CEDPO
CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

Bonn, Bukarest, Dublin, Lissabon, Madrid, Mailand, Paris, Den Haag, Wien, Warschau

Data Act

FAQ für Datenschutzbeauf-tragte

EU-Arbeitsgruppe „Digitale Strategie“
Oktober 2025

Kontaktinformationen:
https://cedpo.eu
info@cedpo.eu

Inhaltsverzeichnis

Vorwort 4
Frage 1: Was ist der Data Act und was ist sein Ziel? 5
Frage 2: Für wen gilt der Data Act? 5
Frage 3: Auf welche Art von Daten findet der Data Act Anwendung? ..... 5~~6~~
Frage 4: Welche verschiedenen Arten von Akteuren gibt es gemäß dem Data Act? 6
Frage 5: Was sind nicht personenbezogene Daten? 7
Frage 6: Wie soll ich eine Datei behandeln, die sowohl personenbezogene als auch nicht personenbezogene Daten enthält? 8
Frage 7: Wann sollte meine Organisation technische und organisatorische Maßnahmen zum Schutz der Daten ergreifen? 9
Frage 8: Was muss berücksichtigt werden, um die mit dem Data Act verbundenen Risiken zu minimieren? 10
Frage 9: Was ist eine gängige Methode für den Datenaustausch gemäß dem Data Act und wie lassen sich Datenschutzrisiken reduzieren? 12
Frage 10: Welche Pflichten hat der Dateninhaber? 13
Frage 11: Wie formalisiert man die Weitergabe von Daten im Business-to-Business-Kontext? 14
Frage 12: Meine Organisation ist ein Dateninhaber. Kann ich die Bereitstellung von Daten verweigern? 14
Frage 13: Welche Auswirkungen hat der Data Act auf die Verwaltung der Rechte betroffener Personen in Fällen, in denen es sich um personenbezogene Daten handelt? 15
Frage 14: Welche Rechtsgrundlagen können für die Verarbeitung personenbezogener Daten herangezogen werden, für die der Data Act gilt? 15
Frage 15: Meine Organisation ist ein Nutzer und möchte die vom Dateninhaber zur Verfügung gestellten Daten auf der Grundlage eines berechtigten Interesses verarbeiten. Ist das möglich? 16
Frage 16: Meine Organisation ist eine öffentliche Einrichtung. In welchen Situationen kann meine Organisation Daten aufgrund eines „außergewöhnlichen Bedarfs" anfordern? 18
Frage 17: Wie wird Profiling im Data Act definiert? 19
Frage 18: Ist Profiling nach dem Data Act verboten? 20
Frage 19: Warum ist Transparenz im Rahmen des Data Acts so wichtig? 22
Nützliche Links 24

Haftungsausschluss 24

Vorwort

Mit dem Inkrafttreten der DS-GVO vor sieben Jahren wurde eine solide Grundlage für den Datenschutz in Europa geschaffen. Im Laufe der Zeit hat sich das regulatorische Umfeld weiterentwickelt, um Europa in eine verantwortungsvolle digitale Zukunft zu führen. Der EU-Data Act markiert einen weiteren Meilenstein auf diesem Weg. Der durchgesickerte Entwurf des Digitalen Omnibus zeigt, dass der Data Act in Zukunft eine immer wichtigere Rolle bei der Regulierung des digitalen Raums spielen wird.

Derzeit führt der Data Act neben anderen aktuellen Datenschutzgesetzen wie dem Data Governance Act (DGA), dem Digital Services Act (DSA) und dem Digital Markets Act (DMA) neue Verpflichtungen und Möglichkeiten ein. Infolgedessen müssen Datenschutzbeauftragte (DSB) ihr Fachwissen zunehmend über die DS-GVO hinaus erweitern und zu einem breiteren Spektrum von Fragen der Datenverwaltung und Compliance beraten.

Um die DSB-Community bei der Bewältigung dieser bevorstehenden Herausforderungen zu unterstützen, hat CEDPO über seine Arbeitsgruppe „EU-Digitalstrategie" in Zusammenarbeit mit seinen erfahrenen Mitgliedern aus ganz Europa praktische und aufschlussreiche Antworten auf häufig gestellte Fragen (FAQs) zum EU-Data Act entwickelt. Diese FAQs konzentrieren sich speziell auf Themen, die für den Datenschutz relevant sind.

Wir bedanken uns herzlich bei allen Mitgliedern der Arbeitsgruppe „EU-Digitalstrategie" und den Mitarbeitern von CEDPO für ihre wertvollen Beiträge.

Mitwirkende WG-Mitglieder: **Thomas Ajoodha, Filippo Bianchini, Lionel Capel, Julie Crawford, Paul Jordan, Paul Lambert, Dr. Maria Maloney, Samira Marquaille, Massimo Pappalardo, Jeremiah Russel, Henry Simwinga.**

Dr. Sachiko Scheuing (GDD) & Filippo Bianchini (ASSO DPO)

Co-Vorsitzende der CEDPO-Arbeitsgruppe „Digitale Strategie der EU"

Frage 1: Was ist der Data Act und was ist sein Ziel?

Der Data Act ist ein wesentlicher Bestandteil der Legislativagenda der EU und hat zum Ziel, die europäische Datenstrategie voranzutreiben, um der EU eine führende Rolle in einer datengesteuerten Gesellschaft zu verschaffen. Der Data Act unterstützt den freien Datenfluss in einem Binnenmarkt, der mehrere Bereiche der Wirtschaft, Forschung und öffentlichen Verwaltung umfasst. Der Data Act zielt darauf ab, Daten durch Mechanismen zum Datenaustausch für alle zugänglicher und nutzbarer zu machen. Das Gesetz verpflichtet Dateninhaber, Daten unter bestimmten Umständen zur Verfügung zu stellen. Gleichzeitig ermöglicht es Nutzern, von den von ihnen generierten Daten zu profitieren, beispielsweise von ihren IoT-Geräten. Konkret verlangt der Data Act, dass vernetzte Produkte so gestaltet sind, dass Nutzer direkt auf die von ihnen generierten Daten zugreifen können (Art. 3 Data Act). Auf den ersten Blick klingt dies ähnlich wie die Datenübertragbarkeit und das Auskunftsrecht gemäß der DS-GVO. Es kann als weitere Spezifizierung dieser Rechte angesehen werden. In Fällen, in denen ein direkter Zugriff nicht möglich ist, müssen die Daten den Nutzern auf Anfrage schnell zur Verfügung gestellt werden (Art. 4 Data Act). Der Schwerpunkt des Data Acts liegt auf der Gewährleistung eines fairen Zugangs zu Daten und dem Schutz der Nutzerrechte, wobei diese Ziele mit dem Schutz personenbezogener Daten in Einklang gebracht werden müssen.

Der Data Act steht im Einklang mit den bestehenden Vorschriften zur Verarbeitung personenbezogener Daten, einschließlich der DS-GVO. Es kann hilfreich sein, die Definitionen manchmal mit anderen relevanten EU-Rechtsvorschriften abzugleichen. So schafft beispielsweise die Verordnung über den freien Verkehr nicht personenbezogener Daten eine wichtige Grundlage für die europäische Datenwirtschaft, indem sie sicherstellt, dass nicht personenbezogene Daten überall in der EU gespeichert, verarbeitet und übertragen werden können.

Frage 2: Für wen gilt der Data Act?

Der Data Act gilt für Organisationen und Personen, die für die Erstellung, Verarbeitung oder Nutzung, Verwaltung und Weitergabe von Daten aus intelligenten Technologien in der EU verantwortlich sind. Insbesondere regelt der Data Act die Dateninhaber, in der Regel Designer, Hersteller oder Dienstleister, die Rohdaten aus diesen intelligenten Technologien generieren oder abrufen können. Der Data Act konzentriert sich stark auf den Bereich Business-to-Business und Business-to-Consumer, regelt aber auch den Datenaustausch zwischen Unternehmen und Behörden.

Kleinst- und Kleinunternehmen sowie mittelständische Unternehmen, die seit weniger als einem Jahr bestehen, sind gemäß Art. 5 des Data Acts von der Weitergabepflicht ausgenommen.

