Swico
Lagerstrasse 33
CH-8004 Zürich

Tel.: +41 44 446 90 90
www.swico.ch
info@swico.ch

Q&A Data Act der EU

Inhalt

1 Betroffenheitsanalyse

1.1 Wer ist betroffen?

- Der Data Act hat weitreichende Wirkung auf alle Akteure der digitalen Wirtschöpfungskette. Er betrifft **Unternehmen**, Nutzer, Datenverarbeiter und den öffentlichen Sektor. Im Einzelnen:
- **Hersteller vernetzter Produkte X** [siehe Ziffer 1.2]**, und Anbieter verbundener Dienste** [siehe Ziffer 1.3]: Unternehmen, die vernetzte Produkte, insbesondere IoT Produkte (z.B. Smart-Home-Geräte, Autos, Maschinen) herstellen oder digitale Dienste (z.B. Apps) anbieten, die für diese Produkte notwendig sind;
- **Nutzer vernetzter Produkte** [siehe Ziffer 1.3] **oder verbundener Dienste**: Verbraucher oder Unternehmen, die vernetzte Produkte oder verbundene Dienste verwenden;
- **Dateninhaber**: Unternehmen, die Daten nutzen oder bereitstellen, meist Hersteller vernetzter Produkte oder Anbieter verbundener Dienste;
- **Datenempfänger**: Personen oder Unternehmen, die auf Verlangen des Nutzers Daten vom Dateninhaber erhalten – darunter auch Konkurrenten oder Datenvermittlungsdienste,
- **Öffentliche Stellen und Behörden**: Institutionen, die in Ausnahmefällen Daten einfordern können,
- **Anbieter von Datenverarbeitungsdiensten**: umfasst zahlreiche Dienste, unter Anderem:
  - «Infrastructure-as-a-Service» (IaaS),
  - «Platform-as-a-Service» (PaaS) und
  - «Software-as-a-Service» (SaaS),
- **Teilnehmer an Datenräumen und Anbieter von Anwendungen, die intelligente Verträge verwenden**: Personen oder Unternehmen, die smarte Verträge entwickeln oder nutzen.

Kleine und mittlere Unternehmen (KMU) profitieren von Erleichterungen gemäss Artikel 2 der Empfehlung 2003/361/EG. Sie müssen in bestimmten Fällen keine Daten an Verbraucher oder Unternehmen weitergeben (vgl. Art. 7 Data Act).

1.2 Auf welche Produkte findet der Data Act Anwendung?

Der Data Act gilt für **alle vernetzten Produkte**, die Nutzungs- oder Umgebungsdaten erfassen und übermitteln können. Ein «vernetztes Produkt» sammelt oder erzeugt Daten und gibt diese weiter über physische Verbindungen, elektronische Kommunikation oder interne Zugänge (z.B. Smart-Home-Geräte, Autos, vernetzte Maschinen).

Ausgenommen sind IT-Infrastrukturen, deren Hauptaufgabe die Datenverarbeitung, Speicherung oder Übertragung im Auftrag Dritter ist, wie Server oder Cloud-Infrastrukturen.

1.3 Was sind verbundene Dienste?

Verbundene Dienste sind digitale Angebote, die so eng mit einem vernetzten Produkt verknüpft sind, dass dieses ohne den Dienst bestimmte Funktionen nicht ausführen kann. Beispiele sind Apps, die für das Produkt essenziell sind.

Vom Data Act umfasst sind auch Dienste, die erst nach dem Erwerb eines Produkts hinzugefügt werden. Solche Dienste können beim Kauf, Mieten oder Leasen enthalten sein. Alternativ können sie später durch den Hersteller oder Dritte ergänzt werden, mit dem Ziel, die Funktion des Produkts zu erweitern, anzupassen oder zu aktualisieren.

1.4 Welche Arten von Daten fallen in den Anwendungsbereich des Data Act?

Der Data Act umfasst Daten, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert werden. Darunter fallen sowohl personenbezogene Daten, als auch blosse Maschinendaten.

Der Data Act betrifft nicht nur direkte Nutzungsdaten, sondern auch indirekt generierte Daten. Dazu gehören Daten über die Umgebung oder Interaktionen des Produkts.

Die Zugangsansprüche des Data Act beschränken sich jedoch auf «Rohdaten». Dazu zählen allerdings auch aufbereitete Daten, die notwendig sind, um diese zu verstehen, wie physikalische Grössen (z.B. Temperatur, Öldruck, Geschwindigkeit, Position). Aus Rohdaten abgeleitete Daten, die erheblichen Aufwand und Investitionen erfordern (z.B. solche, die durch den Einsatz proprietärer und komplexer Algorithmen generiert werden) sind ausgeschlossen. Der Dateninhaber soll nicht verpflichtet werden, erhebliche Investitionen in diese Prozesse zu tätigen.

Beispiel:

Ein Autofahrer nutzt ein modernes, vernetztes Fahrzeug. Während der Nutzung werden verschiedene Arten von Daten generiert:

- **Technische Daten**: Dazu gehören Werte wie Motortemperatur, Öldruck, Reifendruck und Kraftstoffverbrauch,
- **Fahrdaten:** Diese umfassen Geschwindigkeit, Bremsverhalten, Beschleunigung und GPS-Position,
- **Nutzungsdaten:** Hierunter fallen Informationen wie Häufigkeit der Nutzung bestimmter Funktionen, z.B. Klimaanlage oder Infotainmentsystem.

Das Fahrzeug erfasst und speichert diese Daten kontinuierlich. Gemäss dem Data Act hat der Autofahrer das Recht, auf diese Daten zuzugreifen. Er kann sie beispielsweise an eine unabhängige Werkstatt weitergeben, um eine präzisere Diagnose bei Reparaturen zu ermöglichen. Ebenso kann er Fahrdaten an seine Versicherung übermitteln, um möglicherweise von einem nutzungsbasierten Tarif zu profitieren.

Daten, die nicht unter den Data Act fallen:

Der Data Act erfasst keine **abgeleiteten Daten**, die durch aufwändige Analysen oder Algorithmen aus den Rohdaten generiert werden. Beispiele für solche abgeleiteten Daten könnten sein:

- **Fahrerprofile:** Aus Werten wie Beschleunigung, Bremsverhalten und Geschwindigkeit könnte ein proprietärer Algorithmus ein Fahrerprofil erstellen. Dieses könnte die Fahrweise als «sportlich», «defensiv» oder «aggressiv» einstufen,
- **Verschleissprognosen:** Eine eigens trainierte KI könnte auf Basis von Motortemperatur, Öldruck und Fahrverhalten den zukünftigen Verschleiss von Fahrzeugkomponenten vorhersagen,
- **Personalisierte Werbung**: Fahrtrouten und häufig besuchte Orte könnten zur Erstellung von Interessenprofilen genutzt werden, die zielgerichtete Werbung ermöglichen.

Das Beispiel dient lediglich der illustrativen Darstellung des Data Act. Ob die hier genannten Daten in die Kategorie der Rohdaten bzw. der abgeleiteten Daten fallen, muss im Einzelfall geprüft werden. Das gleiche gilt für die Anwendung und Auswirkung sektorspezifischer Vorschriften im Automotive- und Mobilitätssektor.

1.5 Inwiefern sind Schweizer Unternehmen betroffen?

Ähnlich wie die DSGVO hat der Data Act exterritoriale Wirkung. Er gilt für Schweizer Hersteller vernetzter Produkte, die in der EU[1] verkauft werden, und für Anbieter verbundener Dienste, die ihre Leistung in der EU anbieten. Der Data Act betrifft auch Schweizer Dateninhaber, die Daten entsprechenden Empfängern innerhalb der EU bereitstellen sowie Anbieter von Datenverarbeitungsdiensten, die ihre Dienste Kunden in der EU anbieten.

