde benennen, an die der Dateninhaber seine Weigerung zur Datenweitergabe meldet.

Dateninhaber dürfen digitale Benutzerschnittstellen nicht so gestalten, dass sie durch ihre Struktur, Gestaltung oder Funktion die **Wahlfreiheit** des Nutzers oder dessen Autonomie oder Entschei-

dungsfreiheit **unterlaufen** oder beeinträchtigen, auch nicht dadurch, dass sie den Nutzern nicht neutrale Wahlmöglichkeiten anbieten.

Der Nutzer kann neben einem **gerichtlichen Rechtsmittel** im Mitgliedsstaat bei einer Streitigkeit über eine Zugangsbeschränkung eine national zuständig zu machende Behörde anrufen oder die **Streitbelegungsstelle** nach Art 10 befassen.

Geschäftsgeheimnisse müssen gewahrt bleiben und dürfen nur offengelegt werden, wenn vom Dateninhaber oder vom Nutzer ausreichende technische und organisatorische (auch vertragliche) Maßnahmen zu deren Schutz getroffen wurden. Es besteht auch die Möglichkeit, diesbezüglich Datenherausgaben aus bestimmten Gründen zu verweigern. Dies ist aber der national zuständigen Behörde mitzuteilen und dagegen kann wieder mittels gerichtlichem Rechtsmittel, Beschwerde bei der Behörde oder Anrufung der Streitbelegungsstelle des Art 10 vorgegangen werden.

Insbesondere für **Start-ups und Entwickler neuer Produkte** ist Art 4 Abs 10 zu beachten, laut dem ein Nutzer die erlangten Daten weder zur Entwicklung eines vernetzten Produkts nutzen darf, das mit dem vernetzten Produkt, von dem die Daten stammen, **im Wettbewerb steht**, noch diese Daten mit dieser Absicht an einen Dritten weitergeben oder nutzen darf, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers oder Dateninhabers zu erlangen. Bei **Produktentwicklungen** ist also Vorsicht geboten, um nicht in dieses Verbot zu fallen. Diese Bestimmung gilt ausdrücklich nur bei der Entwicklung, nicht hingegen beim späteren Betrieb eines vernetzten Produkts. Weiters ist die Bestimmung auf vernetzte Produkte beschränkt, die Entrichtung von im Wettbewerb stehenden verbundenen Diensten ist allerdings bewusst nicht untersagt worden, um diesbezüglich den Wettbewerb zu beleben.⁵

Dem Nutzer ist es im Übrigen auch ganz allgemein verboten, **Zwangsmittel** einzusetzen oder **Lücken** in der zum Schutz der

5 Europäische Kommission, Frequently Asked Questions, Data Act, Version 10 v. 6. 9. 2024, Punkt 23.

Einleitung

Daten bestehenden technischen Infrastruktur eines Dateninhabers auszunutzen, um Zugang zu den Daten zu erlangen.

Sollte es sich bei den betroffenen Daten um **personenbezogene Daten** handeln und der Nutzer nicht die betroffene Person sein, so darf der Dateninhaber die Daten dem Nutzer nur dann bereitstellen, wenn es für die Verarbeitung eine gültige Rechtsgrundlage gibt und die Bedingungen des Art 9 DSGVO (betrifft die Nutzung von besonderen Datenkategorien) und ebenso des Art 5 Abs 3 RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation, Regelungen über den Zugriff auf Informationen auf Endgeräten eines Nutzers) erfüllt sind.

Dateninhaber dürfen „ohne weiteres verfügbare Daten“ nur auf Grundlage eines **Vertrags mit dem Nutzer** nutzen. Dritten dürfen Dateninhaber nicht-personenbezogene Produktdaten zu keinen anderen kommerziellen oder nicht-kommerziellen Zwecken als zur Erfüllung ihres Vertrages mit dem Nutzer bereitstellen.

Art 5 gibt dem Nutzer ein **Recht auf Weitergabe von Daten an Dritte**. Der Nutzer oder eine für ihn handelnde Partei kann dabei verlangen, dass der Dateninhaber die ohne weiteres verfügbaren Daten und erforderlichen Metadaten unverzüglich und für den Nutzer unentgeltlich in derselben Qualität, die dem Dateninhaber zur Verfügung steht, einem Dritten bereitstellt (Art 5 Abs 1, „Data Portability upon Request“). Dies **ebenfalls** zu denselben „Bedingungen“ wie ihm selbst, also einfach, sicher, in einem strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, kontinuierlich und in Echtzeit. Der DA macht hier einen Querverweis in Richtung des Digital Markets Act und hält fest, dass die dort als „**Torwächter**“ benannten Unternehmen **nicht als Dritte** iSd vorgenannten Bestimmung anzusehen und diese daher nicht berechtigt sind, Nutzer aufzufordern, ihnen ihre Daten bereitzustellen. Auch zur DSGVO gibt es wieder einen Querverweis: Wenn der Nutzer nicht selbst die betroffene Person ist, so müssen für die Nutzung personenbezogener Daten eine **Rechtsgrundlage gem Art 6 DSGVO** vorhanden und die Bedingungen des Art 9 DSGVO und ebenfalls wieder die Bestimmungen zum

Zugriff auf Endgeräte iSd Richtlinie über elektronische Kommunikation erfüllt sein.