Frage 3: Auf welche Art von Daten findet der Data Act Anwendung?

Der Data Act gilt für alle Rohdaten und vorverarbeiteten Daten, die durch die Nutzung eines vernetzten Produkts oder einer damit verbundenen Dienstleistung entstehen und dem Dateninhaber ohne Weiteres zur Verfügung stehen, wie z. B. Produktdaten (die durch die Nutzung vernetzter Produkte entstehen), Daten zu damit verbundenen Dienstleistungen (Aktionsdaten der Nutzer) oder Metadaten (Daten, die zur Interpretation von Produktdaten und Daten zu damit verbundenen Dienstleistungen erforderlich sind). Rohdaten und vorverarbeitete Daten können sowohl personenbezogene als auch nicht personenbezogene Daten sein. Daten, die stark verarbeitet wurden, wie z. B. abgeleitete Daten (z. B. hoch angereicherte Daten, audiovisuelles Material), die unter Verwendung komplexer Algorithmen generiert wurden, unterliegen nicht dem Data Act.

Der Data Act unterscheidet auch zwischen Rohdaten und abgeleiteten Daten. Handelt es sich bei den Rohdaten um personenbezogene Daten, gilt zusätzlich zum Data Act die DS-GVO.

Das Register der Verarbeitungsaktivitäten (RoPA) ist ein guter Ausgangspunkt, um festzustellen, ob der Data Act auf Ihre Organisation anwendbar ist.

Frage 4: Welche verschiedenen Arten von Akteuren gibt es gemäß dem Data Act?

Der Data Act definiert die folgenden drei Hauptakteure: den Dateninhaber, den Datenempfänger und den Nutzer.

Ein **Dateninhaber** ist eine Person oder Organisation, die rechtmäßigen Zugriff auf Rohdaten aus vernetzten Produkten oder damit verbundenen Diensten hat und befugt ist, Zugriff darauf zu gewähren. Im Wesentlichen ist ein Dateninhaber eine natürliche oder juristische Person, die das Recht oder die Pflicht hat, Daten zu nutzen oder weiterzugeben, die während der Erbringung einer damit verbundenen Dienstleistung generiert oder gesammelt wurden. In der Praxis sind Dateninhaber in der Regel Unternehmen, wie z. B. Hersteller vernetzter Produkte oder Anbieter verwandter Dienste, die intelligente Geräte verwalten und über diese Geräte erhobene Kundendaten speichern. Diese Rolle ist wohl die wichtigste im Rahmen des Data Acts. Jede Organisation, ob öffentlich oder privat, die Daten kontrolliert, die durch vernetzte Produkte und Dienste generiert werden, gilt als Dateninhaber.

Zu den Aufgaben eines Dateninhabers gehört es, den Zugang zu den Daten zu erleichtern und sicherzustellen, dass die Daten in einem benutzerfreundlichen Format, wie im Gesetz festgelegt, an andere Dienstleister übertragen werden können. Es ist ihnen außerdem untersagt, den Nutzern unfaire Vertragsbedingungen hinsichtlich des Zugangs zu ihren Daten und ihrer Rechte auf Datenübertragbarkeit aufzuerlegen.

Ein **Datenempfänger** ist eine Person oder Organisation, die auf Anfrage des Nutzers Rohdaten von einem Dateninhaber erhält. Im Wesentlichen ist ein Datenempfänger eine natürliche oder juristische Person, die nicht der Nutzer ist und der der Dateninhaber Daten zur Verfügung stellt, einschließlich Dritter, die auf Anfrage eines Nutzers oder in Übereinstimmung mit einer gesetzlichen Verpflichtung handeln.

In der Praxis sind Datenempfänger in der Regel juristische Personen wie Unternehmen, Behörden, Forschungseinrichtungen oder gemeinnützige Organisationen. Es gibt spezifische Beschränkungen, die große Anbieter oder „Gatekeeper" im Sinne des Digital Markets Act daran hindern, als Dritte in bestimmten Vereinbarungen zur Datenweitergabe zu agieren.

Im Wesentlichen ist ein Datenempfänger eine Einrichtung, die Daten von einem Dateninhaber mit der Absicht erhält, diese für geschäftliche oder berufliche Zwecke zu verwenden. Dies kann Unternehmen umfassen, die Daten zum Nutzerverhalten analysieren, Cloud-Speicher für Daten bereitstellen, die von verbundenen Geräten generiert werden, oder datengesteuerte Dienste anbieten ~~()~~. Der wesentliche Unterschied besteht darin, dass ein Datenempfänger die Daten für kommerzielle oder organisatorische Zwecke verwendet und nicht für den persönlichen Gebrauch, wie es ein Datennutzer tun würde.

Ein **Nutzer** ist eine Person oder Organisation, die ein vernetztes Produkt besitzt oder das Recht hat, es zu nutzen oder damit verbundene Dienste in Anspruch zu nehmen. Im Wesentlichen ist ein Nutzer die natürliche oder juristische Person, die ein intelligentes Gerät besitzt, mietet oder least.

In der Praxis ist der Nutzer in der Regel der Kunde eines intelligenten Geräts. Es ist wichtig zu beachten, dass Personen, die das Gerät nutzen, aber nicht Vertragspartei sind, wie z. B. Familienmitglieder, wahrscheinlich nicht als Nutzer gelten.

Frage 5: Was sind nicht personenbezogene Daten?

Der Data Act definiert nicht personenbezogene Daten als alle Daten, die nicht unter die Kategorie der personenbezogenen Daten fallen, wie in Art. 2 Abs. 4 Data Act festgelegt. Während die DS-GVO in Erwägungsgrund 26 anonyme Daten als Informationen definiert, die nicht mit einer identifizierten oder identifizierbaren natürlichen Person in Verbindung gebracht werden können, enthält sie keine ausdrückliche Definition für nicht personenbezogene Daten.

Die Verordnung über einen Rahmen für den freien Verkehr nicht personenbezogener Daten innerhalb der Europäischen Union führt in Art. 1 nicht personenbezogene Daten als „andere Daten als personenbezogene Daten" ein. Im Vergleich zur Definition personenbezogener Daten in Art. 1 können nicht personenbezogene Daten als alle Informationen verstanden werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person (die „betroffene Person") beziehen. Die Leitlinien der EU-Kommission aus dem Jahr 2019 zur Verordnung über einen Rahmen für den freien Verkehr nicht personenbezogener Daten stützen diese Auslegung.

Darüber hinaus unterteilt die Kommission nicht personenbezogene Daten in zwei Kategorien:

(1) Daten, die ursprünglich nicht zu einer identifizierten oder identifizierbaren natürlichen Person gehörten und
(2) Daten, die ursprünglich personenbezogen waren, später jedoch anonymisiert wurden.

Temperaturmessungen in einem Gebäude sind ein Beispiel für (1), und das Durchschnittsalter der Schüler in einem Klassenzimmer ist ein Beispiel für (2).

Es ist wichtig zu beachten, dass sich die Anonymisierung personenbezogener Daten von der Pseudonymisierung unterscheidet. Während bei der Anonymisierung Daten so verarbeitet werden, dass sie keiner Person zugeordnet werden können, bezieht sich die Pseudonymisierung auf Daten, die durch zusätzliche Informationen weiterhin einer Person zugeordnet werden können. Es ist auch wichtig zu beachten, dass pseudonymisierte Daten zu anonymen Daten werden, wenn sie sich in den Händen von Organisationen befinden, die keine Möglichkeit haben, die betroffene Person wieder zu identifizieren.[1]

Beispiele für nicht personenbezogene Daten sind aggregierte oder anonymisierte Datensätze, die in der Big-Data-Analyse verwendet werden, Daten aus der Präzisionslandwirtschaft, die zur Optimierung des Pestizid- und Wasserverbrauchs beitragen, sowie Daten zum Wartungsbedarf von Industriemaschinen. Wenn jedoch technologische Fortschritte die Re-Identifizierung anonymisierter Daten ermöglichen, würden diese Daten als personenbezogene Daten gelten und die DS-GVO würde dann Anwendung finden.