1.6 Was ist ein sogenannter Gatekeeper?

Gatekeeper (deutsch «Torwächter») sind Unternehmen, die gemäss Art. 3 der Verordnung (EU) 2022/1925 (Gesetz über digitale Märkte, «DMA») definiert werden.

Ein Unternehmen wird als Gatekeeper eingestuft, wenn es:

a) einen erheblichen Einfluss auf den Binnenmarkt hat,
b) einen zentralen Plattformdienst bereitstellt, der für gewerbliche Nutzer ein wichtiges Zugangstor zu Endnutzern ist, und
c) eine gefestigte und dauerhafte Marktposition innehat oder voraussichtlich erlangen wird.

Am 6. September 2023 hat die EU-Kommission sechs Gatekeeper benannt: Alphabet, Amazon, Apple, ByteDance, Meta und Microsoft. Später wurden Apple (iPadOS) und Booking (booking.com) hinzugefügt.

1.7 Welche besonderen Vorschriften gelten für Gatekeeper?

Der Data Act fördert eine breitere Verteilung der Datenwertschöpfung unter den Marktteilnehmern, insbesondere zugunsten von KMU. Gatekeeper haben keinen Anspruch auf Zugang zu Daten. Nutzer und Dritte dürfen Daten, die sie auf Verlangen erhalten haben, nicht an Gatekeeper weitergeben.

---

[1] Der Data Act ist zum Zeitpunkt der Verfassung dieses Q&A in den EWR-Staaten noch nicht in Kraft. Sobald dies der Fall sein wird, sind mit «EU» jeweils auch die «EWR-Staaten» gemeint.

2 Gewährung von Zugangsrechten

2.1 Welche Pflichten müssen Unternehmen beim Datenzugang umsetzen?

Der Data Act gibt Nutzern vernetzter Produkte – ob Privatperson oder Unternehmen – die Nutzungs- und Verfügungsrechte an den mit diesen Produkten generierten Daten. Das herstellende Unternehmen oder der Dateninhaber muss den Zugang zu diesen Daten und deren Weitergabe ermöglichen. Für technische Daten schafft der Data Act damit ein neues Regelwerk für den Datenzugang und die Weitergabe.

Ein herstellendes Unternehmen oder ein Dateninhaber kann dem Nutzer auf zwei Arten Zugang zu den Daten ermöglichen:

- **Direkter Zugang («Data Access by Design»):** Die Daten werden dem Nutzer direkt zugänglich gemacht, beispielsweise über eine integrierte Schnittstelle,
- **Indirekter Zugang («Indirect Access»):** Die Daten werden auf Anfrage bereitgestellt.

In beiden Fällen kann der Nutzer verlangen, dass der Dateninhaber die Daten auch an einen Datenempfänger – also einen Dritten – weitergibt. Dadurch entsteht ein Vertragsnetz zwischen dem Dateninhaber, dem Nutzer und dem Datenempfänger.

Zusätzlich besteht eine **Bereitstellungspflicht in Krisensituationen oder bei öffentlichen Notständen**. In solchen Fällen müssen Dateninhaber relevante Daten bereitstellen, um die Situation zu bewältigen.

a) Direktes Zugangsrecht («Data Access by Design», B2C und B2B)

Das Prinzip «Data Access by Design» erlaubt Nutzern einen direkten Zugang zu Daten («B2C»), wenn der Zugang technisch machbar ist. Produkte und Dienstleistungen müssen so entwickelt werden, dass die Datenzugänglichkeit bereits im Herstellungsprozess integriert wird.

Der Zugriff auf Produkt- und Dienstdaten (inkl. Metadaten) muss:

- einfach, sicher und unentgeltlich sein,
- in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format erfolgen, und
- unter dem Vorbehalt, dass relevant und technisch durchführbar, direkt möglich sein.

Diese Vorgaben werden durch eine Informationspflicht («Transparency Obligation») flankiert. Nutzer müssen vor Vertragsabschluss informiert werden, welche Daten ein Produkt oder Dienst generiert. Ohne diese Information wäre ein effektiver Zugang nicht möglich.

Beispiel für direktes Zugangsrecht:

- **Vernetztes Auto:** Eine integrierte Schnittstelle oder App erlaubt dem Fahrer den direkten Zugriff auf technische Daten (z.B. Motortemperatur, Öldruck), Fahrdaten (z.B. Geschwindigkeit, GPS-Position) und Nutzungsdaten (z.B. Kraftstoffverbrauch).
- **Smart-Kühlschrank**: Ein Display oder eine App bieten Zugang zu Daten wie Temperatur, Energieverbrauch, Füllstand und Haltbarkeitsdaten der Lebensmittel.
- **Smartwatch:** Der Nutzer kann Gesundheits- und Aktivitätsdaten wie Herzfrequenz, Schritte und Schlafmuster direkt einsehen.

b) Indirektes Zugangsrecht (Bereitstellungspflicht)

Wenn Daten nicht direkt zugänglich sind, muss der Dateninhaber dem Nutzer alle ohne Weiteres verfügbaren Daten auf einfaches Verlangen bereitstellen. Der Nutzer kann diese selbst weitergeben oder verlangen, dass der Dateninhaber sie einem Datenempfänger seiner Wahl bereitstellt. Der Datenempfänger verarbeitet die Daten zu den vom Nutzer festgelegten Zwecken. Dabei behält der Nutzer stets die Verfügungsbefugnis über die Daten. Der Dateninhaber darf die Entscheidungen des Nutzers weder behindern noch manipulieren.

Die Bereitstellung der Daten muss:

- unverzüglich, einfach und sicher erfolgen,
- für den Nutzer unentgeltlich sein (nicht aber für den Drittempfänger), und
- in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format erfolgen.

Wenn die Daten an einen Datenempfänger oder Dritten übermittelt werden, müssen sie in derselben Qualität bereitgestellt werden, wie sie dem Dateninhaber zur Verfügung stehen. Dies gilt jedoch nur, wenn es relevant und technisch durchführbar ist. Die Formulierung «relevant und technisch durchführbar» gewährt dem Dateninhaber einen gewissen Spielraum. Dies erlaubt es, die Bereitstellung an die technischen Möglichkeiten des jeweiligen Produkts anzupassen. Der direkte Zugriff oder die Echtzeit-Bereitstellung ist nicht bei allen vernetzten Produkten möglich.

Der Dateninhaber hat somit Flexibilität und kann die Daten entweder direkt («Data Access by Design») oder indirekt («Indirect Access») zugänglich zu machen. Wenn technisch durchführbar und relevant, erfolgt die Datenbereitstellung kontinuierlich und in Echtzeit.

Beispiele für indirektes Zugangsrecht:

- **Vernetztes Fahrzeug:** Ein Autohersteller bietet ein Online-Portal an, über das der Fahrzeugbesitzer auf Daten wie Motorleistung, Kraftstoffverbrauch oder Wartungsinformationen zugreifen kann.
- **Smart Home-Geräte**: Der Hersteller eines intelligenten Thermostats stellt eine App bereit, über die Nutzer historische Daten zu Energieverbrauch oder Nutzungsmustern anfordern können.
- **Industriemaschine**: Ein Maschinenhersteller stellt ein Webportal bereit, über das Betreiber nach Genehmigung spezifische Produktions- und Leistungsdaten einsehen können.
- **Landwirtschaftliche Geräte**: Ein Hersteller von vernetzten Landmaschinen ermöglicht Landwirten, über ein Online-System detaillierte Boden- und Erntedaten abzurufen.

c) Bereitstellungspflicht bei öffentlichen Notständen («Business to Administration», B2A)

Dateninhaber müssen in Krisensituationen und öffentlichen Notständen Daten bereitstellen, wenn dies zur Bewältigung der Lage erforderlich ist. Damit wird sichergestellt, dass nationale Behörden und europäische Institutionen im Notfall die benötigten Informationen erhalten.

