# Data Act – Das Datengesetz für Unternehmen

## FAQ vom Webinar der Bundessparte Information und Consulting, WKÖ

## vom 11. Dezember 2025 von 15:30 bis 16:30 Uhr

Inhalt

## 1. Wechsel zwischen Datenverarbeitungsdiensten

**Kurz:** Ein „Datenverarbeitungsdienst“ (Artikel (Art) 2 Abs. 8 der Datenverordnung (DA)) ist eine digitale Dienstleistung, die bedarfsgerechten Netzwerkzugang zu einem Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen ermöglicht, die dynamisch und effizient zugewiesen, angepasst oder freigegeben werden können. Die technische Elastizität und Automatisierung der Rechenkapazität ist hier relevant (vgl Erwägungsgrund (ErwGr) 80 DA). Die Begriffsdefinition ist unbestimmt, da sie allein nicht klärt, welche Dienstleistungen darunterfallen. Grundsätzlich umfasst sie eine breite Palette von Diensten, die den Modellen Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) zugeordnet werden können (ErwGr 80 DA). SaaS-Anbieter sind besonders betroffen, da sie intensiv mit Kundendaten und Geschäftsprozessen interagieren, was Fragen zur Datenherausgabe bei Anbieterwechseln aufwirft. Die DA verlangt von Anbietern die Bereitstellung maschinenlesbarer Datenformate, die Beseitigung von Wechselhindernissen, verpflichtende Vertragsklauseln, Informationspflichten sowie technische Umsetzungen wie API, um den Wechsel für Kunden zu erleichtern (s auch Art. 30 und 31 DA). Diese verhindern eine missbräuchliche Umgehung der Wechselpflichten durch komplexe Onboarding-Verfahren.

Die in Art. 2 Abs. 8 DA enthaltene Legaldefinition eines Datenverarbeitungsdienstes beschreibt diesen als eine digitale Dienstleistung, die einen bedarfsgerechten Netzwerkzugang zu einem gemeinsamen Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen ermöglicht. Die in der Norm verwendeten Begriffe „schnell bereitgestellt und freigegeben“ sowie „mit minimalem Verwaltungsaufwand oder minimaler Interaktion mit dem Dienstanbieter“ sind als technische Merkmale dieser Rechenressourcen zu verstehen. Sie beziehen sich insbesondere auf deren Fähigkeit, dynamisch und effizient zugewiesen, angepasst oder freigegeben zu werden.

Diese Auslegung wird durch ErwG 80 S 6 DA bestätigt, wonach der Begriff „elastisch“ Rechenressourcen beschreibt, die je nach Bedarf bereitgestellt und freigegeben werden können, um die verfügbaren Ressourcen abhängig von der jeweiligen Arbeitslast kurzfristig zu erhöhen oder zu verringern. Damit bezieht sich die Definition auf die technische Elastizität und Automatisierung der Rechenkapazität und nicht auf die wirtschaftlichen oder betrieblichen Einsatzbedingungen eines Softwaredienstes, der dem Kunden unmittelbar zur Nutzung bereitgestellt wird.

Diese Begriffsdefintion von „Datenverarbeitungsdiensten“ ist kryptisch gestaltet, da man nur allein mit dieser noch nicht abschließend einordnen kann, welcher unter die Definition einen Datenverarbeitungsdienstes fällt und wer nicht. Gemäß ErwG 81 S 1 und 2 DA werden eine beträchtliche Zahl von Diensten mit einer sehr großen Bandbreite an unterschiedlichen Anwendungszwecken, Funktionen und technischen Strukturen, umfasst. Nach allgemeinem Verständnis von Anbietern und Nutzern und im Einklang mit weit verbreiteten Standards fallen Datenverarbeitungsdienste unter eines oder mehrere der folgenden drei Modelle für die Bereitstellung von Datenverarbeitungsdiensten, nämlich „Infrastructure-as-a-Service“ (IaaS), „Platform-as-a-Service“ (PaaS) und „Software-as-a-Service“ (SaaS).

Folglich sind auch Anbieter von Software-as-a-Service (SaaS), deren Dienstleistungen eine gewisse Konfiguration oder Anpassung erfordern (bspw die Einrichtung von Benutzerkonten, die Implementierung von Branding-Elementen oder die Integration standardisierter

Funktionen) als Datenverarbeitungsdienste im Sinne des Art. 2 Abs. 8 DA zu qualifizieren. Maßgeblich ist, dass die betreffende Dienstleistung die in der Definition genannten technischen Merkmale erfüllt und keine Anhaltspunkte für eine individuell entwickelte Softwarelösung bestehen (s. die Ausnahme in Art 31 DA) .

Bei den verschiedenen Cloud-Modellen, wie in ErwG 81 DA genannt, sind die SaaS-Anbieter die am stärksten betroffenen, da diese eng mit den Kundendaten und den Geschäftsprozessen verknüpft sind. Vergleicht man diese mit klassischen Infrastruktur- oder Plattform-Anbietern, bei denen Rechner- oder Speicherkapazitäten bereitgestellt werden, wird bei SaaS-Anbieter nicht nur die Speicherung angeboten, sondern werden die Kundendaten ständig zu bestimmten Zwecken verarbeitet, verknüpft, bereichert und (weiter-)generiert. Es bleibt noch fraglich, welche konkreten Daten beim Anbieterwechsel herausgeben werden müssen, man muss hier die Verträge im Einzelfall genau detailliert prüfen.

Das theoretische Zugangsrecht zu den Daten ist in der Praxis nicht einfach umzusetzen, da auch der technische Aspekt eine große Rolle spielt.

Was ein gängiges maschinenlesbares Format ist, hängt sehr stark von der technischen Komponente und Sektor ab, wie hier Daten heraus- bzw weitergegeben werden.

Hauptpflichten für die Anbieter (nach Kapitel 6) sind:

- maschinenlesbare Datenformate;
- Beseitigung der (wesentlichen) Hindernisse: Der Wechsel muss dem Kunden so einfach wie möglich gestaltet werden;
- Verpflichtende Vertragsklauseln;
- Unanwendbarkeit spezifischer nachteiliger Klauseln (B2B und B2C, vgl AGB-Recht);
- Informationspflichten (Art 26);
- rechtzeitige, transparente und verständliche Informationspflicht über das Wechselverfahren gegenüber Kunden (konkrete Ausgestaltung, Entgelte);
- stufenweiser Abbau von Wechselentgelte;
- Technischen Umsetzungen (Art 30); es sollen APIs bereitgestellt werden, zB wird das ein Download-Button und bekomme die Daten sofort zur Verfügung gestellt.

## 2. Sind mehrjährige SaaS Verträge nicht mehr zulässig?

Kurz: Mehrjährige SaaS-Verträge sind weiterhin erlaubt. Der Data Act verbietet jedoch eine Vertragslaufzeit ohne Kündigungsmöglichkeit. Anbieter müssen ihre Geschäftsmodelle zwischen Flexibilität und Wirtschaftlichkeit neu ausbalancieren.