Frage 6: Wie soll ich eine Datei behandeln, die sowohl personenbezogene als auch nicht personenbezogene Daten enthält?

Die meisten Daten, die unter den Data Act fallen, werden als „nicht personenbezogene Daten“ eingestuft, da sie sich auf industrielle Produkte und Dienstleistungen und nicht auf Personen beziehen. Es ist jedoch nicht ungewöhnlich, dass diese Daten mit personenbezogenen Daten vermischt sind. Wenn eine Datei sowohl personenbezogene als auch nicht personenbezogene Daten enthält, wird sie als gemischter Datensatz bezeichnet.

In Bezug auf gemischte Datensätze wird in Erwägungsgrund 7 des Data Acts darauf hingewiesen, dass die DS-GVO[2] und die ePrivacy-Richtlinie (sofern anwendbar) die Grundlage für eine nachhaltige und verantwortungsvolle Datenverarbeitung bilden.

Eine etwas andere Nuance findet sich in einer anderen EU-Verordnung, die gemischte Datensätze erwähnt: der Verordnung über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union. Gemäß diesem Gesetz und den Leitlinien der Kommission zur Verordnung über den freien Verkehr nicht personenbezogener Daten gilt Folgendes:

1. Die „Verordnung über den freien Verkehr nicht personenbezogener Daten” gilt für den nicht personenbezogenen Teil des Datensatzes.
2. Die DS-GVO gilt für den Teil des Datensatzes, der personenbezogene Daten enthält.
3. Wenn die nicht personenbezogenen Daten und die personenbezogenen Daten „untrennbar miteinander verbunden“ sind, gilt die DS-GVO für den gesamten Datensatz,

[1] Urteil vom 4. September 2025, EDPS gegen SRB, C-413/23 P, ECLI:EU:C:2025:645.
[2] Und die *Verordnung* von 2018 *zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union und zum freien Datenverkehr*.

auch wenn die personenbezogenen Daten nur einen kleinen Teil des Datensatzes ausmachen.

In den Leitlinien der Kommission wird weiter erläutert, dass nicht personenbezogene Daten und personenbezogene Daten „untrennbar miteinander verbunden“ sind, wenn es unmöglich oder technisch oder wirtschaftlich nicht machbar ist, die beiden Datentypen voneinander zu trennen.

Die Empfehlung für den Umgang mit gemischten Datensätzen lautet, einen angemessenen Schutz zu gewährleisten und die Verpflichtungen gemäß der DS-GVO einzuhalten. Wenn es jedoch nicht möglich ist, die betroffene Person zu identifizieren, ist der für die Verarbeitung Verantwortliche von den Verpflichtungen gemäß den Artt.~~.n~~ 15 bis 20 der DS-GVO befreit. Zu diesen Verpflichtungen gehören das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, die Benachrichtigungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung sowie das Recht auf Datenübertragbarkeit gemäß Art. 11 Abs. 2 der DS-GVO.

Frage 7: Wann sollte meine Organisation technische und organisatorische Maßnahmen zum Schutz der Daten ergreifen?

Bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen zum Schutz der Daten getroffen werden. Eine Schutzmaßnahme, die sowohl in der DS-GVO als auch im Data Act hervorgehoben wird, ist die Pseudonymisierung. Es wird empfohlen, im Rahmen des Data Acts denselben Pseudonymisierungsstandard anzuwenden, wie er in der DS-GVO vorgeschrieben ist.

Der Data Act befasst sich auch mit Schutzmaßnahmen in Situationen, in denen personenbezogene Daten aufgrund eines „außergewöhnlichen Bedarfs” an eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine EU-Institution weitergegeben werden müssen. In solchen Fällen muss die anfragende Organisation, die zum Schutz der Daten erforderlichen technischen und organisatorischen Maßnahmen angeben. Darüber hinaus sollte die anfragende Organisation prüfen, ob die personenbezogenen Daten anonymisiert werden können.

Andererseits muss der Dateninhaber personenbezogene Daten anonymisieren, es sei denn, die Anfrage zur Bereitstellung von Daten an eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine EU-Institution erfordert die Offenlegung personenbezogener Daten. In solchen Fällen ist der Dateninhaber verpflichtet, die Daten zu pseudonymisieren.

Es können nationale Gesetze erlassen werden, die die Offenlegung anderer Arten von Daten in bestimmten Situationen regeln, beispielsweise medizinische oder statistische Daten. Wenn diese Daten nicht aggregiert werden können und als personenbezogene Daten weitergegeben werden müssen, sollten geeignete technische und organisatorische Maßnahmen zu ihrem Schutz getroffen werden.

Frage 8: Was muss berücksichtigt werden, um die mit dem Data Act verbundenen Risiken zu minimieren?

Der Data Act schafft einen einheitlichen, kohärenten Rahmen für den Austausch personenbezogener und nicht personenbezogener Daten innerhalb des europäischen Binnenmarkts. Seine Ziele sind die Gewährleistung von Fairness in datengesteuerten Wertschöpfungsketten, die Verbesserung des Zugangs der Nutzer zu Daten, die von vernetzten Produkten und damit verbundenen Diensten generiert werden, sowie die Förderung von Innovationen in allen Sektoren.

Gleichzeitig erhöht die Bereitstellung von mehr Daten zwangsläufig das Risiko von Missbrauch, Datenschutzverletzungen, Verlust von Geschäftsgeheimnissen, Cybersicherheitsvorfällen und diskriminierendem oder ungleichen Zugang. Das Gesetz verbindet daher die neuen Zugriffsrechte mit einer Reihe von mehrschichtigen Schutzmaßnahmen, die je nach der Art der Beziehung, in der Daten ausgetauscht werden, variieren: Business-to-Consumer (B2C), Business-to-Business (B2B) und Business-to-Government (B2G).

Risikominderung in B2C- und B2B-Beziehungen

Im B2C-Kontext (Art. 3 und 4 Data Act) müssen vernetzte Produkte und damit verbundene Dienste so gestaltet sein, dass die Daten standardmäßig für die Nutzer in einem strukturierten, sicheren und maschinenlesbaren Format direkt zugänglich sind. Die Verbraucher müssen kostenlosen Zugang erhalten und vor unfairen oder undurchsichtigen Vertragsbedingungen geschützt werden. Sie müssen eine sinnvolle Kontrolle über ihre Daten behalten, einschließlich der Möglichkeit, den Zugang zu gewähren oder zu widerrufen und die Bedingungen für die Wiederverwendung zu verwalten.

In B2B-Beziehungen, in denen Ungleichgewichte bestehen können, erlaubt der Data Act den Parteien, vertragliche Beschränkungen für die Nutzung oder Weitergabe von Daten festzulegen, wenn diese Nutzung die Sicherheit, Gesundheit oder Geschäftsgeheimnisse gefährden könnte (Art. 4 Abs. 2 und Art. 4 Abs. 6 Data Act). Vereinbarungen müssen Vertraulichkeitsklauseln enthalten, und Unternehmen können die Weitergabe von Daten aussetzen, wenn die vereinbarten Maßnahmen nicht umgesetzt werden oder wenn Geschäftsgeheimnisse gefährdet sind (Art. 4 Abs. 7 Data Act). Das Gesetz verlangt, dass solche Bedingungen fair sind und keine Ausnutzung von Ungleichgewichten in der Verhandlungsmacht, insbesondere bei KMU, zulassen (Art. 5 Abs. 3 Data Act).

Technische und organisatorische Schutzmaßnahmen

Der Data Act erlaubt Dateninhabern, technische Schutzmaßnahmen wie Verschlüsselung, Zugriffskontrollen und Smart Contracts zu implementieren, um unbefugten Zugriff oder unbefugte Nutzung zu verhindern (Art. 11 Abs. 1 Data Act). Diese Maßnahmen dürfen den legitimen Zugriff von Nutzern nicht verhindern, sind jedoch für die Gewährleistung der Einhaltung der Vorschriften und den Schutz sensibler Informationen von entscheidender Bedeutung. Dateninhaber können auch auf Pseudonymisierung und sichere Datenübertragungsprotokolle zurückgreifen, insbesondere wenn es sich um sensible Informationen oder den Zugriff durch Dritte handelt.