Beispiele für Datenbereitstellung in Krisensituationen:

- **Pandemie:** Während einer Gesundheitskrise wie der SARS-CoV-2-Pandemie können Behörden Mobilitätsdaten von Telekommunikationsunternehmen anfordern. Diese Daten helfen dabei, Infektionsketten nachzuverfolgen und effektive Massnahmen zur Eindämmung zu planen.

- **Naturkatastrophen:** Bei Überschwemmungen oder Waldbränden können Behörden Daten von Wetterstationen, Satelliten oder vernetzten Sensoren anfordern. Diese Informationen unterstützen die Planung von Evakuierungen und den Einsatz von Rettungskräften.

d) Einschränkungen des Datenzugangs

- «Gatekeeper»-Unternehmen im Sinne des Data Act sind vom Datenzugang ausgeschlossen.
- Klein- und Kleinstunternehmen sind von der Datenbereitstellungspflicht ausgenommen. Wachsen sie zu mittleren Unternehmen gilt eine einjährige Übergangsfrist.
- Testdaten zu neuen Produkten, Substanzen oder Verfahren sind vom Datenzugang ausgenommen.
- Sicherheitsanforderungen oder öffentliche Interessen können den Datenzugang beschränken («Safety and Security Handbrake»), beispielsweise Diagnose- oder Steuerdaten, die in einem vernetzten Fahrzeug intern gesammelt werden.
- Betriebs- und Geschäftsgeheimnisse müssen nicht offengelegt werden. Ihr Schutz kann durch Vereinbarungen mit Nutzern oder dem Datenempfänger gesichert werden («Trade Secrets Handbrake»). Der Datenzugang kann verweigert werden, wenn ein schwerer wirtschaftlicher Schaden droht.
- Der Zugang des Nutzers kann eingeschränkt sein, wenn datenschutzrechtliche Interessen Dritter betroffen sind.
- Der Nutzer darf die Daten nicht nutzen, um den Dateninhaber auszuspionieren und Datenempfänger (Dritte) dürfen die Daten nicht verwenden, um Konkurrenzprodukte zu entwickeln.
- Der Nutzer darf keine Zwangsmittel einsetzen oder technische Schwachstellen des Dateninhabers ausnutzen, um Datenzugang zu erhalten.
- Der Dateninhaber darf geeignete technische Schutzmassnahmen (siehe Ziffer 6) ergreifen.
- Der Dateninhaber kann vom Datenempfänger eine Gegenleistung verlangen – nicht jedoch vom Nutzer.
- Der Zugriff öffentlicher Stellen («B2A») muss verhältnismässig sein. Die Daten dürfen nicht auf andere Weise rechtzeitig und wirksam erlangt werden können. Besonders sensible Bereiche wie Strafverfolgung oder Steuer- und Zollangelegenheiten sind von der Bereitstellungspflicht ausgenommen.

2.2 Welche Daten müssen in welchem Umfang weitergegeben werden?

Grundsätzlich gilt ein breiter Zugang zu nutzungsspezifischen Daten. Dabei müssen faire Bedingungen, angemessene Gegenleistungen und technische Schutzmassnahmen für den Dateninhaber gewährleistet sein.

Alle durch vernetzte Geräte und Dienste generierten Daten (Produktdaten und Dienstdaten), die ohne Weiteres verfügbar sind, müssen vom Dateninhaber an den Nutzer oder Datenempfänger (Dritter) weitergegeben werden. Ein Beispiel sind Maschinen- und Betriebsdaten.

«Ohne Weiteres verfügbar» bedeutet, dass die Daten ohne unverhältnismässigen Aufwand zugänglich sind. Welche Daten das sind, hängt wesentlich vom Design des Produkts oder Dienstes ab. Sie umfassen Daten, die direkt entstehen und nicht weiterbearbeitet wurden (Rohdaten).

Die weitergegebenen Daten müssen so aufbereitet sein, dass sie den Form- und Qualitätsanforderungen entsprechen und eine wirksame Nutzung durch den Nutzer oder den Datenempfänger ermöglichen. Geschäftsgeheimnisse können durch vertragliche Vereinbarungen geschützt werden. Kommt es in diesem Punkt zu keiner Einigung, kann der Dateninhaber die Weitergabe der Daten verweigern. Diese Verweigerung ist jedoch als letztes Mittel («ultima ratio») zu betrachten und muss nachvollziehbar begründet werden.

2.3 An wen müssen die Daten weitergegeben werden?

In Geschäftsbeziehungen («B2B») müssen Unternehmen Daten weitergegeben. Private und kommerzielle Nutzer können Verträge direkt mit dem Dateninhaber oder mit Datenempfängern (Dritten) abschliessen. In Krisensituationen und bei Notständen müssen Daten an öffentliche Stellen weitergegeben werden («B2A»).

2.4 Wie bekomme ich als KMU den Datenzugang?

Der Data Act soll kleinen und mittleren Unternehmen (KMU) helfen, leichter Zugang zu den Daten zu erhalten, die sie für ihre Geschäfte benötigen. Es gibt zwei mögliche Konstellationen:

1) **KMU als Nutzer**
   Wenn ein KMU ein vernetztes Produkt nutzt, gelten die Prinzipien «Data Access by Design» (siehe Ziffer 2.1) oder «Indirect Access» (siehe Ziffer 2.1) – auch für juristische Personen. Das KMU kann die vom Produkt generierten Daten verwenden, an Datenempfänger weitergeben oder den Dateninhaber zur Weitergabe an Dritte auffordern.

2) **KMU als Datenempfänger**
   KMU haben Anspruch auf Daten unter fairen, nicht-diskriminierenden und transparenten Bedingungen. Missbräuchliche Vertragsklauseln sind unwirksam. KMU und gemeinnützige Forschungseinrichtungen müssen keine Marge zahlen und dürfen nicht durch überhöhte Gebühren ausgeschlossen werden.

2.5 Wer trägt die Kosten für die Datenbereitstellung?

- Herstellende Unternehmen oder Dateninhaber tragen die Kosten für die Entwicklung Data-Act-konformer Produkte im Sinne von «Data Access by Design».
- Datenbereitstellung an Nutzer: Die Kosten dürfen nicht auf die Nutzer übertragen werden. Der Dateninhaber trägt diese Kosten.
- Datenbereitstellung an Datenempfänger: Diese Kosten trägt der Datenempfänger. Der Dateninhaber kann eine angemessene, faire und nicht-diskriminierende Gegenleistung verlangen. Diese muss transparent sein und die Datenweitergabe nicht erschweren. KMU und gemeinnützige Forschungseinrichtungen zahlen keine Margen.

- Krisensituationen **und öffentliche Notstände**: Die Bereitstellung erfolgt unentgeltlich. Klein- und Kleinstunternehmen können ausgenommen sein. Für nicht personenbezogene Daten, die für gesetzliche Aufgaben erforderlich sind, kann eine faire Gegenleistung verlangt werden.

2.6 In welchem Verhältnis stehen die Datenzugangsrechte des Data Act zu den Datenschutzgesetzen?

Das schweizerische Datenschutzgesetz (DSG) und die DSGVO regeln den Schutz personenbezogener Daten. Der Data Act hingegen ist kein Datenschutzrecht. Er betrifft personenbezogene und nicht-personenbezogene Daten, die von vernetzten Geräten oder Diensten generiert werden (Maschinen- und Betriebsdaten).

Der Schwerpunkt des Data Act liegt auf wirtschaftlichen und wettbewerblichen Zielen. Er fördert den Datenaustausch und die breite Nutzung wirtschaftlicher Vorteile. Die grundsätzliche Verfügungsbefugnis über die Daten liegt beim Nutzer.