Der Data Act verbietet nicht mehrjährige SaaS-Verträge abzuschließen. Der DA sieht keine ständige Kündigungsmöglichkeit vor, aber vertragliche Regelungen wie zB „12 oder 24 Monate-“ Vertragslaufzeit ohne Kündigungsmöglichkeit sind nach DA nicht mehr erlaubt.

Anbieter von SaaS müssen jetzt kreativ werden und ihre Geschäftsmodelle zwischen Flexibilität und Wirtschaftlichkeit anpassen, um wettbewerbsfähig und attraktiv für alle Kunden sein zu können.

3. Muss jeder Kunde nach einem Jahr mit zweimonatiger Vorlaufzeit kündigen können?

Kurz: Eine maximale Kündigungsfrist von 2 Monaten muss vertraglich vereinbart werden. Innerhalb dieser 2 Monate und zusätzlicher 30 Tage Umsetzungsfrist muss der Datentransfer erfolgen. Bei technischer Undurchführbarkeit können bis zu 7 Monate gewährt werden, diese erfordern aber eine gute Begründung binnen 14 Tagen. Anbieter müssen nach 2 Monaten Kündigungsfrist den Vertrag beenden und beim Datentransfer mitwirken.

Eine vertragliche Klausel zur Kündigungsfrist darf eine für den Wechsel maximale Kündigungsfrist von 2 Monaten vorsehen (Art 25 Abs 2 lit d DA). Zusätzlich besteht eine Umsetzungsfrist von 30-Tagen für den Datentransfer. Ein SaaS-Anbieter bzw alle Clouddienste-Anbieter sind verpflichtet, diese Beendigungsmöglichkeit für Kunden vorzusehen. Es muss dem Kunden die Möglichkeit gegeben werden den Anbieter zu wechseln, wenn dieser das wünscht und möchte.

Art 25 Abs 4 Da berechtigt Anbieter bei technischer Undurchführbarkeit des verbindlich Übergangszeitraumes nach Abs 2 lit a auf max. 7 Monaten auszudehnen. Hierüber sind die Kunden jedoch binnen 14 Tagen hinzuweisen. Es muss begründet werden, warum es technisch nicht möglich ist.

4. Ab wann gilt die allfällige Regelung?

Kurz: Der Data Act ist seit 11. Januar 2024 in Kraft. Seit 12. September 2025 ist er vollständig anwendbar. Ab 12. Januar 2027 sind Wechselentgelte verboten.

Unternehmen müssen ihre Verträge überprüfen, veraltete Klauseln identifizieren und technische Lösungen für Datenportabilität entwickeln.

Der Data Act ist seit 11. Jänner 2024 in Kraft, somit gilt mit der Übergangsbestimmung in Art 50 DA, dass Clouddienst-Anbieter noch ein geringes Wechselentgelt verlangen dürfen, dies ist ab dem 12. Jänner 2027 vorbei, denn ab da dürfen keine Wechselentgelte mehr eingehoben werden. In Geltung ist der Data Act seit dem 12. September 2025.

Unternehmensintern müssen Vertragsklauseln auf ihre Zulässigkeit geprüft werden. Weiters muss auch technisch überprüft bzw gelöst werden, wie Switches und Datenportabiliät gewährleistet werden können.

5. Gelten die Regelungen für SaaS nur dann, wenn es nicht mit erheblichen Implementierungsaufwand verbunden ist? Bspw benötigt die Implementierung eines CRM im Betrieb wesentliche Zeit und Aufwand.

Kurz: Wechselregelungen erfasst alle standardisierten, skalierbaren Cloud-Services – unabhängig von zusätzlichen Beratungs- oder Customizing-Leistungen. Maßgeblich ist, ob das Produkt standardisiert am Markt angeboten wird. Ausgenommen sind nur Dienste, die speziell für einen einzelnen Kunden entwickelt wurden und nicht als wiederverwendbares Produkt vermarktet werden. Ein CRM mit monatelangem Onboarding und Customizing kann trotzdem darunter fallen, sofern das Basisprodukt standardisiert ist.

Kapitel 6 des Data Act erfasst alle Datenverarbeitungsdienste, die typischerweise Cloud-Services anbieten und auf Abruf bereitgestellt und wieder freigegeben werden können. Ob der einzelne Kunde zusätzliche Beratungs- oder Customizing-Leistungen benötigt, ist für die

grundsätzliche Anwendbarkeit zunächst nicht entscheidend. Maßgeblich ist, ob das Produkt als solches standardisiert und skalierbar angeboten wird. Ausgenommen sind „custom-built for a single customer“ Dienste - wenn wesentliche Komponenten speziell für einen Kunden entwickelt werden und der Dienst nicht im Katalog des Anbieters am Markt skaliert angeboten wird (Art 31 DA). Nur wenn das CRM im Wesentlichen als Einzellösung maßgeschneidert entwickelt und nicht als wiederverwendbare Cloud-Produkte am Markt angeboten wird, spricht vieles dafür, dass Kapitel 6 nicht anwendbar ist.

SaaS-Dienste iSd Data Act können typischerweise mit minimalem Aufwand/Interaktion „schnell“ bereitgestellt werden, was praktisch „fast sofort nutzbar“ bedeutet (s. FAQ der Europäischen Kommission Q 58a zu SaaS). Manche SaaS sind wegen umfangreichen Onboardings (Konfiguration/Integrationen) nicht unmittelbar nach Zahlung einsatzbereit und kann die Implementierung Tage bis Monate dauern. Insgesamt spricht die Systematik (v.a. Art. 31 DA) dafür, dass der Gesetzgeber grundsätzlich alle SaaS erfassen will – ausgenommen vor allem kundenspezifische Einzellösungen, die nicht breit über den Servicekatalog angeboten werden („Datenverarbeitungsdienste, deren Hauptmerkmale mehrheitlich speziell auf die besonderen Bedürfnisse eines einzelnen Kunden zugeschnitten sind oder deren Komponenten alle für die Zwecke eines einzelnen Kunden entwickelt wurden und die nicht in großem kommerziellen Umfang über den Dienstleistungskatalog des Anbieters von Datenverarbeitungsdiensten angeboten werden“).

6. Gibt es Empfehlungen odgl., wie SaaS-Anbieter mit den Vorgaben von Kapitel VI, insbesondere mit dem zu vereinbarenden 2-monatigen Sonderkündigungsrecht für Kunden (Art. 25 Abs. 2 lit. d) umgehen können? Das Sonderkündigungsrecht läuft offensichtlich dem Konzept langfristiger Kundenbindungen, denen dafür im Gegenzug günstigere Konditionen eingeräumt werden können, zuwider.

Kurz: SaaS-Anbieter sollten alternative Kompensationsmodelle entwickeln, die sich sachlich rechtfertigen lassen (denkbar wären einmalige Setup-Gebühren, Implementierungskosten oder Gebühren für Zusatzleistungen). Diese sind zulässig, sofern sie nicht als Wechselhindernisse fungieren. Vertragsklauseln für wirtschaftlich gerechtfertigte Kompensation bei vorzeitigem Ausstieg sind beschränkt zulässig. Zentral ist Transparenz: Alle Entgelte und Zusatzkosten müssen klar kommuniziert sein. Der Wechselprozess sollte kundenfreundlich gestaltet und die Beziehung während der Laufzeit attraktiv bleiben.