Die Weitergabe von Daten unterliegt ebenfalls einer Zweckbindung. Dritte dürfen die Daten nur für die mit dem Nutzer vereinbarten Zwecke verarbeiten und müssen sie löschen, sobald sie nicht mehr benötigt werden (Art. 6 Abs. 1 Data Act). Bei personenbezogenen Daten ist die vollständige Einhaltung der DS-GVO obligatorisch. Bei Verstößen gegen diese Verpflichtungen können Dateninhaber die Löschung der Daten und die Einstellung der damit verbundenen Dienste oder Produkte verlangen (Art. 11 Absätze 2 bis 4 Data Act). Im B2B-Kontext können technische Maßnahmen auch Audit-Trails zur Überwachung der Einhaltung umfassen.

Verwaltung von Geschäftsgeheimnissen in verschiedenen Szenarien der gemeinsamen Nutzung

Unabhängig davon, ob Daten an Nutzer oder Dritte weitergegeben werden, sieht das Gesetz einen starken Schutz für Geschäftsgeheimnisse vor. Diese dürfen nur offengelegt werden, wenn dies unbedingt erforderlich ist und wenn geeignete technische und vertragliche Sicherheitsvorkehrungen getroffen wurden (Art. 4 Abs. 6 und Art. 5 Abs. 9 Data Act). Werden diese Schutzmaßnahmen nicht eingehalten, können die Dateninhaber die Weitergabe aussetzen und müssen die zuständige Behörde informieren (Art. 5 Abs. 10 Data Act). In Verträgen muss festgelegt werden, wie Geschäftsgeheimnisse geschützt werden, und es müssen Vertraulichkeitsverpflichtungen festgelegt werden.

Zugang des öffentlichen Sektors und die B2G-Dimension

In Ausnahmefällen können Behörden Daten anfordern, wenn ein eindeutiges öffentliches Interesse besteht (Art. 17 Data Act). Diese Anfragen müssen konkret, verhältnismäßig und gerechtfertigt sein. Die Behörde darf die Daten nur für den angegebenen Zweck verwenden, muss strenge Sicherheitsmaßnahmen anwenden und die Daten löschen, wenn sie nicht mehr benötigt werden (Art. 18 und 19 Data Act). Wenn möglich, müssen personenbezogene Daten anonymisiert oder pseudonymisiert werden. Öffentliche Stellen müssen außerdem ähnliche technische und organisatorische Maßnahmen wie private Akteure umsetzen und bei der Verarbeitung sensibler Daten die Vertraulichkeitsanforderungen einhalten.

Der Kontext ist entscheidend

Die im Data Act festgelegten Verpflichtungen und Schutzmaßnahmen sind kontextsensitiv. Bei der Weitergabe von Daten im B2C-Bereich steht die Stärkung der Nutzer und der Verbraucherschutz im Vordergrund. Bei B2B-Beziehungen werden faire Vertragsbedingungen und Vertraulichkeit betont. Der Zugang zu Daten im B2G-Bereich ist auf Ausnahmefälle beschränkt und

streng reguliert. Dieser mehrschichtige Ansatz ermöglicht eine wirksame Risikominderung, ohne ein einheitliches Modell vorzuschreiben.

Zusammenfassend lässt sich sagen, dass der Data Act durch die Festlegung maßgeschneiderter Regeln für verschiedene Kontexte der Datenweitergabe und die Förderung der Verwendung vertraglicher, technischer und organisatorischer Schutzmaßnahmen eine solide Rechtsgrundlage für die Minimierung von Risiken bietet. Die Umsetzung dieser Schutzmaßnahmen erfordert jedoch mehr als nur die Einhaltung der Rechtsvorschriften. Technische Lösungen wie APIs und standardisierte Zugangsmechanismen spielen eine wichtige Rolle bei der Gewährleistung einer sicheren, überprüfbaren und vertrauenswürdigen Datenweitergabe zwischen allen Akteuren.

Frage 9: Was ist eine gängige Methode für den Datenaustausch gemäß dem Data Act und wie lassen sich Datenschutzrisiken reduzieren?

Es gibt mehrere Möglichkeiten, die mit dem Data Act verbundenen Risiken zu verringern. Der erste Schritt ist die Umsetzung von Richtlinien zur Steuerung des Datenaustauschs. Wie bei der Einhaltung der DS-GVO kann eine solide Verwaltung des Datenaustauschs durch Verträge und Dokumentationen formalisiert werden, in denen die Rollen und Verantwortlichkeiten jeder Partei festgelegt sind. Dies ist besonders nützlich zwischen Dateninhabern und Dritten. Verträge können Verfahren zur Verwaltung des Zugriffs und, falls erforderlich, zur Zuweisung von Zugriffskontrollrechten, zur Festlegung von Sicherheitsanforderungen sowie zur Gewährleistung der Rechenschaftspflicht und Rückverfolgbarkeit enthalten.

Der Datenempfänger ist in der Regel ein Datenverarbeiter innerhalb des Austauschprozesses. Der Vertrag mit dem Dritten könnte jedoch eine gemeinsame Verantwortlichkeit für die Verarbeitung vorsehen, wenn der Dritte rechtlich oder praktisch einen bestimmenden Einfluss auf die Verarbeitungszwecke und -bedingungen ausübt. Dies könnte beispielsweise der Fall sein, wenn der Dritte eine Austausch-API bereitstellt, mit der sich der Dateninhaber für den Datenaustausch verbindet.

Maßnahmen zur Verhinderung unbefugten Zugriffs, empfohlen von verschiedenen nationalen Regulierungsbehörden: Wie bei der DS-GVO sollte ein risikobasierter Ansatz verfolgt werden, bei dem das erforderliche Schutzniveau der Schwere der möglichen Folgen für die betroffene Person oder den Nutzer angemessen ist. Die Empfehlung der französischen Datenschutzbehörde CNIL umfasst beispielsweise Folgendes:

- Teilen Sie die zu teilenden Daten durch physische oder logische Datensegmentierung oder beides auf. Die Verfügbarkeit von Daten kann in bestimmten Situationen wichtig werden, in denen der Nutzer ohne diese Daten ernsthaft beeinträchtigt werden könnte. In solchen Situationen kann die Aufbewahrung von Daten in separaten „Kompartimenten" potenzielle Datenverletzungen reduzieren.
- Verwenden Sie zusätzliche technische Maßnahmen wie einen digitalen Safe, um Passwörter und Authentifizierungsprotokolle zu schützen.

- Führen Sie ein umfassendes Protokoll über Zugriffe und Aktionen in der Datenbank, um Datenmissbrauch und Fehler zu identifizieren und sicherzustellen, dass der Dateninhaber/Datenempfänger (oder sein Beauftragter) die erforderlichen Datenaktualisierungen im Rahmen der kontinuierlichen Weitergabe bereitgestellt hat.
- Schaffung einer „Sandbox"-Umgebung für den Datenaustausch, in der Benutzer sicher mit den Daten experimentieren können.

Aufgrund der spezifischen Art der vom Data Act erfassten Daten ist die Datenübertragung über Anwendungsprogrammierschnittstellen (APIs) möglicherweise die am häufigsten verwendete Methode. APIs unterstützen den sicheren Austausch von personenbezogenen und nicht personenbezogenen Daten zwischen Dateninhabern und autorisierten Dritten. APIs bieten in der Regel ein höheres Maß an Sicherheit als Datenaustauschplattformen oder E-Mail-Dienste, wodurch das Risiko von Datenverletzungen während des Austauschs verringert werden kann.

APIs sind ein bevorzugtes Werkzeug für den Datenaustausch, insbesondere wenn:

- große Datenmengen häufig aktualisiert werden,
- Dritte regelmäßig auf die Daten zugreifen müssen, um Zugriffsanfragen von Benutzern zu erfüllen, insbesondere wenn eine hohe Anzahl solcher Anfragen vorliegt, und
- Der Dritte die Daten direkt an den Nutzer überträgt, ohne sie dauerhaft zu speichern.

Frage 10: Welche Pflichten hat der Dateninhaber?

Der EU-Data Act legt mehrere wichtige Pflichten für Dateninhaber fest.