3 Vorvertragliche Informationen

3.1 Welche vorvertraglichen Informationspflichten gegenüber (potenziellen) Kunden bestehen?

- **Vernetzte Produkte**

  Vor Abschluss eines Kauf-, Miet- oder Leasingvertrags müssen Nutzer klar und verständlich über Art und Umfang der generierten Produktdaten sowie über Speicherung und Zugriffsmöglichkeiten informiert werden.

- **Verbundene Dienste**

  Hier gelten noch weitergehende Informationspflichten. Dazu gehören:

  - Beabsichtigte Nutzung der Daten durch den Dateninhaber,
  - Identität und Erreichbarkeit des Dateninhabers,
  - Verfahren zur Weitergabe und Beendigung der Weitergabe,
  - mögliche Geschäftsgeheimnisse in den Daten.
  - Zudem sind Vertragsdauer und Bedingungen für eine vorzeitige Beendigung anzugeben.

4 Datennutzungsverträge

4.1 Was wird unter einem Datennutzungsvertrag verstanden?

Ein Datennutzungsvertrag regelt die Nutzung von Daten. Der Data Act verlangt an verschiedenen Stellen den Abschluss solcher Verträge. Neu ist vor allem der Vertrag zwischen Dateninhaber und Nutzer. Wichtig ist auch der Vertrag zwischen Dateninhaber und Dritten, wenn Daten auf Wunsch des Nutzers an weitere Datenempfänger herausgegeben werden müssen (vgl. dazu nachfolgend).

4.2 Wann müssen Dateninhaber mit ihren Nutzern einen Datennutzungsvertrag abschliessen?

Immer, sobald der Dateninhaber ohne weiteres verfügbare Daten nutzt. Der Abschluss eines Vertrages ist also beispielsweise erforderlich, wenn der Dateninhaber die Daten zur Produktentwicklung oder Bereitstellung seiner weiteren Dienstleistungen verwenden möchte.

4.3 Wann müssen Dateninhaber mit Dritten einen Datennutzungsvertrag abschliessen?

Der Dateninhaber muss insbesondere dann einen Datennutzungsvertrag mit einem Dritten abschliessen, wenn er auf Verlangen des Nutzers verpflichtet ist, die Daten dem Dritten (Datenempfänger) bereitzustellen.

Ein Vertrag ist auch erforderlich, wenn der Dateninhaber Daten aus eigener Initiative weitergeben möchte. So wird sichergestellt, dass der Dritte die Daten nur im Rahmen des vereinbarten Nutzungsrechts verwendet und sie nicht erneut weitergibt (ausser er ist dazu berechtigt).

4.4 Was ist der Mindestinhalt eines solchen Datennutzungsvertrages?

Ein Datennutzungsvertrag muss den Umfang des Nutzungsrechts einschliesslich möglicher Weitergaberechte regeln. Der Data Act gibt aber keinen konkreten Mindestinhalt vor. Dieser ergibt sich vielmehr aus den Umständen des Einzelfalls. Beispielsweise kann auch eine Vereinbarung zur Wahrung von Geschäftsgeheimnissen erforderlich sein.

Der Data Act reguliert dafür aber explizit den Inhalt des Datennutzungsvertrages. So dürfen Vertragsklauseln nicht zum Nachteil des Nutzers die Anwendung der Rechte des Nutzers ausschliessen oder davon abweichen oder die Wirkung dieser Rechte ändern. Zudem unterstehen die Verträge aufgrund des Data Acts nun auch im B2B-Bereich einem «AGB-Recht», nachdem missbräuchliche Klauseln unwirksam sind. Inhaltlich betroffen sind davon vornehmlich Regelungen zur Haftung, Gewährleistung und Rechtsbehelfen.

Die EU-Kommission wird Mustervertragsklauseln zur Verfügung stellen. Diese sind allerdings unverbindlich. Zudem ist davon auszugehen, dass sich die Nutzerzentriertheit des Data Act auch in diesen Mustervertragsklauseln widerspiegeln wird und die Interessen der Dateninhaber nur insoweit berücksichtigt werden, als dies im Data Act explizit vorgesehen ist.

4.5 Können die Datennutzungsrechten des Dateninhabers gegenüber dem Nutzer im Rahmen der Allgemeinen Vertragsbedingungen (AGB) vereinbart werden?

Ja, Datennutzungsrechte können im Rahmen der AGB vereinbart werden. Es gelten jedoch die Vorschriften des Verbraucherschutzrechts. Auch im B2B-Bereich müssen besondere Anforderungen eingehalten werden (vgl. vorige Antwort).

4.6 Reicht es aus, wenn der Datennutzungsvertrag auf der Homepage des Herstellers publiziert wird?

Die allgemeinen Anforderungen für die Einbindung AGB gelten auch hier. Es ist ratsam, im Vertrag auf den Datennutzungsvertrag zu verweisen. Bei Online-Verträgen sollte die Zustimmung aktiv erfolgen, z.B. durch das Anklicken einer Checkbox.

5 Datennutzungsrecht durch Dritte (Datenempfänger)

5.1 Welche Verarbeitungspflichten hat ein Dritter, der Daten auf Verlangen eines Nutzers erhält?

Der Data Act regelt nur den Zugang zu Daten und dessen Einschränkungen. Eine Verarbeitungspflicht ergibt sich nicht aus dem Data Act, sondern aus der Beziehung zwischen dem Nutzer und dem Dritten. Diese Beziehung basiert meist auf einer privatrechtlichen Vereinbarung.

5.2 Was ist bei der Weitergabe von personenbezogenen Daten zu beachten?

Die Datenschutzregeln müssen eingehalten werden. Personenbezogene Daten anderer Personen dürfen nur weitergegeben werden, wenn eine gültige Rechtsgrundlage gemäss Art. 6 DSGVO (oder Art. 9 DSGVO) vorliegt. Der Übermittlungsweg muss zusätzlich gesichert sein, um die Vertraulichkeit der Kommunikation zu gewährleisten (gemäss Art. 5 Abs. 3 der E-Privacy-Richtlinie.).

5.3 Welche Datenverwendungen verbietet der Data Act dem Nutzer?

Grundsätzlich darf der Nutzer Daten, die er vom Dateninhaber erhalten hat, an Dritte weitergeben. Es gibt jedoch Ausnahmen, bei denen die Weitergabe eingeschränkt oder untersagt ist:

- **Gefährdung der Sicherheit**

Der Dateninhaber und der Nutzer können vereinbaren, den Datenaustausch zu beschränken, wenn dadurch die im Unionsrecht oder nationalen Recht festgelegten Sicherheitsanforderungen verletzt würden. Dies betrifft nur Fälle, in denen die Weitergabe schwerwiegende Auswirkungen auf die Gesundheit oder Sicherheit von Menschen haben könnte (Art. 4 Abs. 2).

  - **Beispiel Fahrzeugdaten:** Ein Autohersteller kann den Datenaustausch verweigern, wenn Fahrzeugdaten wie Softwareprotokolle oder Steuerungsdaten Schwachstellen offenlegen könnten, die Hackerangriffe ermöglichen.
  - **Beispiel medizinische Geräte:** Ein Hersteller von vernetzten Herzschrittmachern kann den Zugang zu sensiblen Daten verweigern, wenn unsachgemässe Nutzung oder Manipulation die Funktionsfähigkeit des Geräts gefährden und gesundheitliche Schäden verursachen könnte.

- **Entwicklung konkurrierender Produkte**

Der Nutzer darf die erhaltenen Daten nicht an Dritte weitergeben, um ein konkurrierendes vernetztes Produkt zu entwickeln. Das Verbot gilt jedoch nicht für konkurrierende Dienstleistungen wie

Reparatur- oder Wartungsservices im Aftermarket-Bereich oder mit dem IoT-Gerät verbundene Dienstleistungen, die das Verhalten des Geräts steuern (z.B. App zur Anpassung der Helligkeit von Lichtern oder zur Regulierung der Temperatur des Kühlschranks) (gemäss Art. 4 Abs. 10).