SaaS-Anbieter können uU im Hinblick auf die gesetzlich vorgesehene zweimonatige Kündigungsfrist nach dem Data Act geeignete Kompensationsmodelle entwickeln, um die Kundenbindung weiterhin sicherzustellen. Angesichts der veränderten rechtlichen Rahmenbedingungen ist nachvollziehbar, dass eine wirtschaftliche Neubewertung des Geschäftsmodells erforderlich wird. Dabei ist zu prüfen, ob alternative Entgeltstrukturen geschaffen werden können, die nicht im Widerspruch zu den Vorgaben des Data Act stehen.

So kann etwa die Einführung von einmaligen Einrichtungs- oder Setup-Gebühren, Kosten für Implementierung, Hardware oder zusätzliche Dienstleistungen ein zulässiges Mittel sein, um bereits entstandene Aufwendungen zu decken. Ebenso können vertragliche Kompensationsklauseln vorgesehen werden, die bei einem vorzeitigen Vertragsausstieg während einer vereinbarten Mindestlaufzeit greifen, sofern diese keine unzulässigen Wechselhindernisse im Sinne des Art. 23 DA darstellen. Diese können zB den tatsächlichen Schaden abdecken, dh auch Ersparungen müssen eingerechnet werden. Ein Entgelt in Höhe

des Restentgelts, ohne Ersparungen abzuziehen, kann als Wechselhindernis gesehen werden, und wäre daher unzulässig. Bei der Ausgestaltung etwaiger Vertragsstrafen ist besondere Vorsicht geboten, um sicherzustellen, dass diese nicht gegen die Grundsätze der Verordnung verstoßen.

Zentral bleibt die Transparenz gegenüber dem Kunden: sämtliche Entgelte, Gebühren und Zusatzkosten sind klar, verständlich und offen zu kommunizieren. Darüber hinaus sollte der Anbieter den Wechselprozess so kundenfreundlich wie möglich gestalten und die vertragliche Beziehung für den Kunden während der Laufzeit attraktiv halten, um Abwanderungen zu vermeiden.

Klauseln, die auf einer sachlichen, wirtschaftlich gerechtfertigten Kompensation beruhen, können in diesem Zusammenhang grundsätzlich zulässig bleiben, sofern sie keine wesentlichen oder missbräuchlichen Hindernisse für den Anbieterwechsel begründen. Wechselt ein Kunde beispielsweise von einem Anbieter zu einem anderen, obliegt es dem bisherigen Anbieter kraft seiner Mitwirkungspflichten, den Wechsel technisch und organisatorisch bestmöglich zu unterstützen.

In der Praxis können sich dabei Konflikte ergeben, etwa wenn der Anbieter die Umsetzungsfrist von bis zu sieben Monaten ausschöpft (Art. 23 Abs. 2 DA), während der Kunde einen rascheren Wechsel anstrebt. Solange die Datenübertragung nicht abgeschlossen oder die Daten endgültig gelöscht sind, besteht in diesen Fällen die vertragliche Zahlungspflicht fort. Die zweimonatige Frist ist daher nicht als starre Kündigungsfrist, sondern vielmehr als Wechselankündigungsfrist zu verstehen, die von beiden Parteien mit einem gewissen Maß an Flexibilität gehandhabt werden sollte – insbesondere in der Anfangsphase der praktischen Umsetzung des Data Act.

7. Muss das Zugangsrecht zu „Rohdaten“ in jedem Fall gewährt werden oder kann etwaig mit Datensparsamkeit iSd DSGVO argumentiert werden? Im Konkreten müssten wir, um Daten dem Unternehmen zuordnen zu können, abspeichern, welche Daten von welcher Quelle und welchem Unternehmen erhoben wurde. Ein direkter Zugang ist derzeit nicht möglich, bzw würde künftig in der Softwareentwicklung teuer sein. Es handelt sich um IOT in der predictive maintenance.

Kurz: Das Zugangsrecht zu Rohdaten muss grundsätzlich gewährt werden – auch im IoT-Umfeld. Datensparsamkeit nach DSGVO begründet kein generelles Zugangsverbot. Rohdaten können personenbezogen oder nicht-personenbezogen sein. Bei nicht-personenbezogenen Daten findet die Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) keine Anwendung. Bei personenbezogenen Daten gelten DSGVO-Bestimmungen mit Vorrang. Das Prinzip „Access by Design" verlangt, dass Datenzugang technisch ermöglicht wird. Eine pauschale Verweigerung des Datenzugangs mit Hinweis auf das Prinzip der Datensparsamkeit ist unzulässig.

Rohdaten können sowohl personenbezogene als auch nicht personenbezogene Daten darstellen, je nachdem, ob sie sich auf eine identifizierte oder identifizierbare natürliche Person beziehen und damit unter den Anwendungsbereich der DSGVO fallen. Der Data Act definiert „Daten“ weit gefasst als jede digitale Darstellung von Handlungen, Tatsachen oder Informationen, einschließlich Ton-, Bild- und audiovisueller Inhalte sowie entsprechender Zusammenstellungen (Art 2 Z 1 DA). Erfasst werden insbesondere Roh- und vorverarbeitete

Daten, die aus der Nutzung vernetzter Produkte oder verbundener Dienste entstehen und dem Dateninhaber ohne unverhältnismäßigen Aufwand zugänglich sind.

In der praktischen Anwendung handelt es sich bei Rohdaten um sogenannte Primärdaten, die unmittelbar beim Betrieb eines Produkts oder Dienstes generiert werden, etwa durch Sensoren, Nutzungsprotokolle oder Interaktionen mit digitalen Assistenten. Diese Daten können sowohl rein technische Messwerte ohne Personenbezug als auch Informationen mit Personenbezug umfassen. Dateninhaber haben daher im Rahmen interner Prüfprozesse eine klare Trennung zwischen personenbezogenen und nicht personenbezogenen Daten sicherzustellen. Soweit möglich, sind diese unterschiedlichen Datenkategorien getrennt zu speichern, sofern keine rechtfertigenden Gründe entgegenstehen. Im Bereich der nicht personenbezogenen Daten findet das Prinzip der Datenminimierung (Art 5 Abs 1 lit c DSGVO) keine unmittelbare Anwendung.

Sobald Rohdaten jedoch eine identifizierte oder identifizierbare Person betreffen, gelten die Bestimmungen der DSGVO uneingeschränkt. In einem Konfliktfall geht die DSGVO der Data-Act-Regelung vor. Das Zugangsrecht zu Rohdaten nach Art 4 Abs 1 DA muss gleichwohl grundsätzlich gewährt werden – unentgeltlich, in einem strukturierten, gängigen und maschinenlesbaren Format sowie möglichst in Echtzeit und kontinuierlich. Dies gilt auch für IoT-Daten, etwa im Kontext vorausschauender Wartungssysteme (Predictive Maintenance).