Datenzugriff durch Design und als Standardeinstellung

Dateninhaber müssen vernetzte Produkte oder damit verbundene Dienste (z. B. intelligente Geräte) so konzipieren und herstellen, dass die vom Gerät generierten Daten standardmäßig und kostenlos für den Nutzer zugänglich sind. Dazu gehören auch relevante Metadaten, die für die Interpretation und Nutzung der Daten erforderlich sind. Der Zugriff muss einfach, sicher, umfassend und strukturiert sein und in einem gängigen und maschinenlesbaren Format erfolgen.

Anträge auf Datenzugriff

Wenn Nutzer nicht direkt über das intelligente Gerät auf die Daten zugreifen können, muss der Dateninhaber die Daten auf Anfrage zur Verfügung stellen. Diese Anfragen müssen ohne unangemessene Verzögerung, in einem gängigen und maschinenlesbaren Format, kostenlos und, sofern relevant und machbar, kontinuierlich und in Echtzeit erfüllt werden. Darüber hinaus können Nutzer vom Dateninhaber verlangen, dass er die vom Gerät generierten Daten an Dritte weitergibt. Bei der Erfüllung einer solchen Anfrage muss der Dateninhaber die Daten unter den oben beschriebenen Bedingungen bereitstellen. Im Gegensatz zur Weitergabe von Daten an den Nutzer kann der Dateninhaber in einem solchen Fall jedoch eine angemessene Vergütung von dem Dritten für die Weitergabe der Daten verlangen. Der Dateninhaber muss sicherstellen, dass Zugriffsanfragen auf unkomplizierte Weise bearbeitet werden können und nicht durch unnötige Verfahren oder Informationsanfragen des Nutzers erschwert werden.

Transparenz

Vor Abschluss eines Vertrags über den Kauf, die Miete oder das Leasing eines vernetzten Produkts muss der Dateninhaber dem Nutzer klare und verständliche Informationen zur Verfügung stellen. Dazu gehören Angaben zu Art und Umfang der Daten, zu den Aufbewahrungsfristen, dazu, ob das Produkt kontinuierlich und in Echtzeit Daten generiert und dazu, ob die Daten remote oder auf dem Gerät gespeichert werden. Der Nutzer muss auch darüber informiert werden, wie er seine Rechte auf Zugriff, Abruf oder Löschung von Daten ausüben kann.

Ebenso muss der Dateninhaber vor Abschluss eines Vertrags über Dienstleistungen im Zusammenhang mit einem vernetzten Produkt den Nutzer über die Art und den Umfang der Daten, die Aufbewahrungsfristen, Dritte, die die Daten verwenden dürfen, und die Zwecke, für die die Daten verwendet werden, informieren. Der Dateninhaber muss dem Nutzer auch erklären, wie er die Weitergabe von Daten an Dritte beantragen, die Weitergabe von Daten beenden und im Falle eines Verstoßes gegen den Data Act Beschwerde einlegen kann.

Datenübertragbarkeit

Der Data Act ermöglicht es Benutzern, ihre Daten an Dritte zu übertragen, was den Wechsel zwischen Dienstleistern oder die Verwendung von Daten mit verschiedenen Anwendungen erleichtert. Der Dateninhaber muss diesen Prozess nahtlos gestalten und sicherstellen, dass die Daten in einem gängigen und maschinenlesbaren Format bereitgestellt werden.

Frage 11: Wie formalisiert man die Weitergabe von Daten im Business-to-Business-Kontext?

Die Bedingungen für die Datenweitergabe müssen in einem Vertrag zwischen den beteiligten Parteien formalisiert werden. Die Vereinbarung muss fair, angemessen, nichtdiskriminierend und transparent sein, was besonders wichtig ist, wenn es sich bei der Vertragspartei um ein kleines oder mittleres Unternehmen, eine gemeinnützige Organisation oder eine Forschungseinrichtung handelt.

Wenn ein Dateninhaber Daten gemäß dem Data Act an ein anderes Unternehmen (den Datenempfänger) weitergibt, kann er vom Datenempfänger eine angemessene Gebühr für die bereitgestellten Daten verlangen.

Frage 12: Meine Organisation ist ein Dateninhaber. Kann ich die Bereitstellung von Daten verweigern?

Der Nutzer und der Dateninhaber können den Datenzugriff einschränken, wenn dieser Zugriff die gesetzlich vorgeschriebenen Sicherheitsanforderungen des Produkts gefährden könnte. Sie können auch vereinbaren den Zugriff, die Nutzung oder die Weitergabe von Daten zu beschränken oder zu untersagen.

In Fällen, in denen Geschäftsgeheimnisse betroffen sind, ist der Dateninhaber berechtigt, Vereinbarungen zur Wahrung der Vertraulichkeit der Daten und zum Schutz von Geschäftsgeheimnissen zu treffen. Dazu gehört auch die Vereinbarung technischer und organisatorischer Maßnahmen zur Gewährleistung der Vertraulichkeit.

Darüber hinaus ist der Dateninhaber nicht verpflichtet, Daten an Dritte außerhalb der EU weiterzugeben.

Frage 13: Welche Auswirkungen hat der Data Act auf die Verwaltung der Rechte betroffener Personen in Fällen, in denen es sich um personenbezogene Daten handelt?

Der Data Act ändert nichts an den in der DS-GVO festgelegten Rechten und Pflichten. Vielmehr stärkt und erleichtert es das Recht auf Datenübertragbarkeit gemäß Art. 20 DS-GVO. Konkret verpflichtet der Data Act die Dateninhaber, Kunden die Möglichkeit zu geben, ihre Daten innerhalb von 30 Tagen zu übertragen.

Beim Umgang mit personenbezogenen Daten fungiert der Dateninhaber in vielen Fällen als Verantwortlicher und muss Datenzugriffsanfragen gemäß der DS-GVO bearbeiten. Handelt es sich bei dem Nutzer um eine Organisation, wird diese zum Verantwortlichen. Der Verantwortliche muss überprüfen, ob personenbezogene Daten betroffen sind und sicherstellen, dass eine Rechtsgrundlage für die Bereitstellung dieser Daten besteht, insbesondere wenn der Nutzer nicht die betroffene Person ist.

Frage 14: Welche Rechtsgrundlagen können für die Verarbeitung personenbezogener Daten herangezogen werden, für die der Data Act gilt?

Der Data Act gilt unbeschadet der DS-GVO, d. h. die DS-GVO hat Vorrang vor dem Data Act (Art. 1 Abs. 5, Erwägungsgrund 7 Data Act). Folglich muss jede Verarbeitung personenbezogener Daten auf eine gültige Rechtsgrundlage gestützt werden.

Dafür stehen den Dateninhabern die Rechtsgrundlagen des Art. 6 DS-GVO zur Verfügung. Wenn die betroffene Person auch der einzige Nutzer ist, ist die Situation unkompliziert, da sich der Dateninhaber auf die Rechtsgrundlage der Einhaltung einer rechtlichen Verpflichtung berufen kann (siehe Art. 6 Abs. 1 lit. c DS-GVO, Art. 4 Data Act).

Wenn der Nutzer jedoch eine Organisation ist, in der mehrere Personen das verbundene Gerät nutzen, kann die Situation komplexer werden. Wenn ein Unternehmen beispielsweise ein gemeinschaftlich genutztes Fahrzeug einsetzt, muss es eine Rechtsgrundlage wählen, die die Daten der Mitarbeiter berücksichtigt. In solchen Fällen muss die Verarbeitung personenbezogener

Daten, die von Mitarbeitern bei der Nutzung eines Poolfahrzeugs generiert werden, möglicherweise auf einer Einwilligung (Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 DS-GVO) oder der Erfüllung eines Vertrags (Art. 6 Abs. 1 lit. b DS-GVO) beruhen. Es ist wichtig zu beachten, dass sich der Data Act stark auf vertragliche Vereinbarungen stützt und somit Art. 6 Abs. 1 lit. b DS-GVO für die Verarbeitung personenbezogener Daten im Rahmen eines Vertrags ergänzt. Beispielsweise kann ein Nutzer im Rahmen eines Vertrags personenbezogene Daten an Dritte weitergeben, um eine Dienstleistung zu erbringen, wobei Art. 6 Abs. 1 lit. b DS-GVO als Rechtsgrundlage dient.