- **Einschränkungen der Datenverarbeitung durch Dritte**

Der Data Act legt klare Grenzen für die Verarbeitung von Daten durch Dritte fest:

  - **Zweckbindung:** Ein Dritter darf die erhaltenen Daten nur zu den vertraglich mit dem Nutzer vereinbarten Zwecken und Bedingungen verarbeiten.
  - **Verhältnismässigkeit**: Die Daten müssen gelöscht werden, sobald sie für den vereinbarten Zweck nicht mehr benötigt werden.

- **Datenschutzanforderungen**

  - Personenbezogene Daten dürfen nur weitergegeben werden, wenn eine gültige Rechtsgrundlage gemäss Art. 6 DSGVO (gegebenenfalls Art. 9 DSGVO) besteht.
  - Der Übermittlungsweg muss gesichert sein, um die Vertraulichkeit der Kommunikation zu gewährleisten.

- **Untersagte Verwendungen durch Dritte**
  Dem Dritten ist es unter anderem folgendes untersagt:

  - **Profiling**: Die Nutzung der Daten für Profiling ist nur erlaubt, wenn dies für den vom Nutzer gewünschten Dienst notwendig ist (Art. 6 Abs. 2 lit. b).
  - **Weitergabe an andere Dritte**: Eine Weitergabe ist nur zulässig, wenn ein Vertrag mit dem Nutzer dies vorsieht und der neue Dritte die vereinbarten Massnahmen zum Schutz von Geschäftsgeheimnissen einhält (Art. 6 Abs. 2 lit. b).
  - **Weitergabe an Gatekeeper**: Es ist verboten, Daten an Gatekeeper (gem. Digital Markets Act) weiterzugeben (Art. 6 Abs. 2 lit. d und Art. 5 Abs. 3).
  - **Entwicklung konkurrierender Produkte:** Die Nutzung der Daten für die Entwicklung eines Konkurrenzprodukts oder deren Weitergabe zu diesem Zweck ist untersagt (Art. 6 Abs. 2 lit. e).
  - **Ausforschung des Dateninhabers:** Nicht-personenbezogene Daten dürfen nicht verwendet werden, um Einblicke in die wirtschaftliche Lage, Vermögenswerte oder Produktionsmethoden des Dateninhabers zu gewinnen (Art. 6 Abs. 2 lit. e).
  - **Gefährdung der Sicherheit:** Die Daten dürfen nicht in einer Weise genutzt werden, die die Sicherheit des Produkts oder verbundenen Dienstes gefährdet (Art. 6 Abs. 2 lit. f).
  - **Verletzung von Schutzmassnahmen:** Technische und organisatorische Massnahmen (TOMs), die den Schutz von Geschäftsgeheimnissen gewährleisten, dürfen nicht missachtet oder untergraben werden (Art. 6 Abs. 2 lit. g).
  - **Hinderung des Nutzers:** Ein Nutzer darf vertraglich oder technisch nicht daran gehindert werden, die erhaltenen Daten an andere Parteien weiterzugeben (Art. 6 Abs. 2 lit. h).

- **Unbefugte Nutzung und Verstösse**

Eine unbefugte Nutzung durch den Dritten oder den Nutzer liegt in folgenden Fällen vor:

  - **Missbrauch von Informationen:** Falsche Angaben zur Erlangung von Daten sind untersagt (Art. 11 Abs. 3 lit. a).

- **Unbefugte Zwecke:** Daten dürfen nicht für nicht genehmigte Zwecke wie die Entwicklung eines Konkurrenzprodukts verwendet werden (Art. 6 Abs. 2 lit. e, Art. 11 Abs. 3 lit. b).
- **Unrechtmässige Weitergabe:** Die Weitergabe von Daten an andere Parteien ohne Berechtigung ist verboten (Art. 11 Abs. 3 lit. c).
- **Verletzung vereinbarter TOMs:** Die Nichteinhaltung der zum Schutz von Geschäftsgeheimnissen vereinbarten Schutzmassnahmen durch den Dritten oder den Nutzer ist unzulässig (Art. 11 Abs. 3 lit. d, Art. 11. Abs. 4).
- **Änderung von Schutzmassnahmen:** Schutzmassnahmen dürfen ohne Zustimmung des Dateninhabers nicht verändert oder aufgehoben werden. Weder durch den Dritten noch durch den Nutzer (Art. 11 Abs. 3 lit e und Art. 11 Abs. 4).
- **Unrechtmässiger Erwerb durch Dritte:** Eine andere Partei, die Daten vom Nutzer in einer Weise erhält, die gegen den Data Act verstösst. (Art. 11 Abs. 4)

- **Einschränkungen der Datennutzung durch den Dateninhaber?**

Der Dateninhaber darf nicht ohne Weiteres verfügbare Daten verwenden, um Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden eines Dritten zu gewinnen (Art. 4 Abs. 10). Ebenso ist es untersagt, Daten so zu nutzen, dass die gewerbliche Position des Dritten auf den Märkten, in denen er tätig ist, untergraben wird. Eine solche Nutzung ist nur erlaubt, wenn der Dritte ihr ausdrücklich zustimmt und die Möglichkeit hat, diese Zustimmung jederzeit technisch zu widerrufen (Art. 5 Abs. 6)

Darüber hinaus darf der Dateninhaber nicht-personenbezogene Produktdaten nur zu Zwecken verwenden, die direkt mit der Erfüllung des Vertrags mit dem Nutzer verbunden sind. Falls erforderlich, kann der Dateninhaber Dritte vertraglich verpflichten, die erhaltenen Daten nicht an andere Parteien weiterzugeben.

5.4 Schutz vor Datenmissbrauch durch die Konkurrenz?

Der Nutzer darf die erhaltenen Daten nicht dazu verwenden, ein konkurrierendes vernetztes Produkt zu entwickeln. Ebenso ist es untersagt, die Daten mit dieser Absicht an Dritte weiterzugeben oder sie zu nutzen, um Einblicke in die wirtschaftliche Lage, Vermögenswerte oder Produktionsmethoden des Herstellers bzw. des Dateninhabers zu erlangen (Art. 4 Abs. 10).

Auch Dritte dürfen die bereitgestellten Daten ohne Genehmigung nicht zur Entwicklung konkurrierender Produkte verwenden oder an andere weitergeben, es sei denn, dies ist ausdrücklich vertraglich geregelt (Art. 6 Abs. 2). Verstösst ein Dritter gegen diese Bestimmung, hat der Dateninhaber verschiedene Ansprüche, um die Verletzung zu ahnden. Weitere Details dazu finden Sie in Ziff. 6.4. (siehe Ziffer 6.4)

5.5 Welche Massnahmen kann ein Unternehmen zum Schutz von Geschäftsgeheimnissen implementieren?

Dateninhaber können geschützte (Meta-)Daten identifizieren und mit technischen und organisatorischen Massnahmen (TOMs) verbinden, um Geschäftsgeheimnisse zu schützen. Diese TOMs hat der Dateninhaber auch im Vertrag mit dem Nutzer vereinbart. Beispiele für solche Massnahmen sind:

- Mustervertragsklauseln
- strenge Zugangsprotokolle
- technische Normen
- Verhaltenskodizes

Werden diese Massnahmen nicht eingehalten oder kann keine Einigung erzielt werden, darf der Dateninhaber die Weitergabe verweigern oder aussetzen (Art. 5 Abs. 10). Dies gilt für Daten, die als Geschäftsgeheimnisse eingestuft werden.

Auch präventiv kann der Dateninhaber die Weitergabe wegen einer drohenden Geheimnisverletzung verweigern. Dies allerdings nur dann, wenn der Dateninhaber trotz technischer und organisatorischer Massnahmen (TOMs) zum Schutz der Daten mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch eine Offenlegung von Geschäftsgeheimnissen erleiden wird. Dies muss schriftlich und begründet geschehen.

