

## EU-Verordnung

# DER EU DATA ACT IM TRILOGVERFAHREN

cepDossier Nr. 1/2023

[Vorschlag COM\(2022\) 68](#) der EU-Kommission vom 23. Februar 2022 für eine **Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)**.

[Stellungnahme](#) des Europäischen Parlaments („EP“) in erster Lesung vom 14. März 2023

[Allgemeine Ausrichtung](#) des Rates der EU („Rat“) vom 24. März 2023

*Hinweis 1:* Das cep hat Teile des Kommissionsvorschlags bereits in der [cepAnalyse 11/2022](#) untersucht. Dieses cepDossier behandelt die Kapitel I-IV des Data Act und stellt u.a. dar, wie sich das EP und der Rat für die laufenden Trilogverhandlungen zu den Pflichten von Unternehmen positionieren, Daten vernetzter Produkte an andere Unternehmen (B2B) und Verbraucher (B2C) weiterzugeben.

*Hinweis 2:* Verweise auf Rechtsvorschriften im Data Act beziehen sich jeweils auf das oben verlinkte Dokument desjenigen EU-Organs, dessen Position dargestellt wird.

## Hintergrund | Ziel | Betroffene

**Hintergrund:** Daten, die von vernetzten Produkten wie Industriemaschinen, Fahrzeugen und Haushaltsgeräten erzeugt und gesammelt werden, verbleiben häufig in den Händen weniger Unternehmen und werden bislang nur unzureichend als „Ressource für die Sicherung des ökologischen und des digitalen Wandels“ genutzt. Die Kommission will mit dem Data Act daher faktische, technische und rechtliche Hindernisse für den Datenaustausch wie Unsicherheiten über Rechte und Pflichten und vertragliche Ungleichgewichte beseitigen und das Vertrauen in den Datenaustausch stärken, um das „enorme“ Potenzial von Daten besser auszuschöpfen.

**Ziel:** Der Data Act will in den Kapiteln I-IV einen einheitlichen, sektorübergreifenden Rahmen für den Datenzugang und die Datennutzung schaffen und insbesondere

- den Zugang zu Daten verbessern, die bei der Nutzung vernetzter Produkte und verbundener Dienste erzeugt und von einem Unternehmen kontrolliert werden, und zwar sowohl für Verbraucher (Business to Consumer, B2C) als auch für andere Unternehmen (Business to Business, B2B),
- Grundregeln für die Erfüllung gesetzlicher Datenbereitstellungspflichten festlegen, und
- Kleinst- sowie kleine und mittlere Unternehmen (KMU) vor missbräuchlichen Vertragsklauseln schützen.

### Hauptbetroffene der Kapitel I-IV Data Act:

- Hersteller und Entwickler vernetzter Produkte, Erbringer verbundener Dienste und sonstige Dateninhaber, die Daten kontrollieren und rechtlich berechtigt, verpflichtet oder in der Lage sind, Daten bereitzustellen;
- Alle Besitzer und Nutzer vernetzter Produkte oder verbundener Dienste;
- sonstige Personen, deren Daten durch erfasste vernetzte Geräte gesammelt werden,
- Dritte, denen auf Verlangen des Nutzers Daten vernetzter Produkte zur Weiternutzung bereitgestellt werden.

## Kurzdarstellung der wesentlichen Änderungsvorschläge und Klarstellungen von EP und Rat

### ► Was sind vernetzte Produkte?

#### **Kommission:**

- Vernetzte Produkte sind laut Kommission ausschließlich körperliche bewegliche (auch in Gebäude eingebaute) Gegenstände, die mittels ihrer Komponenten Daten über ihre Nutzung oder ihre Umgebung erlangen, erzeugen oder sammeln und über öffentlich zugängliche elektronische Kommunikationsdienste übermitteln können, z.B. Fahrzeuge, Haushaltsgeräte, Konsumgüter, Medizin- und Gesundheitsprodukte, landwirtschaftliche und industrielle Maschinen [Art. 2 (2), Erwägungsgrund („EG“) 14].