Der Data Act begründet dabei keine eigenständige Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Jede Datenverarbeitung, einschließlich der Weitergabe von Daten an Nutzer oder durch sie benannte Dritte, bedarf einer eigenständigen datenschutzrechtlichen Rechtfertigung nach der DSGVO. Die Vorrangstellung der DSGVO führt nicht zwingend zum Ausschluss des Zugangsrechts, sondern verpflichtet vielmehr zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen wie Anonymisierung, Pseudonymisierung oder Zugriffsbeschränkungen. Eine pauschale Verweigerung des Datenzugangs mit Hinweis auf das Prinzip der Datensparsamkeit ist daher unzulässig.

Zudem fördert der Data Act sogenannte „Access by Design“-Konzepte. Vernetzte Produkte und Dienste sind so zu gestalten, dass ein Datenzugang technisch von vornherein möglich ist. Ist ein direkter Zugang aus technischen oder wirtschaftlichen Gründen nicht realisierbar, muss zumindest eine alternative Lösung zur Datennutzbarmachung vorgesehen werden.

Zur Umsetzung des Zugangsrechts kann die Speicherung und Nutzung von Metadaten oder Zuordnungsinformationen erforderlich sein, um die Herkunft und Zuordnung der Daten eindeutig zu identifizieren. Eine derartige Verarbeitung ist zulässig und wird im Rahmen der Auslegung des Data Act als notwendige Maßnahme angesehen, soweit dabei die Anforderungen der DSGVO eingehalten werden.

### 8. Fallen Cloud-Lösungen jedenfalls unter „verbundene Dienste“ iS der Begriffsdefinitionen?

Kurz: Cloud-Lösungen fallen nicht automatisch unter „verbundene Dienste". Sie werden idR als „Datenverarbeitungsdienste" (IaaS, PaaS, SaaS) eingestuft (Art. 2 Z. 8 DA). Verbundene Dienste sind digitale Dienste, die so eng mit einem vernetzten Produkt verknüpft sind, dass dieses ohne sie wesentliche Funktionen nicht ausführen kann. Nur ausnahmsweise – wenn eine Cloud-Lösung für die Funktionsfähigkeit eines vernetzten Produkts zwingend erforderlich ist – kann sie als verbundener Dienst gelten.

Cloud-Lösungen fallen nicht automatisch unter den Begriff der „verbundenen Dienste“ im Sinne der Begriffsdefinitionen nach dem Data Act und sind daher rechtlich eigenständig zu behandeln. Verbundene Dienste im Sinne des Artikels 2 Ziffer 6 Data Act sind digitale Dienste, die so eng mit einem vernetzten Produkt verknüpft sind, dass dieses ohne den betreffenden Dienst eine oder mehrere seiner wesentlichen Funktionen nicht ausführen könnte. Typischerweise handelt es sich dabei um Anwendungen oder spezielle Softwarelösungen, die der Steuerung oder Bedienung vernetzter Geräte dienen.

Demgegenüber werden Cloud-Lösungen (IaaS, PaaS, SaaS) in der Regel als „Datenverarbeitungsdienste“ im Sinne des Art 2 Z 8 DA qualifiziert. Diese umfassen digitale Dienste, die dem Kunden zentralisierte, dezentrale oder verteilte Rechenressourcen über die Cloud bereitstellen und damit Cloud- sowie Edge-Dienste ausdrücklich einschließen.

Zusammenfassend gilt daher, dass Cloud-Lösungen nach dem System des Data Act grundsätzlich nicht als verbundene Dienste, sondern als Datenverarbeitungsdienste einzustufen sind (insbesondere in den Kapiteln VI und VIII der Verordnung geregelt). Nur in Ausnahmefällen kann sie als verbundener Dienst im Sinne der Verordnung gelten, bspw wenn eine bestimmte Cloud-Lösung für die Funktionsfähigkeit eines vernetzten Produkts zwingend erforderlich ist. Im Regelfall bleibt jedoch die rechtliche Trennung zwischen beiden Kategorien bestehen.

### 9. Warum gibt es den Data Act? Wir haben ohnehin schon sehr viel Regulierung.

Kurz: Die europäische Datenstrategie 2020-2025 verfolgt das Ziel, einen fairen, innovativen und nachhaltigen Datenbinnenmarkt zu schaffen, in dem personenbezogene und nicht-personenbezogene Daten sicher sind und Unternehmen auf große Datenmengen hoher Qualität zugreifen können. Das Ziel ist die Schaffung eines echten Binnenmarkts für Daten, in dem datengetriebene Produkte und Dienstleistungen den EU-Normen und -Werten entsprechen. Dies sichert Europas technologische Souveränität und erschließt das Potenzial neuer Technologien wie KI.

Mit der **europäische Datenstrategie 2020-2025** wurde das Ziel verfolgt, die Chancen der digitalen Entwicklung für alle Menschen nutzbar zu machen. Digitale Technologien sollen den Zugang zu Wissen, Kommunikation und wirtschaftlicher Teilhabe erleichtern und dabei Sicherheit, Datenschutz und gesellschaftliche Verantwortung gewährleisten. Gleichzeitig soll ein faires, innovatives und nachhaltiges Umfeld für Unternehmen und die gesamte Gesellschaft geschaffen werden. Um dieser offenen und globalen digitalen Wirtschaft in Form von technologischer Leistungsfähigkeit und den rasanten Entwicklungen in der Gesellschaft einen (rechtlichen) Rahmen zu bieten, hatte sich die EU die Aufgaben gestellt, einen Normungsprozess für die neue „Technologiegeneration“ zu starten. Aus wirtschaftspolitischen Rahmenbedingungen entsprangen die wichtigsten Datenregulierungsrechtsakte für die Schaffung eines neuen sicheren und dynamischen „Datenbinnenmarkts“ (Data Act und Data Governance Act, DSGVO, NIS-2, ePrivacyRL).

### 10. Bedeutet der Data Act, dass ich bei allen IoT-Geräten nun Zugriff auf meine Daten habe?

Kurz: In den meisten Fällen ja, aber mit Grenzen. Der DA verpflichtet Hersteller und Anbieter verbundener Dienste, Datennutzern (Käufer, Mieter, Leasingnehmer) unverzüglich und

unentgeltlich Zugriff auf Rohdaten in gängigen, maschinenlesbaren Formaten zu gewähren. Das gilt für vernetzte Autos, SmartHome-Geräte, Wearables, Waschmaschinen etc. Der Zugriff bezieht sich primär auf Nutzungs- und Produktdaten (Sensor-, Betriebs-, Nutzungsdaten), nicht auf Betriebsgeheimnisse, Sicherheitsdaten oder abgeleitete Analysen. Rechtliche Grenzen müssen beachtet werden: personenbezogene Daten (DSGVO), Geschäftsgeheimnisse und Cybersicherheit.

Durch den DA werden Hersteller / Dateninhaber u.a. von vernetzten Produkten (IoT) und Anbieter verbundener Dienste verpflichtet, dem Datennutzer (durch Kauf-, Miet- oder Leasingvertrag) einen (direkten/indirekten) Zugriff auf die eigens generierten Daten bei der Nutzung des IoT-Gerätes zu gewährleisten und diese auch (wenn vom Datennutzer gewünscht) an Dritte zu Verfügung zu stellen (Beispiele: vernetzte Autos, SmartHome-Geräte, intelligente Lichtsysteme, Sicherheitskameras, Wearables wie SmartWatches, Waschmaschinen, uU Smartphones). Diese Daten müssen unverzüglich, einfach, sicher, unentgeltlich, in einem gängigen, maschinenlesbaren Format bereitgestellt werden, soweit die Daten ohne Weiteres verfügbar sind.