Schließlich verarbeitet der Datenempfänger in den meisten Fällen die Daten im Auftrag des Dateninhabers oder Nutzers.

Frage 15: Meine Organisation ist ein Nutzer und möchte die vom Dateninhaber zur Verfügung gestellten Daten auf der Grundlage eines berechtigten Interesses verarbeiten. Ist das möglich?

Gemäß Art. 6 Abs. 1 lit. f DS-GVO des ersten UnterAbs.es von Art. 6 Abs. 1 DS-GVO kann die Verarbeitung nur dann als für die berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich angesehen werden, wenn

- der Verantwortliche die Nutzer über ein berechtigtes Interesse informiert hat, das mit der Datenverarbeitung verfolgt wird;
- die Datenverarbeitung nur insoweit erfolgt, als dies für die Zwecke dieses berechtigten Interesses unbedingt erforderlich ist und
- aus einer Abwägung der gegensätzlichen Interessen unter Berücksichtigung aller relevanten Umstände hervorgeht, dass die Interessen oder Grundfreiheiten und Rechte der Nutzer dieses berechtigte Interesse des Verantwortlichen oder eines Dritten nicht überwiegen.

Bei der Abwägungsprüfung werden im Wesentlichen die konkurrierenden Interessen des für die Verarbeitung Verantwortlichen gegen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen abgewogen.

Bewertung der Einschränkungen und Beschränkungen?

Die Verwendung von personenbezogenen Daten, die von vernetzten Geräten generiert werden, kann gemäß den geltenden EU- und nationalen Rechtsvorschriften eingeschränkt oder begrenzt werden. Beispielsweise können nationale Arbeitsgesetze die Überwachung von Mitarbeitern durch vernetzte Geräte am Arbeitsplatz regeln.

Darüber hinaus kann das berechtigte Interesse nicht als Rechtsgrundlage herangezogen werden, wenn die vom Dateninhaber erhaltenen Daten unter die besonderen Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO fallen. Dazu gehören biometrische Daten

und gesundheitsbezogene Daten, die von verbundenen medizinischen Geräten generiert werden.

Wenn die vom Dateninhaber erhaltenen Daten für automatisierte Entscheidungen verarbeitet werden, die rechtliche Auswirkungen auf die betroffene Person haben oder sie in ähnlicher Weise erheblich beeinträchtigen (z. B. automatisierte Bonitätsbewertung), kann das berechtigte Interesse ebenfalls nicht als gültige Rechtsgrundlage herangezogen werden.

In diesen Fällen ist eine andere Rechtsgrundlage erforderlich.

Beispiele für Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person

Die betroffenen Rechte und Freiheiten hängen grundsätzlich von den besonderen Umständen des Einzelfalls ab.[3]

Beispielsweise kann die Weitergabe oder Verwendung – ohne Zustimmung des Nutzers – der von einem vernetzten Auto oder einem Heimassistenten generierten personenbezogenen Daten eine Bedrohung darstellen:

- für das Privat- und Familienleben der betroffenen Personen, das durch Art. 7 der Charta der Grundrechte der Europäischen Union (GRCh) geschützt ist und
- für das Recht auf Sicherheit, das durch Art. 6 GRCh geschützt ist.

Wie der Datenschutzbeauftragte in diesem Prozess helfen kann

Die Abwägungsprüfung muss von Fall zu Fall durchgeführt werden, wobei alle möglichen Risiken für die betroffenen Personen zu berücksichtigen sind. Gemäß der Stellungnahme 06/2014 der WP29 zum Begriff der berechtigten Interessen des für die Verarbeitung Verantwortlichen sollte der für die Verarbeitung Verantwortliche:

- die Grundrechte und Interessen der betroffenen Person, die beeinträchtigt werden könnten, ermitteln
- die angemessenen Erwartungen der betroffenen Personen berücksichtigen
- die Auswirkungen auf die betroffene Person bewerten und sie mit den Vorteilen vergleichen, die der für die Verarbeitung Verantwortliche von der Verarbeitung erwartet.

Es ist wichtig zu beachten, dass Kinder einen besonderen Schutz ihrer personenbezogenen Daten verdienen, da sie sich der potenziellen Risiken möglicherweise weniger bewusst sind.

Die Rolle des Datenschutzbeauftragten bei der Bewertung berechtigter Interessen ist zwar nicht ausdrücklich in der DS-GVO geregelt, entspricht jedoch der Rolle des Datenschutzbeauftragten bei einer Datenschutz-Folgenabschätzung. Daher sollte der Datenschutzbeauftragte auf Anfrage des für die Verarbeitung Verantwortlichen Beratung hinsichtlich der Abwägungsprüfung leisten und deren Durchführung überwachen.

[3] Siehe Urteil vom 4. Mai 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, Rn. 31.

Frage 16: Meine Organisation ist eine öffentliche Einrichtung. In welchen Situationen kann meine Organisation Daten aufgrund einer „außergewöhnlichen Notwendigkeit" anfordern?

Das Konzept der „außergewöhnlichen Notwendigkeit" wird bereits zu Beginn des Data Acts eingeführt, wo in Art. 1 Abs. 1 Data Act dargelegt wird, dass ein Teil des Zwecks des Gesetzes darin besteht, die Vorschriften über die Verfügbarkeit von Daten, die sich im Besitz des Dateninhabers befinden, für öffentliche Stellen zu harmonisieren, wenn eine „außergewöhnliche Notwendigkeit" für die Daten besteht, um eine bestimmte Aufgabe im öffentlichen Interesse zu erfüllen. Dies setzt einen hohen Standard, da die Bereitstellung auf öffentliche Einrichtungen beschränkt ist und eine „außergewöhnliche Notwendigkeit" speziell für eine Aufgabe im öffentlichen Interesse erforderlich ist. Die zur Verfügung gestellten Daten dürfen nur zur Erfüllung dieses außergewöhnlichen Bedarfs verwendet werden.

Wenn es alternative Mittel zur Erfüllung der Aufgabe gibt, könnte man argumentieren, dass diese Bestimmung nicht gilt. Der Begriff „außergewöhnlich" schließt wahrscheinlich eine normale, regelmäßige Nutzung aus, was bedeutet, dass nur wirklich außergewöhnliche Umstände in Frage kommen. Darüber hinaus muss es eine vorab festgelegte, identifizierte Aufgabe geben, die sowohl außergewöhnlich ist als auch diesen Bedarf auslöst. Wenn eine öffentliche Stelle einer solchen „außergewöhnlichen Notwendigkeit" und eine „spezifische Aufgabe" nicht im Voraus klar identifizieren und dokumentieren kann, kann sie sich möglicherweise nicht auf diese Bestimmung berufen.

Darüber hinaus sollte die Bestimmung zum Geltungsbereich in Verbindung mit den spezifischen Details darüber gelesen werden, was einen außergewöhnlichen Bedarf ausmacht und wann er gilt, wie später im Data Act näher erläutert wird. Art. 1 Abs. 3 Data Act bekräftigt diese potenziellen Einschränkungen und besagt, dass Daten nur im Falle einer „außergewöhnlichen Notwendigkeit der Nutzung" zur Verfügung gestellt werden dürfen. Dies gibt Anlass zur Vorsicht, dass die Bestimmung zum Geltungsbereich unbeabsichtigt die Anwendung späterer Bestimmungen einschränken könnte, möglicherweise in einer Weise, die vom Gesetzgeber nicht beabsichtigt war.

Die wichtigsten Definitionen im Data Act definieren den Begriff „außergewöhnlicher Bedarf" nicht ausdrücklich. Art. 2 Abs. 29 Data Act fasst jedoch den „öffentlichen Notstand" und „Ausnahmesituationen" zusammen, was dazu führen könnte, dass einige die außergewöhnliche Notwendigkeit als vom öffentlichen Notstand erfasst interpretieren. Der Begriff „außergewöhnliche Umstände" wird auch in verschiedenen Zusammenhängen erwähnt, beispielsweise in Art. 4 Abs. 8 und Art. 5 Abs. 11 Data Act, einschließlich solcher, die sich auf geistiges Eigentum beziehen.