Die Ausübung der **Betroffenenrechte**, insbesondere des **Rechts auf Datenübertragbarkeit des Art 20 DSGVO**, darf nicht durch Versäumnisse des Dateninhabers oder des Dritten, Vorkehrungen für die Übermittlung der Daten zu treffen, behindert, verhindert oder beeinträchtigt werden. Für nicht-personenbezogene Daten schafft der DA aber kein Löschrecht, ein solches muss zwischen den Parteien vertraglich vereinbart werden. Bei der Weitergabe von Daten an Dritte müssen **Geschäftsgeheimnisse** gewahrt werden und es kann daher die Datenweitergabe auch verweigert oder ausgesetzt werden, was wiederum durch gerichtliches Rechtsmittel, Beschwerde bei der Behörde oder Befassung der Streitbeilegungsstelle des Art 10 bekämpft werden kann.

Art 6 bestimmt, dass **Dritte, die die Daten auf Verlangen des Nutzers erhalten**, nur zu den Zwecken und unter den Bedingungen, **die sie mit dem Nutzer vertraglich vereinbart haben, verarbeiten dürfen**, bei personenbezogenen Daten entsprechend der DSGVO. Die Dritten dürfen den Nutzer bei Wahlmöglichkeiten wiederum nicht beeinflussen oder behindern, und sie dürfen die erhaltenen Daten unbeschadet Art 22 Abs 2 lit a und c DSGVO **nicht für Profiling nutzen**, es sei denn, dies ist erforderlich, um den vom Nutzer gewünschten Dienst zu erbringen. Weiters dürfen sie die Daten **nicht einem Dritten bereitstellen**, es sei denn, die Daten werden auf der Grundlage eines Vertrags mit dem Nutzer bereitgestellt. Überdies ist es dem Dritten untersagt, die Daten einem **Torwächter** iSd DMA bereitzustellen oder – siehe dazu schon oben – die erhaltenen Daten zu nutzen, um ein **Produkt zu entwickeln**, dass mit dem vernetzten Produkt, von dem die Daten stammen, **im Wettbewerb steht**, oder die Daten zu diesem Zweck an einen anderen Dritten weiterzugeben. Umgekehrt ist es dem Dritten aber nicht erlaubt, einen Nutzer, der Verbraucher ist, daran zu hindern (auch auf Grundlage eines Vertrages), die erhaltenen Daten anderen Parteien bereitzustellen.

Alle davor genannten Pflichten der Art 3 bis 6 gelten nach Art 7 jedoch nicht für Daten, die bei der Nutzung von vernetzten Pro-

Einleitung

dukten generiert werden, die von einem **Klein- oder Kleinstunternehmen** hergestellt oder konzipiert werden oder die bei der Nutzung von verbundenen Diensten generiert werden, die von einem solchen Unternehmen erbracht werden. Dies ist aber nicht anwendbar, sofern es sich bei diesen Klein- oder Kleinstunternehmen um ein **Partnerunternehmen** oder ein **verbundenes Unternehmen** iSd Art 3 des Anhangs der Empfehlung 2003/361/EG (betrifft die Definition der KMU in der EU) handelt und sofern das Klein- oder Kleinstunternehmen nicht als **Unterauftragsnehmer** mit der Herstellung oder der Konzeption eines vernetzten Produkts oder der Erbringung eines verbundenen Dienstes beauftragt wurde. Das gleiche gilt für Daten, die durch die Nutzung von vernetzten Produkten generiert werden, die von einem Unternehmen hergestellt werden, das seit weniger als einem Jahr als Mitglied eines Unternehmens des Art 2 der vorgenannten Empfehlung eingestuft ist oder für verbundene Dienste, die von einem solchen Unternehmen erbracht werden, und für vernetzte Produkte für ein Jahr nach dem Zeitpunkt ihres In-Verkehr-Bringens durch ein **mittleres Unternehmen**. Der DA nimmt somit – im Vergleich zu anderen, bisher in dieser Publikationsserie bearbeiteten Digitalisierungsrechtsakte – auch mittlere Unternehmen, die gerade erst von einem Kleinunternehmen zu solchen geworden sind, für ein Jahr aus.

Pflichten der Dateninhaber, die verpflichtet sind, Daten bereitzustellen

Ist ein Dateninhaber nach Art 5 (oder nach anderem Unionsrecht oder nationalem Recht) **verpflichtet, Daten bereitzustellen**, so muss er diese zu **fairen, angemessenen und nicht-diskriminierenden Bedingungen in transparenter Weise** bereitstellen (Art 8 Abs 1). Ein Dateninhaber darf daher in Bezug auf die Modalitäten der Bereitstellung von Daten nicht zwischen vergleichbaren Kategorien von Datenempfängern diskriminieren (Art 8 Abs 3).

Art 8 Abs 4 hält fest, dass Daten einem Datenempfänger nur dann bereitgestellt werden dürfen, wenn der Nutzer dies entsprechend Art 3 ff verlangt hat. Ist dies der Fall, so darf der Dateninhaber vom Datenempfänger für die Bereitstellung von Daten im Rahmen von Geschäftsbeziehungen zwischen Unterneh-