Achtung Art 3 Abs 1 DA gilt erst für Produkte, die ab 12.9.2026 in Verkehr gebracht werden, jedoch sollten jetzt schon die technische Ausführung und Lösung ausgearbeitet werden.

Primär bezieht sich der Zugriff auf (eigenen) Nutzungs- und Produktdaten (Rohdaten des Geräts, z.B. Sensor-, Betriebs- oder Nutzungsdaten), nicht aber um Betriebsgeheimnisse des Herstellers, Sicherheitsdaten, abgeleitete Analysen oder aufbereitete Daten zu erlangen. Es müssen rechtliche Grenzen, vor allem in Bezug auf personenbezogene Daten (DSGVO), Geschäftsgeheimnisse (Wettbewerbs- und Strafrecht!) oder aus sonstigen Sicherheitsgründen beachten (Cybersicherheit) beachtet werden.

### 11. Wenn ich als KMU in einer Lieferkette eingebunden bin, zB einem großen Unternehmen zuliefere, bin ich von den Regelungen betroffen?

Kurz: Unter Umständen, sofern das Klein- oder Kleinstunternehmen als Dateninhaber oder -nutzer mit vernetzten Produkten oder verbundenen Diensten im EU-Binnenmarkt agiert. Kleinst- und Kleinunternehmen (< 50 MA, < 10 Mio. EUR Umsatz/Bilanz) sind von meisten Herausgabepflichten ausgenommen. Mittlere Unternehmen (< 250 Pers., < 50 Mio. EUR Umsatz) haben bis 12.9.2026 in gewissen Regelungen Schonfrist. Als Zulieferer vernetzter Produkte oder Komponenten müssen jedoch Verträge überprüft und Compliance entlang der Lieferkette sichergestellt werden.

Kleinst- und Kleinunternehmen sind von verschiedenen Pflichten der Datenherausgabe meist ausgenommen, jedoch hat man als Zulieferer von vernetzten Produkten oder Komponenten zur Datenweitergabe als Teil der digitalen Lieferkette zu gewährleisten, Verträge prüfen und Compliance entlang der gesamten Lieferkette sicherstellen.

- Kleinstunternehmen: weniger als 10 Beschäftigte, Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überteigend (Art 2 Abs 3 Anhang der Empfehlung 2003/361/EG);
- Kleinunternehmen: weniger als 50 Beschäftigte, Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigend (Art 2 Z 25 und 26 DA mit Verweis auf Art 2 Abs 2 Anhang der Empfehlung 2003/361/EG);

- Mittlere Unternehmen: weniger als 250 Beschäftigte, Jahresumsatz von höchstens 50 Mio. EUR oder Jahresbilanzsumme höchstens 43 Mio. EUR

Mittelgroße Unternehmen haben noch bis 12. September 2026 Zeit, sich auf die Regelungen vorzubereiten (vgl. Art 7 DA).

## 12. Was, wenn ich personenbezogene Daten verarbeite, kommt der Data Act td zur Anwendung?

Kurz: Der DA reguliert sowohl personenbezogene als auch nicht-personenbezogene Daten. Im Konfliktfall hat die DSGVO Vorrang (Art. 1 Abs. 5 DA).

Der DA bietet keine eigene Rechtsgrundlage für Datenverarbeitung. Bei Verpflichtung zur Bereitstellung personenbezogener Daten müssen Anbieter zusätzlich zu DA-Anforderungen auch DSGVO-Anforderungen erfüllen – insbesondere für sensible Daten vernetzter Gesundheitsprodukte.

Der DA reguliert die effiziente Nutzbarmachung und gerechte Verteilung von personenbezogenen sowie nicht-personenbezogenen Daten entlang der Datenwertschöpfungskette. Der DA zeichnet sich durch seinen horizontalen und sektorübergreifenden Regulierungsansatz aus, wodurch von seinem Anwendungsbereich mitunter vernetzte Produkte und verbundene Dienste erfasst sind.

Zur Erreichung der Ziele hat der europäische Gesetzgeber einen Gleichlauf von personenbezogenen und nicht-personenbezogenen Daten vorgesehen, was angesichts der unscharfen Abgrenzung beider Kategorien insbesondere für den Datenzugang sinnvoll erscheint. Der Schutz personenbezogener Daten wird erstmals in ErwG 7 DA erwähnt, wo klargestellt wird, dass der DA das Datenschutzrecht einerseits ergänzt, es andererseits aber unberührt lässt. Art. 1 Abs. 5 DA konkretisiert dies, indem festgelegt wird, dass der DA unbeschadet des Unions- und nationalen Datenschutzrechts gilt. Im Konfliktfall genießen die Bestimmungen der DSGVO ausdrücklich Vorrang vor den Regelungen des DA. Die DSGVO findet somit immer dann Anwendung, wenn personenbezogene Daten einer natürlichen Person automatisiert verarbeitet werden.

Komplexe datenschutzrechtliche Fragen ergeben sich aus den in Kapitel II DA festgelegten Verpflichtungen der Dateninhaber zur Bereitstellung (sensibler) personenbezogener Daten vernetzter Gesundheitsprodukte, da jede Offenlegung solcher Daten gemäß Art. 4 Z 2 DSGVO und Art. 2 Z 7 DA eine Verarbeitung darstellt. Da der DA hierfür keine eigene Rechtsgrundlage bietet, müssen Dateninhaber neben der Einhaltung der im DA vorgesehenen Pflichten auch die Anforderungen der DSGVO an eine rechtmäßige Verarbeitung erfüllen.

## 13. Ist „access by design" dasselbe wie "privacy by design"?

Kurz: Nein. Beide überschneiden sich in der Technikgestaltung, unterscheiden sich aber im Zweck: Datenschutz versus Datenzugang.

**Privacy by Design** gemäß Art. 25 Abs. 1 DSGVO fordert, dass Datenschutzprinzipien bereits in der Entwicklung von Systemen integriert werden, um personenbezogene Daten von vornherein zu minimieren, pseudonymisieren oder anonymisieren und unnötige Verarbeitungen zu vermeiden.

**Access by Design** hingegen wird im Data Act (Kapitel II, Art 3 Abs 1) als datenpolitisches Prinzip verstanden, das den Zugang zu und die Nutzung von Daten – einschließlich nicht-personenbezogener Daten – von Anfang an durch technische und organisatorische Maßnahmen ermöglichen soll, ohne den Datenschutz zu beeinträchtigen (vgl. ErwG 20).

Beide Konzepte überschneiden sich in der Technikgestaltung, unterscheiden sich aber grundlegend im Zweck. Privacy by Design laut DSGVO bezweckt Datenschutz, Access by Design bezweckt wirtschaftlichen Datenzugang zu gewissen Informationen (inkl personenbezogener Daten).