Die wichtigsten Bestimmungen zu außergewöhnlichen Erfordernissen sind in Kapitel V aufgeführt. Art. 14 Data Act mit dem Titel „Pflicht zur Bereitstellung von Daten wegen außergewöhnlicher Notwendigkeit" besagt, dass öffentliche Stellen, die Kommission, die Europäische

Zentralbank oder Einrichtungen der Union, die ein außergewöhnliches Erfordernis im Sinne von Art. 15 Data Act für die Nutzung bestimmter Daten – einschließlich der für die Interpretation und Nutzung dieser Daten erforderlichen Metadaten – nachweisen, einen ordnungsgemäß begründeten Antrag stellen müssen. Rechtsträger, die keine öffentlichen Stellen sind und über die relevanten Daten verfügen, sind dann verpflichtet, diese zur Verfügung zu stellen.

Art. 15 Data Act legt fest, dass die „außergewöhnliche Notwendigkeit" sowohl zeitlich als auch vom Umfang her begrenzt sein muss und nur unter bestimmten Umständen bestehen kann, die in einer festen Liste klar aufgeführt sind. So befasst sich beispielsweise Art. 15 Abs. 1 lit. a Data Act mit der Reaktion auf einen öffentlichen Notfall, während Art. 15 Abs. 1 lit. b Data Act andere Umstände abdeckt, die keine personenbezogenen Daten betreffen dürfen. Bemerkenswert ist, dass es gemäß Art. 15 Abs. 2 Data Act eine Ausnahme für Kleinst- und Kleinunternehmen gibt, obwohl selbst kleine Unternehmen mit einem bescheidenen Umsatz erhebliche Datenmengen verwalten können.

In Art. 17 Data Act wird betont, dass die öffentliche Stelle die außergewöhnliche Notwendigkeit „nachweisen" muss, was einen höheren Beweisstandard impliziert, als eine Notwendigkeit einfach als außergewöhnlich zu bezeichnen. Diese Anforderung könnte Situationen ausschließen, die nicht wirklich außergewöhnlich sind. Art. 17 Abs. 1 lit. c Data Act erwähnt ausdrücklich die Notwendigkeit, zu erläutern, wie personenbezogene Daten verarbeitet werden, was möglicherweise zu strittigen Fragen hinsichtlich der Auslegung und Anwendung führen kann. Darüber hinaus erwähnt Art. 17 Abs. 2 lit. e Data Act die Anforderung der Pseudonymisierung, und Art. 17 Abs. 2 lit. c Data Act betont die Bedeutung der Verhältnismäßigkeit bei der Beurteilung der außergewöhnlichen Notwendigkeit, wodurch deren Anwendung weiter eingeschränkt wird.

Art. 18 Abs. 2 Data Act befasst sich mit dem Verfahren zur Beantwortung von Datenanfragen, einschließlich Fristen, Änderungen und Unterscheidungen zwischen außergewöhnlichen Erfordernissen im Falle eines öffentlichen Notstands und anderen Arten von außergewöhnlichen Erfordernissen. Eine Entschädigung für die Bereitstellung von Daten kann ebenfalls in Betracht gezogen werden, wie in Art. 20 Data Act dargelegt. Darüber hinaus wird in Art. 21 Data Act die Weitergabe von Daten an Forschungs- und Statistikorganisationen im Zusammenhang mit außergewöhnlichen Erfordernissen behandelt.

Verweise auf außergewöhnliche Bedürfnisse finden sich im gesamten Data Act, insbesondere in den Erwägungsgründen 5, 31, 63, 65, 66, 69, 70-73, 75, 77, 103 und 107 des Data Acts. Diese Verweise und die spezifischen Art. bilden zusammen den Rahmen für das Verständnis und die Anwendung des Konzepts des außergewöhnlichen Bedarfs im Data Act.

Frage 17: Wie wird Profiling im Data Act definiert?

Sowohl in der DS-GVO als auch im Data Act wird dieselbe Definition für Profiling verwendet, nämlich Art. 4 Abs. 4 der DS-GVO, der Profiling als *„jede Form der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte einer natürlichen Person zu bewerten, insbesondere um Aspekte bezüglich ihrer Arbeitsleistung, wirtschaftlichen Situation, Gesundheit, persönlichen Vorlieben,*

Interessen, Zuverlässigkeit, ihres Verhaltens, ihres Aufenthaltsorts oder ihrer Bewegungen zu analysieren oder vorherzusagen" definiert.

Frage 18: Ist Profiling nach dem Data Act verboten?

Profiling ist gemäß dem Data Act grundsätzlich nicht verboten. In einem ganz bestimmten Kontext ist Profiling jedoch nicht zulässig, nämlich wenn *der Nutzer* (oftmals die betroffene Person) die Daten an Organisationen weitergibt. Art. 6 Abs. 2 Buchstabe b Data Act stärkt die Rechte der Nutzer und bietet ihnen eine weitere Möglichkeit, sich besser vor unerwünschten Profiling-Praktiken zu schützen.

Diese Situation ist in Art. 6 Abs. 2 lit. b Data Act festgelegt:

6.2 Der Dritte darf nicht:

...(b) ungeachtet Art. 22 Abs. 2 Buchstaben a und c der Verordnung (EU) 2016/679 *die erhaltenen Daten für die Profilerstellung verwenden, es sei denn, dies ist für die Erbringung der vom Nutzer angeforderten Dienstleistung erforderlich;*

Zur Verdeutlichung der Auslegung führen wir im Folgenden die relevanten Teile von Art. 22 der DS-GVO auf. Art. 22 Abs. 1 DS-GVO lautet:

1. Die betroffene Person hat das Recht, ***nicht*** *einer Entscheidung unterworfen zu* ***werden****, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruht und ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.*

In **Art. 22 Abs. 2 Buchstaben a und c** der DS-GVO heißt es:

(a) Abs. 1 gilt nicht, wenn die Entscheidung: für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen erforderlich ist;
(b) ...
(c) auf der ausdrücklichen Einwilligung der betroffenen Person beruht.

Die gemeinsame Auslegung beider Texte kann zu Verwirrung führen, insbesondere angesichts der Vielzahl der darin enthaltenen negativen Aussagen. Die Klausel „ungeachtet des Art. 22 Abs. 2 Buchstaben a und c der Verordnung (EU) 2016/679" ist als „trotz des Art. 22 Abs. 2 Buchstaben a und c" zu verstehen. Unter normalen Umständen sind in Art. 22 Abs. 2 DS-GVO zwei Ausnahmen zu Art. 22 Abs. 1 DS-GVO aufgeführt. Diese beiden Ausnahmen gelten jedoch nicht im Zusammenhang mit Art. 6 Abs. 2 lit. b Data Act.

Zur weiteren Klarstellung sollte Art. 6 Abs. 2 lit. b i. V. m. Art. 5 des Data Act ausgelegt werden. Dabei wird deutlich, dass Profiling in Situationen verboten ist, in denen die folgenden drei kumulativen Kriterien zutreffen, wobei

- Die betreffenden personenbezogenen Daten sind Teil eines Produkts (z. B. einer automatischen Espressomaschine) oder von Dienstleistungsdaten, die durch die Nutzung vernetzter Produkte erstellt wurden,

- die personenbezogenen Daten vom Nutzer der Espressomaschine an Ihr Unternehmen weitergegeben werden und Ihr Unternehmen nicht der Dateninhaber ist und
- die Profilerstellung für die Erbringung der vom Betroffenen angeforderten Dienstleistung nicht erforderlich ist.