Folgend ein Beispiel dafür, wie eine Gefährdung von Geschäftsgeheimnissen aussehen könnte, die eine Verweigerung rechtfertigen würde: Ein Smart-Home-Hersteller sammelt Daten zu Heizverhalten und Energieverbrauch seiner vernetzten Thermostate. Ein Gebäudeverwalter will diese Daten einem Drittanbieter zur Effizienzoptimierung übergeben. Da die Daten direkt die KI-Algorithmen zur Energieeinsparung offenlegen, könnten Wettbewerber sie nachahmen, was dem Hersteller erheblichen wirtschaftlichen Schaden zufügen würde.

6 Technische Schutzmassnahmen

6.1 Wer ist verantwortlich für den Schutz der Daten?

Der Dateninhaber muss geeignete technische Schutzmassnahmen ergreifen, um unbefugten Zugang zu Daten, einschliesslich Metadaten, zu verhindern. Dazu gehören Massnahmen wie Verschlüsselung und der Einsatz intelligenter Verträge («Smart Contracts» [Siehe Ziffer 6.3]).

Der Dateninhaber muss auch sicherstellen, dass:

- die Übergabe gesetzmässig erfolgt,
- eine allfällige Vereinbarung einer Gegenleistung (Art. 9) entspricht,
- der Dritte seinen Pflichten nachkommt und gegebenenfalls Massnahmen ergreifen sowie,
- die vereinbarten Mustervertragsklauseln eingehalten werden.

Dies betrifft insbesondere die Verhinderung unbefugter Nutzung oder Offenlegung.

6.2 Grenzen von Schutzmassnahmen?

Technische Schutzmassnahmen dürfen keine ungleiche Behandlung von Datenempfängern bewirken. Weder Nutzer noch Dritte dürfen in der Ausübung ihrer Rechte durch diese Massnahmen eingeschränkt werden, sofern sie mit EU- oder nationalem Recht im Einklang stehen. Änderungen oder die Aufhebung solcher Schutzmassnahmen sind nur mit der ausdrücklichen Zustimmung des Dateninhabers zulässig (Art. 11 Abs. 1).

Zum Beispiel, wenn der Dateninhaber den Zugriff auf die Daten durch technische Massnahmen wie Zugriffsverweigerung oder Verschlüsselung für gewisse Dritte beschränkt oder mit unzumutbaren Kosten verbindet.

6.3 Was sind intelligente Verträge?

Intelligente Verträge (Smart Contracts) sind Computerprogramme, die automatisch Vereinbarungen oder Teile davon ausführen (self-executing). Sie basieren auf einer Abfolge elektronischer Datensätze, deren Integrität und korrekte chronologische Reihenfolge sichergestellt sind.

Praxisbeispiel: Ein Unternehmen betreibt eine IoT-Datenplattform, auf der Maschinenhersteller Sensordaten teilen. Dieser Datenaustausch basiert auf einem Vertrag (sog. Data Sharing Agreement), der von der natürlichen Sprache in eine Struktur gebracht werden kann, die eine Automatisierung ermöglicht (sog. Smart Contract). Ein solcher Smart Contract kann beispielsweise die automatische Zahlung für den Datenaustausch regeln und den Zugang zu den Daten ab dem vereinbarten Datum automatisch schliessen.

Vor dem EU Data Act war der Smart Contract unveränderlich und führte Transaktionen automatisch aus. Nach dem EU Data Act muss ein Kill Switch integriert sein, um ihn bei Fehlern oder Sicherheitsproblemen stoppen oder anpassen zu können. Eine regulierte Instanz erhält das Recht, den Vertrag zu pausieren oder zu modifizieren. Dies widerspricht der Dezentralisierung und birgt Missbrauchsrisiken. Unternehmen müssen nun zwischen Automatisierung und Kontrolle abwägen.

6.4 Forderungen bei unberechtigter Nutzung Dritter?

Im Falle einer unberechtigten Nutzung können der Dateninhaber und gegebenenfalls der Nutzer folgende Massnahmen von Dritten oder Datenempfängern verlangen:

- **Löschung der Daten:** Die bereitgestellten Daten und alle Kopien davon müssen gelöscht werden (Art. 11 Abs. 2 lit. a),
- **Einstellung und Vernichtung**: Die Herstellung, das Inverkehrbringen oder die Nutzung von Waren oder Dienstleistungen, die auf unrechtmässig erlangten Daten basieren, muss eingestellt werden. Rechtsverletzende Waren können vernichtet werden, insbesondere wenn die ernsthafte Gefahr besteht, dass durch deren Nutzung ein erheblicher Schaden verursacht wird oder droht. Diese Massnahmen dürfen jedoch nicht unverhältnismässig im Vergleich zu den Interessen des Dateninhabers, des Inhabers des Geschäftsgeheimnisses oder des Nutzers sein (Art. 11 Abs. 2 lit. b),
- **Information des Nutzers:** Der Nutzer muss über die unbefugte Nutzung der Daten sowie über die ergriffenen Massnahmen zur Behebung informiert werden (Art. 11 Abs. 2 lit. c),
- **Entschädigung**: Ein Ausgleich ist für Schäden zu leisten, die durch Missbrauch oder unbefugte Offenlegung der Daten entstanden sind (Art. 11 Abs. 2 lit. d).

7 Bereitstellung von Daten für öffentliche Stellen

7.1 Wann sind Dateninhaber verpflichtet, Daten an öffentliche Stellen oder die EU-Institutionen bereitzustellen?

Dateninhaber müssen Daten an Behörden bereitstellen, wenn diese eine aussergewöhnliche Notwendigkeit nachweisen. So wird sichergestellt, dass nationale und europäische Institutionen im Notfall über die benötigten Informationen verfügen (Art. 15 Abs. 1).

7.2 Was gilt als «aussergewöhnliche Notwendigkeit» im Sinne des Data Acts?

Es gibt zwei Situationen, in denen eine aussergewöhnliche Notwendigkeit vorliegt:

1. Daten zur Bewältigung eines öffentlichen Notstands

Eine aussergewöhnliche Notwendigkeit besteht, wenn die angeforderten Daten entscheidend sind, um einen öffentlichen Notstand zu bewältigen, und auf anderem Weg nicht rechtzeitig und wirksam beschafft werden können.

Beispiele:

- **Pandemien:** Mobilitätsdaten von Telekommunikationsunternehmen könnten verwendet werden, um Infektionsketten nachzuverfolgen,
- Stromausfälle: Behörden könnten Daten von Energieversorgern anfordern, um die Wiederherstellung der Versorgung zu koordinieren.
- **Lebensmittelkontamination:** Zugriff auf Lieferkettendaten von Lebensmittelherstellern und -händlern könnte erforderlich sein, um betroffene Produkte schnell zu identifizieren und zurückzurufen.

2. Daten für öffentliche Aufgaben im Interesse der Allgemeinheit

Wenn keine personenbezogenen Daten erforderlich sind, kann eine aussergewöhnliche Notwendigkeit auch bestehen, wenn eine öffentliche Stelle oder eine EU-Institution aufgrund fehlender Daten daran gehindert wird, eine rechtlich vorgesehene Aufgabe im öffentlichen Interesse zu erfüllen. Diese Massnahme ist nur zulässig, wenn alle anderen Möglichkeiten ausgeschöpft sind und keine Klein- oder Kleinstunternehmen betroffen sind.