### 14. Ist im Data Act auch etwas zur Datensicherheit geregelt?

Nein, explizite Datensicherheitsregelungen finden sich stattdessen in der DSGVO sowie im NISG 2026 und Cyber Resilience Act, welche den DA ergänzen. Vgl hierzu auch: it-safe.at

### 15. Gibt es schon eine Behörde in Österreich und wann ist mit Strafen zu rechnen?

Kurz: Derzeit noch nicht.

Prinzipiell müssen EU-Mitgliedstaaten zuständige Behörden benennen (Art. 37 Abs. 1 DA). Diese überwachen die DA-Einhaltung und arbeiten eng mit der Datenschutzbehörde zusammen. Die zeitliche Anwendung von Strafen ist noch nicht festgelegt. Sofern mehrere Behörden benannt werden, ist aus ihrer Mitte ein Datenkoordinator zu ernennen, welcher insbesondere die Zusammenarbeit zwischen den zuständigen Behörden erleichtert.

Die national zuständige(n) Behörde(n) muss/müssen die Einhaltung des Data Acts durch alle genannten Akteure überwachen und beaufsichtigen. Sie haben dabei die Durchsetzung des Data Acts zu gewährleisten. Auf nationaler Ebene muss die zuständige Behörde vor allem sehr eng mit der Datenschutzbehörde zusammenarbeiten, da diese ausdrücklich und ex lege für personenbezogene Daten iSd Data Act benannt wird (vgl. Art. 37 Abs. 3 DA).

Sind personenbezogene Daten betroffen, kann eine Strafe auch jetzt auf Basis der DSGVO ausgesprochen werden.

### 16. Omnibus-Regelungen

Kurz: Die EU plant Entbürokratisierungsmaßnahmen, um Datenrechtsakte (Data Act, Data Governance Act, Open Data RL, AI Act) zu vereinen. Geplant sind Änderungen bei Geschäftsgeheimnissen und individuell erstellter Software. Allerdings ist nicht sicher, ob und wann ein „Digital Omnibus" in welcher Form kommt. Der Data Act ist seit 12.9.2025 in Geltung – alle Regelungen müssen umgesetzt werden.

EU plant derzeit einige Entbürokratisierungs- und Vereinfachungsmaßnahmen auf europäischer Ebene, die insbesondere auch die Digitalisierungsrechtsakte betreffen: Data Act, Data Governance Act, Open Data RL, Free Flow of non-personal data und natürlich auch AI-Act. Dies sind jedoch einmal konkrete Beispiele der Europäischen Kommission und müssen in einem Trilog-Verfahren zusammen mit Europäischem Parlament und dem Europäischen Rat. Geplant sind alle Datenrechtsakte zu vereinen und zu einem großen „Data Act" zusammenzufassen, um eine einheitliche Regelung zu gewährleisten. Es sollen geringfügige Änderungen beim Schutz der Geschäfts- und Betriebsgeheimnisse und bei individuell erstellten Softwarelösungen (Art 31 DA) geben.

Es ist jedoch heute noch nicht fix, ob und wann es diesen „Digital Omnibus" in welcher Form geben wird. Feststeht, dass der DA seit 12.9.2025 in Geltung ist und daher alle Regelungen schon eingehalten und umgesetzt werden müssen.

### 17. Gibt es Standards für den Datenaustausch? In welcher Form soll es erfolgen?

Kurz: Der Datenaustausch muss einfach, unentgeltlich und in strukturiertem, gängigem, maschinenlesbarem Format erfolgen (z.B. JSON, CSV) inklusive Metadaten und in gleicher Qualität wie intern genutzt. Bereitstellung direkt vom vernetzten Produkt/verbundenen Dienst via API oder Echtzeit-Streaming, wo technisch möglich.

Bei Weitergabe an Dritte (auf Nutzerwunsch) gelten faire Vertragsbedingungen (FRAND-Bedingungen). Gatekeeper nach DMA sind ausgeschlossen.

Der Datenaustausch muss für Datennutzer einfach, unentgeltlich und in einem strukturiertem, gängigem, maschinenlesbarem Formaten zB wie JSON oder CSV, inklusive Metadaten und in gleicher Qualität wie intern genutzt – direkt vom vernetzen Produkt/verbundenen Dienst, API oder Echtzeit-Streaming, wo technisch möglich; Bei Weitergabe an Dritte (auf Nutzerwunsch) gelten faire Vertragsbedingungen (FRAND-Bedingungen); Gatekeeper nach DMA sind ausgeschlossen.

### 18. Wie kann ich verhindern, dass die Daten von meinen Konkurrenten weiterverwendet werden?

Kurz: Durch schriftliche Schutzmaßnahmen: Datenlizenzverträge mit Nutzern und Dritten, in denen Weiterverwendung für wettbewerbswidrige Zwecke ausgeschlossen wird. Geschäfts- und Betriebsgeheimnisse durch NDAs schützen. Geeignete technische und organisatorische Maßnahmen vor Datenfreigabe treffen. Bei hoher Wahrscheinlichkeit schwerwiegenden wirtschaftlichen Schadens können Einwände erhoben werden. Nutzer dürfen erhaltene Daten nicht zur Entwicklung konkurrierender vernetzter Produkte oder zur Offenlegung wirtschaftlicher Informationen des Herstellers nutzen.

Hier sollte man (vertragliche) Schutzmaßnahmen gestalten, kreativ sein; Missbrauch kann durch FRAND-Bedingungen eingeschränkt werden, Datenlizenzverträge mit Nutzern und Dritten abschließen, in welchen explizit die Weiterverwendung der Daten an Dritten für wettbewerbswidrige Zwecke ausgeschlossen wird (zB Art 5 Abs 5 DA).

Geschäfts- und Betriebsgeheimnisse durch NDAs schützen; geeignete TOMs vor Datenfreigabe treffen; bei hoher Wahrscheinlichkeit schwerwiegenden wirtschaftlichen Schadens Einwände erheben (vgl. Art 4 Abs 10 DA).

Der Nutzer darf die aufgrund eines Verlangens erlangten Daten weder zur Entwicklung eines vernetzten Produkts nutzen, das mit dem vernetzten Produkt, von dem die Daten stammen, im Wettbewerb steht, noch darf er diese Daten mit dieser Absicht an einen Dritten weitergeben oder nutzen, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers oder gegebenenfalls des Dateninhabers zu erlangen.

Empfehlenswert sind die Mustervertragsklauseln der Europäischen Kommission.

### 19. Ich erhebe Daten von Räumfahrzeugen im ländlichen Bereich (Schneeräumung); diese Daten werden aggregiert und Analysten daraus getroffen, welche Daten muss ich jetzt herausgeben?

Kurz: Der Data Act gilt für alle, die vernetzte Produkte oder Dienste in der EU in Verkehr bringen oder nutzen (Marktortprinzip). Hersteller und Anbieter müssen Roh-, Nutzungs- und Produktdaten sowie verbundene Dienstdaten und „ohne weiteres verfügbare Daten" bereitstellen. Metadaten mit Kontext und Zeitstempel sind erforderlich. Aggregierte, aufbereitete oder abgeleitete Analysedaten müssen nicht herausgegeben werden.