Nachdem diese Auslegung geklärt ist, besteht die nächste wichtige Frage darin, zu bestimmen, was „*notwendig für die Erbringung der vom Nutzer angeforderten* Dienstleistung" ist. Dies wird wahrscheinlich von Fall zu Fall interpretiert werden. Beispielsweise gibt ein *Nutzer* eines Musik-Streaming-Dienstes seine Nutzungsdaten an ein anderes Medienunterhaltungsunternehmen weiter, damit er die gleichen personalisierten Empfehlungen erhalten kann. Dies erfordert, dass das Medienunterhaltungsunternehmen (*Datenempfänger*) ein Profiling durchführt. Da die Anfrage vom *Nutzer* stammt und das Profiling für die Erbringung der angeforderten Dienstleistung erforderlich ist, ist diese Art des Profilings durch den *Datenempfänger* höchstwahrscheinlich zulässig. Das Medienunterhaltungsunternehmen darf jedoch kein Profiling durchführen, um herauszufinden, zu welcher Tageszeit Podcasts angehört werden, damit das Medienunterhaltungsunternehmen seine Betriebsprozesse verbessern kann. Dies würde wahrscheinlich gegen Art. 6 Abs. 2 lit. b Data Act verstoßen.

Die zugrunde liegende Annahme könnte sein, dass *Datenempfänger* nicht die ursprünglichen Dateninhaber sind und daher höchstwahrscheinlich nur begrenzte Kontrolle oder Verständnis darüber haben, wie die Daten erhoben wurden oder wie der Nutzer sie verwenden wollte. Die Erstellung von Profilen für Dienste, die nicht mit dem Produkt oder der Dienstleistung in Verbindung stehen, für die sich der Nutzer angemeldet hat, würde zu Recht als Eingriff in seine Datenschutzrechte gemäß der DS-GVO angesehen werden.

Betrachten Sie das folgende Szenario: Ein Versorgungsunternehmen könnte möglicherweise Thermostatdaten von Wohnhäusern zum Energieverbrauch zu seinem eigenen finanziellen Vorteil nutzen. Das Unternehmen könnte die Energieverbrauchsgewohnheiten analysieren, Spitzenverbrauchszeiten, d. h. Abende und Wochenenden, ermitteln und diese Informationen den Hausbesitzern zur Verfügung stellen. Es könnte sogar in der Lage sein, die Energieverbrauchsgewohnheiten ähnlicher Haushalte oder Gebäudetypen für Hausbesitzer als Benchmarks zu vergleichen. Stellen Sie sich eine Situation vor, in der ein Kunde des Versorgungsunternehmens zu einem anderen Versorgungsunternehmen wechselt. Es kann eine Anfrage zur Weitergabe der Thermostatdaten gestellt werden, damit das neue Versorgungsunternehmen Energiespartipps geben kann und der Kunde diese vom ersten Tag an nutzen kann. Wenn zu diesem Zweck eine Profilerstellung erforderlich ist, ist dies in diesem Szenario zulässig.

Das neue Versorgungsunternehmen könnte dann die Erstellung eines Treueprofils in Betracht ziehen, das dazu verwendet werden kann, Anreiz-Energiepläne auszuwählen, die die Person an eine längere Vertragslaufzeit mit einem ermäßigten Tarif binden können. Wenn der Hausbesitzer zu dem neuen Plan wechselt, profitiert das neue Versorgungsunternehmen von finanzieller Stabilität und der Hausbesitzer von geringeren Kosten. Da die Erstellung eines Profils jedoch streng genommen für die Erbringung der Dienstleistung für den Hausbesitzer nicht erforderlich ist, verbietet der Data Act diese Profilerstellung durch das neue Versorgungsunternehmen.

Frage 19: Warum ist Transparenz im Rahmen des Data Acts so wichtig?

Wenn wir traditionell über Daten und Transparenz nachdenken, konzentrieren wir uns auf Transparenzregeln, die sich auf die Bereitstellung von Vorabinformationen über die Verwendung personenbezogener Daten und die Einholung einer klaren und fairen Einwilligung zu deren Erhebung beziehen. Transparenz spielt auch eine Rolle dabei, sicherzustellen, dass Einzelpersonen sich ihrer Rechte bewusst sind und diese ausüben können. Darüber hinaus ist Transparenz in Datenverträgen, Richtlinien und Geschäftsbedingungen zwischen Unternehmen sowie zwischen Unternehmen und Einzelpersonen von entscheidender Bedeutung.

Im Zusammenhang mit dem Data Act verschiebt sich der Zweck der Transparenz jedoch leicht. Während die traditionellen Datenschutzvorschriften weiterhin gelten, betont der Data Act die Transparenz im Zusammenhang mit dem Datenaustausch zwischen Unternehmen. So hebt beispielsweise Art. 5 Data Act die Notwendigkeit von Transparenz und fairen, nichtdiskriminierenden Bedingungen hervor, wenn Dateninhaber Daten für Datenempfänger zur Verfügung stellen, insbesondere bei Datenübertragungen zwischen Unternehmen. Hier entspricht Transparenz möglicherweise eher den Wettbewerbsregeln als den traditionellen Datenschutzvorschriften.

Es kann zu Meinungsverschiedenheiten hinsichtlich dieser Auslegung kommen, aber diese Fragen werden sich höchstwahrscheinlich klären, wenn die gemäß Art. 10 Data Act eingerichteten Streitbeilegungsstellen beginnen, über solche Angelegenheiten wie Transparenz zu entscheiden. Es wird wichtig sein zu sehen, ob diese Verfahrensregeln nur den Data Act berücksichtigen oder ob sie auch Datenschutzvorschriften berücksichtigen werden.

Art. 28 des Data Acts bezieht sich auf das traditionelle Modell der Vorabinformationen, insbesondere in Bezug auf vertragliche Verpflichtungen im Zusammenhang mit dem internationalen Datenzugriff und -transfer. Obwohl in diesem Abschnitt der Begriff „Transparenz" nicht ausdrücklich erwähnt wird, sind die Verpflichtungen zur Vorabinformation über Websites klar und Praktiker müssen diese Anforderungen vollständig erfüllen, um potenzielle Probleme zu vermeiden.

Transparenz wird auch in Art. 19 Data Act behandelt, der „Transparenzverpflichtungen" einführt, die unter bestimmten Umständen die Aufbewahrung von Daten vorschreiben können und möglicherweise die Anforderungen zur Löschung oder Vernichtung von Daten außer Kraft setzen. Dies gilt insbesondere für öffentliche Stellen.

Darüber hinaus können solche Anforderungen auch dann notwendig oder impliziert sein, wenn keine ausdrücklichen Transparenzanforderungen bestehen, damit andere Bestimmungen wirksam funktionieren können. So kann es beispielsweise schwierig sein, eine Maßnahme zu rechtfertigen, wenn bestimmte Aspekte nicht in ausreichender Weise transparent waren. Dies hängt eng mit dem Konzept des Verständnisses und der Achtung der angemessenen Erwartungen von Personen zusammen. Ein praktisches Beispiel ist die Frage, ob die historische Nutzung von Daten auf eine neue KI-Anwendung ausgeweitet werden kann, ohne diese Erwartungen zu verletzen.

Schließlich wird Transparenz auch in mehreren Erwägungsgründen des Data Acts erwähnt, darunter in den Erwägungsgründen 5, 24, 25, 34, 42, 51, 65, 69 und 73 Data Act, die Leser zur weiteren Kontextualisierung lesen sollten.

Nützliche Links

- Text des Data Acts https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
- Informationen zur europäischen Datenstrategie https://digital-strategy.ec.europa.eu/en/policies/strategy-data
- Website der Europäischen Kommission zum Data Act https://digital-strategy.ec.europa.eu/en/policies/data-act, einschließlich einer FAQ zum Data Act unter https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act
- Verordnung über den Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union https://eur-lex.europa.eu/eli/reg/2018/1807/oj
- Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN
- DS-GVO https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Leitlinien der CNIL: Empfehlung zur Verwendung von Anwendungsprogrammierschnittstellen (API) für den sicheren Austausch personenbezogener Daten (auf Französisch) https://www.cnil.fr/sites/cnil/files/2023-07/recommandation_api.pdf

Haftungsausschluss

Die in diesen FAQ enthaltenen Informationen dienen ausschließlich der allgemeinen Information und Aufklärung. Sie sind nicht als Rechtsberatung zu verstehen. Für eine auf Ihre Situation zugeschnittene Beratung wenden Sie sich bitte an einen qualifizierten Rechtsbeistand.