Beispiele:

- **Verkehrsplanung:** Städte könnten anonymisierte Mobilitätsdaten von E-Scooter-Anbietern anfordern, um die Verkehrsinfrastruktur zu optimieren.
- **Wirtschaftsanalyse:** Statistische Ämter könnten aggregierte Finanzdaten von Unternehmen nutzen, um genauere Wirtschaftsprognosen zu erstellen.
- **Stadtentwicklung:** Kommunen könnten anonymisierte Nutzungsdaten von Smart-Home-Geräten verwenden, um den Energieverbrauch in Stadtteilen zu analysieren und nachhaltige Konzepte für die Stadtentwicklung zu erarbeiten.

7.3 Welche Informationen muss ein Datenverlangen durch eine öffentliche Stelle enthalten?

Ein Datenverlangen einer öffentlichen Stelle muss folgende Angaben enthalten:

- **Datenumfang:** Präzise Informationen darüber, welche Daten und Metadaten benötigt werden.
- **Zweck und Dauer:** Der spezifische Zweck und die geplante Dauer der Datennutzung müssen klar definiert sein.
- **Verarbeitung personenbezogener Daten:** Falls personenbezogene Daten verarbeitet werden, muss erläutert werden, wie diese Verarbeitung der aussergewöhnlichen Notwendigkeit dient.
- **Schutzmassnahmen:** Angaben zu den technischen und organisatorischen Massnahmen zum Schutz der personenbezogenen Daten.
- **Nachweis der Notwendigkeit:** Der Nachweis, dass eine aussergewöhnliche Notwendigkeit besteht.
- **Rechtsgrundlage:** Die relevante Rechtsvorschrift, die der öffentlichen Stelle oder EU-Institution die Aufgabe im öffentlichen Interesse überträgt.

Der Umfang der verlangten Daten sowie die Häufigkeit des Zugriffs müssen im Hinblick auf die aussergewöhnliche Notwendigkeit gerechtfertigt und nachvollziehbar begründet sein.

7.4 Welche besonderen Anforderungen gelten bei personenbezogenen Daten?

Ein Datenverlangen sollte vorrangig nicht-personenbezogene Daten betreffen. Erst wenn diese nicht ausreichen, um auf den öffentlichen Notstand zu reagieren, dürfen personenbezogene Daten angefordert werden. In diesem Fall müssen technische und organisatorischen Massnahmen (TOMs) zum Schutz der Daten festgelegt werden. Zudem ist dieses Datenverlangen der Aufsichtsbehörde im Mitgliedsstaat, die für die Überwachung der Anwendung der DSGVO zuständig ist, zu melden.

Der Dateninhaber muss die personenbezogenen Daten vor der Übergabe an die öffentliche Stelle oder der EU-Institution anonymisieren. Ist zur Erfüllung des Datenschutzverlangens die Offenlegung erforderlich, muss der Dateninhaber die Personendaten pseudonymisieren.

7.5 Was sind die Pflichten der öffentlichen Stellen im Umgang mit den erhaltenen Daten

Öffentliche Stellen dürfen die Daten nur für den angegebenen Zweck nutzen. Sie müssen TOMs ergreifen, um die Vertraulichkeit und Integrität der Daten zu wahren. Sobald die Daten nicht mehr gebraucht werden, müssen sie gelöscht werden. Eine Archivierung ist nur erlaubt, wenn sie den EU- oder nationalen Vorgaben entspricht.

Die Stellen dürfen die Daten nicht verwenden, um ein Konkurrenzprodukt zu entwickeln oder zu verbessern. Eine Weitergabe der Daten oder Erkenntnisse zu diesem Zweck an Dritte ist ebenfalls untersagt.

7.6 Haben Dateninhaber Anspruch auf eine Entschädigung für die Bereitstellung von Daten?

Dateninhaber können eine faire Entschädigung für die Bereitstellung von Daten an öffentliche Stellen verlangen, wenn das Verlangen auf der Erfüllung einer Aufgabe im öffentlichen Interesse beruht. Die Entschädigung umfasst die technischen und organisatorischen Kosten, einschliesslich Ausgaben für Anonymisierung und Pseudonymisierung.

Keine Entschädigung erfolgt, wenn die Daten für amtliche Statistiken benötigt werden und der Erwerb nach nationalem Recht nicht zulässig ist.

Sofern das Verlangen nicht an ein Kleinst- oder Kleinunternehmen geht, müssen die Daten im Falle eines öffentlichen Notstands unentgeltlich bereitgestellt werden und es wird eine öffentliche Anerkennung ausgesprochen.

7.7 Welche Rechte haben Dateninhaber, wenn sie mit einem Datenverlangen nicht einverstanden sind

Dateninhaber können das Verlangen ablehnen oder dessen Änderung beantragen,

- wenn sie der Meinung sind, dass sie keine Kontrolle über die verlangten Daten haben,
- das Verlangen nicht den gesetzlichen Anforderungen entspricht (vgl. Frage 7.3), oder
- bereits ein ähnliches Verlangen zu demselben Zweck von einer anderen öffentlichen Stelle gestellt wurde und der Dateninhaber dort nicht über das Löschen der Daten unterrichtet wurde.

Wenn die öffentliche Stelle der Ablehnung des Dateninhabers widerspricht oder wenn der Dateninhaber Einspruch gegen das Verlangen einlegen will und durch eine Änderung des Verlangens keine Einigung erfolgt, kann der Dateninhaber bei der nach Art. 37 zuständigen Behörde Beschwerde einlegen.

7.8 Muss ich der öffentlichen Stelle oder der EU-Institution meine Geschäftsgeheimnisse offenlegen?

Geschäftsgeheimnisse müssen nur offengelegt werden, wenn dies für den Zweck des Verlangens unbedingt erforderlich ist. In diesem Fall muss die anfragende Stelle geeignete technische und organisatorische Massnahmen (TOMs) ergreifen, um die Vertraulichkeit zu schützen. Dazu gehören beispielsweise Mustervertragsklauseln, technische Standards oder Verhaltenskodizes.

8 Ermöglichung von Cloud-Switching

8.1 Was für inhaltliche und formellen Mindestanforderungen müssen Verträge mit Cloud- bzw. Edge-Anbietern erfüllen?

8.2 Welche Informations- und Transparenzpflichten haben Cloud- bzw. Edge-Anbieter?

Cloud- bzw. Edge-Anbieter, das sind Dienste, die Rechenleistung, Speicherplatz oder Anwendungen über das Internet oder nahe am Ort der Datennutzung zur Verfügung stellen, müssen ihren (potenziellen) Kunden folgende Informationen bereitstellen:

- **Wechsel- und Übertragungsverfahren:** Details zu verfügbaren Verfahren für den Wechsel und die Übertragung von Inhalten, einschliesslich Informationen über Methoden, Formate sowie bekannte Einschränkungen oder technische Beschränkungen.
- **Datenstrukturen und -formate:** Angaben zu den verwendeten Datenstrukturen, Formaten, relevanten Normen und offenen Interoperabilitätsspezifikationen.

Bei einem Wechsel im internationalen Umfeld sind Anbieter verpflichtet, folgende Informationen auf ihren Websites bereitzustellen und aktuell zu halten:

- **Gerichtsbarkeit:** Die Zuständigkeit, der die IKT-Infrastruktur für die Datenverarbeitung unterliegt.
- **Technische und organisatorische Massnahmen (TOMs) gegen unrechtmässigen Zugriff:** Eine allgemeine Beschreibung der technischen, organisatorischen und vertraglichen Massnahmen, die verhindern, dass staatliche Stellen ausserhalb der EU unrechtmässig auf in der Union **gespeicherte** nicht-personenbezogene Daten zugreifen oder diese übertragen. Dies gilt insbesondere, wenn ein solcher Zugriff gegen EU-Recht oder nationales Recht verstossen würde.

8.3 Was sind die technischen Anforderungen?

Cloud- und Edge-Anbieter, also Anbieter von Infrastructure as a Service (IaaS), müssen den Wechsel ihrer Kunden unterstützen. Dazu gehören:

- Bereitstellung von Kapazitäten, Informationen und Dokumentationen,
- technische Unterstützung, und
- gegebenenfalls notwendige Instrumente.