Der persönliche Anwendungsbereich folgt dem Marktortprinzip (Art 1 Abs 3 DA): Er gilt unabhängig vom Sitz der Unternehmen für alle, die vernetzte Produkte oder Dienste in der EU in Verkehr bringen oder nutzen.

- Hersteller /Dateninhaber vernetzter Produkte und Anbieter verbundener Dienste in der EU
- Datennutzer solcher Produkte/Dienste in der EU (Privatpersonen oder Unternehmen)
- Datenempfänger in der EU

Prinzipiell müssen Roh- , Nutzungs- und Produktdaten (Art 2 Abs 15, ErwG 15), verbundene Dienstdaten (Art 2 Abs 16, ErwG 15, 17) angereicherte Daten (ErwG 15) sowie „ohne weiters verfügbare Daten“ (Art 2 Abs 17, ErwG 20, 21) und Metadaten bereitgestellt werden

*(ErwG 15: Die Daten, die bereitzustellen sind, sollten die einschlägigen Metadaten, einschließlich ihres grundlegenden Kontexts und Zeitstempels, umfassen, um die Daten in Kombination mit anderen Daten, z. B. Daten, die sortiert und mit anderen, mit ihnen verbundenen Datenpunkten klassifiziert wurden oder die in ein gängiges Format umformatiert wurden, nutzbar zu machen.)*

Aggregierte, aufbereitete oder abgeleitete (Analyse-)Daten müssen nicht zur Verfügung gestellt werden iSd Data Acts.

### 20. Gibt es eine Checkliste, was Unternehmen machen müssen?

Im Unternehmen kann anhand dieser Checkliste geprüft werden:

**Interne Überprüfung:**

- Verträge prüfen auf DA-Konformität
- Klauseln identifizieren, die dem DA widersprechen
- Geschäftsmodelle überarbeiten

**Technische Umsetzung:**

- Datenportabilität prüfen und sicherstellen
- API-Lösungen entwickeln
- Maschinenlesbare Formate definieren
- Datentransfer in 30-Tage-Frist realisierbar machen

**Vertragsrecht:**

- Kunstndigungsfristen (max. 2 Monate) implementieren
- Kompensationsmodelle überarbeiten
- Transparenz in Entgeltstrukturen schaffen
- Wechselprozesse kundenfreundlich gestalten

**Datenschutz und Compliance:**

- DSGVO-Konformität sicherstellen
- Sicherheitsmaßnahmen bei Datenherausgabe treffen
- Geschäftsgeheimnisse durch Verträge schützen
- Lieferketten-Compliance prüfen

**Timeline:**

- Mittlere Unternehmen: Schonfrist bis 12.9.2026
- Alle anderen: Sofortige Umsetzung erforderlich

21. Wenn so eine Anfrage zum Datenexport von einem/einer Endkund:in bei mir als Anbieter eingeht, welche Frist gilt dann, diese Daten in einem maschinenlesbaren Datenformat zu liefern. Sprich: Könnte ich als Anbieter diese Daten auch manuell für den/die Endkund:in exportieren?

**Allgemeiner Datenzugang / Export**

Wenn Nutzer:innen Daten nicht direkt aus dem Produkt/Service ziehen können, muss der Dateninhaber die Daten „ohne unangemessene Verzögerung“ und in einem strukturierten, gängigen, maschinenlesbaren Format bereitstellen (Art. 4 Abs. 1 Data Act).

Wie man dieses Format erzeugt (manuell oder automatisiert) ist technisch nicht vorgegeben; entscheidend ist, dass das Ergebnis die Anforderungen aus Art. 4 (Qualität, Format, Zugänglichkeit) erfüllt und der Prozess nicht unangemessen verzögert wird.

**Speziell beim Cloud-/SaaS-Switching**

Für Switching-Szenarien muss der Vertrag u.a. vorsehen, dass der Kunde seine exportierbaren Daten in einem definierten Zeitraum abrufen kann („data retrieval

period“), der mindestens 30 Kalendertage ab Ende der Übergangsperiode dauert (Art. 25 Abs. 2 lit. g Data Act).

Der Beginn des Switching-Prozesses darf vertraglich höchstens mit einer Kündigungs-/Ankündigungsfrist von zwei Monaten hinausgezögert werden (Art. 25 Abs. 2 lit. d, Abs. 3 Data Act).

## 22. Kann man die Herstellerpreiserhöhungen nicht mehr an Kunden weitergeben? Sind auch Preisanpassungsklauseln bedenklich?

Preisanpassungsklauseln sind weiterhin möglich, aber Art. 13 Abs 5 lit g Data Act stuft Klauseln als unfair ein, die „*den vertraglich vereinbarten Preis (…) ohne eine im Vertrag spezifizierte stichhaltige Begründung wesentlich abändert, ohne dass der anderen Partei das Recht eingeräumt wird, den Vertrag im Falle einer solchen Abänderung zu kündigen.*“

Einseitige Anpassungen ohne sachlichen Grund (z.B. reale Herstellerkostensteigerungen) oder ohne Kündigungsrecht für den Kunden sind daher problematisch. Proportionale, transparent begründete Anpassungen (z.B. Indexierung) bleiben weiterhin zulässig.

## 23. Was gilt für Hersteller, die auf Hardware und / oder Betriebssysteme von Google "aufsetzen" und dieses Produkt mit einer eigenen Anwendung verkaufen? Muss die Verarbeitung auch dieser Daten vorvertraglich vereinbart werden und auf Anfrage bereitgestellt werden, obwohl man keinen direkten Zugriff hat

Ist man direkt vom Data Act betroffen, muss man sicherstellen, dass die entsprechenden Pflichten erfüllt werden können. Das beinhaltet, dass man Dienstleister / Plattformen auswählt, mit denen dies möglich ist. Es sollten daher (ähnlich wie im Datenschutz) mit Dienstleistern Verträge abgeschlossen werden, die einen Data Act-konformen Datenfluss gewährleisten.

## 24. Betrifft mich das auch als Gemeinde, also den öffentlichen Sektor?

Der Begriff der „öffentlichen Stelle“ nach Art 2 Z 28 DA ist weit und umfassend definiert. Eine öffentliche Stelle sind nationale, regionale und lokale Behörden, Körperschaften und Einrichtungen des öffentlichen Rechts. Der Begriff „Stelle“ kann auch Ämter, Behörden, Beobachtungstellen, Ausschüsse usw. erfassen. Eine Gemeinde ist nach dem österreichischen Staats- und Verwaltungsaufbau eine juristische Person des öffentlichen Rechts. Daher betrifft eine Gemeinde das Kapitel V des Data Acts sehr wohl (B2G). Eine Gemeinde kann somit ein Datenbereitstellungsverlangen bei Unternehmen fordern, wenn nach Art 15 Abs 1 DA eine außergewöhnliche Notwendigkeit der Nutzung für bestimmte Daten gegeben ist und diese zeitlich befristet und nur unter bestimmten Umfängen bereitgestellt werden kann (zB Naturkatastrophen, Pandemien).