PaaS- und SaaS-Anbieter müssen ihren Kunden zudem unentgeltlich eine Schnittstelle bereitstellen. Diese Schnittstelle muss ausreichend Informationen enthalten, damit eine Software zur Datenübertragung reibungslos mit dem Dienst kommunizieren kann.

8.4 Wer trägt die Kosten für ein Cloud-Switching?

Cloud-Anbieter können bis zum 11. Januar 2027 ermässigte Wechselentgelte von ihren Kunden verlangen. Ab dem 12. Januar 2027 dürfen solche Gebühren nicht mehr erhoben werden, womit langfristig die Kosten für den Anbieterwechsel abgeschafft werden.

8.5 Was für Anforderungen müssen Betreiber von Datenräumen («Operators of Data Spaces»«) erfüllen, um die Interoperabilität von Daten, Datenaustausch-Mechanismen und - Datendiensten («Data Sharing Mechanisms and Services»«) sicherzustellen? Oder: Anforderungen an Betreiber von Datenräumen für Interoperabilität

«Interoperabilität» bezeichnet die Fähigkeit verschiedener Datenräumen, Systemen, Anwendungen oder Dienste, Daten nahtlos auszutauschen und zu nutzen, um ihre Funktionen auszuführen. Betreiber von Datenräumen müssen folgende Anforderungen erfüllen, um die Interoperabilität sicherzustellen:

- **Datensatzbeschreibung:** Inhalte von Datensätzen, Nutzungsbeschränkungen, Lizenzen, Datenerhebungsmethoden und Datenqualität müssen klar definiert sein. Dies ermöglicht dem Datenempfänger das Auffinden, Zugreifen und Nutzen der Daten,
- **Struktur und Formate:** Datenstrukturen, Formate, Vokabular, Taxonomien, Klassifikationsschemata und Codelisten müssen einheitlich und öffentlich zugänglich beschrieben werden,
- **Technische Mittel:** Zugangsmöglichkeiten wie APIs (Anwendungsprogrammierschnittstellen) und ihre Nutzungsbedingungen sowie die Dienstqualität müssen so beschrieben werden, dass ein automatisierter Zugang und Datenaustausch in maschinenlesbarem Format möglich ist,

- **Interoperabilität von Smart Contracts:** Falls erforderlich, müssen Betreiber technische Mittel bereitstellen, die eine nahtlose Interoperabilität von Smart Contracts innerhalb der Dienste ermöglichen.

8.6 Was für Vorschriften zur Daten- und Cloud-Interoperabilität stellt der Data Act?

Der Data Act legt keine festen Mindestanforderungen für Anbieter von Datenverarbeitungsdiensten fest. Stattdessen definiert die EU-Kommission Anforderungen an Spezifikationen und Normen, die entwickelt werden sollen.

Ein zentrales Register wird eingerichtet, um Normen für die Interoperabilität von Datenverarbeitungsdiensten zu verwalten. Dieses Register enthält Verweise auf harmonisierte Normen und gemeinsame Spezifikationen.

Für die Daten- und Cloudinteroperabilität macht der Data Act folgende Vorgaben:

- **Leistungsorientierung:** Die Interoperabilität zwischen Datenverarbeitungsdiensten desselben Typs muss gewährleistet werden.
- **Übertragbarkeit:** Digitale Vermögenswerte sollen zwischen Datenverarbeitungsdiensten desselben Typs leichter übertragen werden können.
- **Funktionsäquivalenz:** Datenverarbeitungsdienste desselben Typs sollen, soweit technisch möglich, die gleiche Funktionalität bieten.

9 Benennung eines Vertreters in der EU

9.1 Wann ist die Benennung eines Vertreters in der EU erforderlich und was sind seine Pflichten?

Unternehmen, die ausserhalb der EU ansässig sind, beispielsweise in der Schweiz, aber Produkte oder Dienstleistungen auf dem EU-Markt anbieten, müssen einen EU-Vertreter benennen. Dieser Vertreter muss seinen Sitz in der EU haben. Alle diese Unternehmen müssen einen Vertreter mit Sitz in der EU benennen. Der EU-Vertreter unterstützt die Einhaltung des Data Acts und dient als Ansprechpartner für die zuständigen Behörden. Diese können sich direkt an den Vertreter wenden, ohne zusätzlich das ausserhalb der EU ansässige Unternehmen zu kontaktieren.

Zu den Aufgaben des Vertreters gehört:

- Zusammenarbeit mit den zuständigen Behörden,
- Bereitstellung von Nachweisen über Massnahmen und Vorschriften.

9.2 Welche (Informations-)Pflichten haben Unternehmen gegenüber einem Vertreter in der EU?

Ein EU-Vertreter muss in der Lage sein, Fragen zur Einhaltung des Data Acts (Compliance) zu beantworten.

Nutzer oder Drittanbieter können sich an die EU-Behörde wenden, wenn ihnen der Zugang zu Daten verweigert wird oder es Unklarheiten bezüglich fairer Vertragsklauseln gibt. Der EU-Vertreter muss daher alle relevanten Informationen besitzen, um diese Fragen zu klären. Dazu gehören z.B. Angaben zu den Massnahmen des Unternehmens zur Einhaltung des Data Acts oder zur Art des Datenzugangs.

10 Sanktionen und Vollzug

10.1 Welche Sanktionsmöglichkeiten und Rechtsfolgen sieht der Data Act vor?

Der Data Act sieht verschiedene Sanktionsmöglichkeiten und rechtliche Konsequenzen vor:

Bussgelder:

- Bussgelder können bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes betragen, ähnlich der DSGVO.
- Die genaue Höhe wird von den Mitgliedstaaten festgelegt und muss wirksam, verhältnismässig und abschreckend sein.
- Verstössen gegen den Schutz personenbezogener Daten können von Datenschutzbehörden gemäss der DSGVO geahndet werden.

Zivilrechtliche Folgen:

- Vertragsklauseln, die Rechte des Nutzers oder anderer Parteien nach Kapitel III einschränken, sind unwirksam,
- Betroffene haben das Recht, Beschwerde einzulegen und einen gerichtlichen Rechtsbehelf zu nutzen.

10.2 Wer ist für den Vollzug zuständig?

Die Mitgliedstaaten müssen Behörden benennen, die den Data Act überwachen und durchsetzen. Für personenbezogene Daten sind die Datenschutzbehörden, die bereits für die DSGVO zuständig sind, auch für die Anwendung des Data Act verantwortlich.

Die Durchsetzung umfasst:

- Überwachung der Einhaltung,
- Verhängung von Sanktionen bei Verstössen,
- Möglichkeit für Betroffene, Beschwerden einzureichen und gerichtliche Rechtsbehelfe zu nutzen.

10.3 Welche Rechtsmittel stehen Nutzern von vernetzten Produkten und verbundenen Diensten zur Durchsetzung ihrer Rechte zur Verfügung?

Nutzern – sowohl juristische als auch natürliche Personen - von vernetzten Produkten und verbundenen Diensten haben folgende Rechtsmittel, um ihre Rechte durchzusetzen:

- **Beschwerderecht:** Nutzer können Beschwerde bei der zuständigen nationalen Behörde einlegen, wenn sie eine Verletzung ihrer Rechte vermuten.
- **Gerichtlicher Rechtsbehelf:** Nutzer haben das Recht auf einen gerichtlichen Rechtsbehelf, wenn ihre Rechte nicht ordnungsgemäss erfüllt werden.

Das Beschwerderecht kann bei der zuständigen Behörde des Mitgliedstaates geltend gemacht werden, in welchem der Nutzer seinen gewöhnlichen Aufenthaltsort, seinen Arbeitsort oder seine Niederlassung hat.