### 25. Art 17 Abs 2 lit g und h: unter welchem link kann das geprüft werden, ob die Veröffentlichung erfolgt ist?

Zur Gewährleistung der Transparenz der öffentlichen Hand sieht der DA an mehreren Stellen vor, dass das Verlangen öffentlich zu machen ist (zB Art 17 Abs 2 DA). Dabei wird danach entschieden, von wem dieses Verlangen gestellt wurde. Sofern ein Verlangen durch eine öffentliche Stelle erfolgt, muss dieses dem Datenkoordinator gemeldet werden (Art 37 Abs 6 lit b DA), welcher durch die Mitgliedsstaaten gesetzlich eingerichtet wurde. Da es in Österreich noch keine zuständige Behörde oder einer Datenkoordinator gibt, kann man hier noch auf keine Webseite oder Link verweisen. Eventuell publizieren die öffentlichen Stellen auf den eigenen Webseiten die Datenzugangsverlangen.

### 26. Gibt es das Musterformular gemäß Art 17 Abs 6 schon?

Bisher wurde noch kein abgenommenes Musterformular von der Europäischen Kommission veröffentlicht. Entwürfe finden sich jedoch hier: https://digital-strategy.ec.europa.eu/de/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding.

### 27. Art 32 (Staatlicher Zugang und staatliche Übermittlung im internationalen Umfeld)

#### a. Abs 1: spricht von „staatlichen Zugang zu und die staatliche Übermittlung von“ – Abs 5 nur von Datenzugangsverlangen. Kann diese Unterscheidung Absicht sein und bezieht sich Abs 5 demnach nicht auf Verlangen zur Übermittlung?

Art 32 DA richtet sich an Anbieter von Datenverarbeitungsdiensten und regelt die Zulässigkeit der Übermittlung nicht-personenbezogener, von Behörden abgerufener Daten in Drittländer nach dem Prinzip „Erlaubnis mit Verbotsvorbehalt“, anders als Art 44 DSGVO. Der „Zugang zu“ und die „Übermittlung von“ Daten sind dabei zu unterscheiden, auch wenn sie mangels Definition ähnlich weit verstanden werden können.

Unter dem Rückgriff auf Art 2 Z 13 DGA liegt „*Zugang*“ bereits vor, wenn Daten im Einklang mit technischen, rechtlichen oder organisatorischen Vorgaben genutzt werden, ohne dass sie übertragen oder heruntergeladen werden müssen. „*Übermittlung*“ wird im Datenschutzrecht sehr weit ausgelegt und kann auch ein bloßes Bereithalten umfassen, sodass sich beide Begriffe stark annähern. In der englischen Fassung („governmental access“) spricht jedoch viel dafür, nur einen aktiven Transfer in ein Drittland zu erfassen, nicht aber den bloßen Remote-Zugriff aus dem Drittland auf in der EU gespeicherte Daten.

Hier handelt es sich um einen sprachlichen Fehler, nach Abs. 5 hat der Anbieter von Datenverarbeitungsdiensten seinen Kunden mitzuteilen, ob ein Datenzugangs- bzw. Übermittlungsverlagen eines Drittstaates vorliegt, sofern es sich nicht zu Strafverfolgungszwecken dient.[1]

[1] *Denga* in *Specht/Hennemann* (Hrsg.), Data Act und Data Governance Act[2], S 588.

b. Abs 2: Urteil/Entscheidung nur anerkannt/vollstreckbar, wenn auf so einer Übereinkunft beruhend. Kann man draus interpretieren, dass die Übereinkunft in der Anfrage genannt sein muss, also dass sich die Anfragenden darauf beziehen? In Abs 3 wird jedoch auf das „Bestehen" der Übereinkunft abgestellt.

Die Befolgung von Entscheidungen aus einem Drittland ist nur unter bestimmten Voraussetzungen zulässig. Solche gerichtlichen oder verwaltungsbehördlichen Entscheidungen sind hoheitliche Anordnungen, auch wenn sie auf Initiative Privater ergehen. Abs 2 stellt klar, dass völkerrechtliche Abkommen (etwa Rechtshilfeabkommen) dazu führen können, dass solche Entscheidungen anerkannt und vollstreckt werden.

Abs 3 greift, wenn keine völkerrechtliche Grundlage für die Entscheidung des Drittstaats besteht. In diesem Fall dürfen Entscheidungen nur befolgt werden, wenn bestimmte rechtsstaatliche Mindeststandards eingehalten sind. Dabei kann es leicht zu Situationen kommen, in denen Adressaten kollidierenden Pflichten aus verschiedenen Rechtsordnungen ausgesetzt sind, etwa einer Geheimhaltungspflicht einerseits und einer Offenlegungspflicht andererseits.[2]

c. Abs 3: Lt Bitcom Umsetzungsleitfaden ist im Fall des angeforderten staatlichen Zugangs ein solcher Zugriff 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.

Es sollte jedenfalls die Rechtsgrundlage geprüft werden.

28. Muss bei Vorliegen einer internationalen Vereinbarung tatsächlich auch noch die Vereinbarkeit mit EU-Recht/nationalem Recht geprüft werden oder ist das mit Vorliegen einer solchen Vereinbarung nicht ohnehin erfüllt? Wer ist in Österreich als die "zuständige nationale Stelle oder die für die internationale Zusammenarbeit in Rechtssachen zuständigen Behörde" anzusehen?

Das Vorliegen eines völkerrechtlichen Abkommens ist zwar Voraussetzung für die Anerkennung und Vollstreckbarkeit von Entscheidungen aus Drittstaaten (Art 32 Abs 2 DA), es wird jedoch nicht die Prüfung ersetzt, ob der bestimmte Zugriff mit Unionsrecht und nationalem Recht rechtlich vereinbar ist. Es muss dahingehend immer noch eine materielle Prüfung von datenschutzrechtlichen, wettbewerbsrechtliche und/oder nationale Sicherheitsregelungen unabhängig vorgenommen werden.

Jeder Mitgliedsstaat eine oder mehrere zuständigen nationalen Behörden(n) einrichten (Art 37 DA). Diese wurde in Österreich noch nicht eingerichtet.

[2] zB US-Cloud Act.

„Ich mache IT recht damit ihr euch um die Technik kümmern könnt.“

Mag. Katharina Bisset, MSc ist selbstständige Rechtsanwältin in NÖ, Co-Founderin der LegalTech Unternehmen NetzBeweis GmbH und der Nerds of Law. Davor war sie mehrere Jahre in großen IT-Unternehmen tätig. Ihre Spezialgebiete sind IT-, IP-, und Datenschutzrecht. Zusätzlich zur juristischen Ausbildung hat sie einen MSc in Business Process Management and Engineering. Sie ist darüber hinaus Disziplinarrätin in der RAK NÖ und Lektorin.

Die FAQ wurden im Zuge des Webinars „Data Act – Das Datengesetz für Unternehmen“ vom 11. Dezember 2025 von 15:30 bis 16:30 Uhr erstellt. Die Inhalte wurden mit größtmöglicher Sorgfalt erstellt und entspricht dem juristischen Kenntnisstand zum Zeitpunkt des Webinars. Dennoch wird keine Haftung für Richtigkeit, Vollständigkeit und Aktualität übernommen.