#### **Europäisches Parlament:**

- Das EP ändert diese Definition leicht ab. Produkte sind körperliche, aber nicht zwingend bewegliche Gegenstände. Zudem will das EP auch Produkte erfassen, die Daten über nicht öffentlich zugängliche elektronische Kommunikationsdienste oder über physische Verbindungen oder geräteinterne Zugänge übermitteln können. Als Beispiele nennt das EP zusätzlich private, zivile oder gewerbliche Infrastrukturen, Schiffe, Luftfahrzeuge und Anlagen zur Energieerzeugung und -übertragung. [Art. 2 (2), EG 14]

#### **Rat:**

- Vernetzte Produkte sind laut Rat körperliche, aber nicht zwingend bewegliche Gegenstände. Dabei erfasst der Rat nun auch Produkte, die Daten über ihr Betriebssystem – und nicht nur mittels ihrer Komponenten – erlangen, erzeugen oder sammeln. Als zusätzliches Beispiel für vernetzte Produkte erwähnt der Rat nun auch „Lifestyle-Geräte“. [Art. 2 (2), EG 14]

► **Was sind keine vernetzten Produkte?**

**Kommission:**

- Keine vernetzten Produkte sind Gegenstände, deren Hauptfunktion darin besteht, Daten zu speichern und zu verarbeiten, d.h. von Menschen erzeugte Inhalte anzuzeigen, abzuspielen oder z.B. für die Nutzung durch Online-Dienste aufzuzeichnen und zu übertragen (z.B. PCs, Server, Tablets, Smartphones, Kameras, Webcams, Tonaufnahmesysteme, Textscanner) [Art. 2 (2), EG 14, 15].

**Europäisches Parlament:**

- Keine vernetzten Produkte sind Gegenstände, deren Hauptfunktion die Speicherung, Verarbeitung und Übertragung von Daten im Namen Dritter ist. Zudem will das EP nur in der EU in den Verkehr gebrachte Gegenstände erfassen und Prototypen in der Entwicklungsphase ausnehmen [Art. 2 (2), EG 14, 15].

**Rat:**

- Keine vernetzten Produkte sind Produkte, bei denen der Nutzer bei der Verwendung Inhalte aufnimmt, überträgt, anzeigt oder abspielt, sowie die Inhalte selbst, da diese häufig unter Rechte des geistigen Eigentums fallen [EG 15].

► **Was sind verbundene Dienste?**

**Kommission:**

- Laut Kommission sind das digitale Dienste, z.B. Software, die so mit einem vernetzten Produkt verbunden oder in es integriert sind, dass das Produkt ohne ihn eine seiner Funktionen nicht ausführen könnte [Art. 2 (3), EG 16].

**Europäisches Parlament:**

- Laut EP muss ein verbundener Dienst zusätzlich den Zugriff des Anbieters oder des Dienstes auf Daten des vernetzten Produkts umfassen. Keine verbundenen Dienste sind elektronische Kommunikationsdienste sowie Dienste zur Stromversorgung und Bereitstellung der Konnektivität [Art. 2 (3), EG 16].

**Rat:**

- Laut Rat sind verbundene Dienste digitale Dienste, die mit einem vernetzten Produkt zum Zeitpunkt des Erwerbs, der Anmietung bzw. des Leasings des Produkts verbunden sind. Wie das EP nimmt der Rat elektronische Kommunikationsdienste aus. [Art. 2 (3), EG 16]

► **Wer ist als Dateninhaber verpflichtet, Unternehmen oder Verbrauchern Daten bereitzustellen?**

**Kommission:**

- Dateninhaber ist laut Kommission jede natürliche oder juristische Person, die [Art. 2 (6), EG 4, 19]
  - nach dem Data Act oder anderen Rechtsvorschriften berechtigt oder verpflichtet ist, Daten bereitzustellen (rechtliche Kontrolle), oder
  - bei nicht-personenbezogenen Daten zur Bereitstellung in der Lage ist, weil sie die technische Gestaltung des Produkts bzw. Dienstes kontrolliert (faktische Kontrolle).
 Das ist regelmäßig der Hersteller eines vernetzten Produkts oder der Erbringer eines verbundenen Dienstes.
- Von den Datenteilungspflichten ausgenommen sind laut Kommission
  - Kleinst- und Kleinunternehmen (KKU) mit weniger als 50 Mitarbeitern und einem Jahresumsatz bzw. einer Jahresbilanz von maximal 10 Mio. Euro [Art. 7 (1) i.V.m. Art. 2 Anhang der Empfehlung 2003/361/EG], sofern sie keine größeren Partnerunternehmen oder verbundenen Unternehmen haben oder von größeren Unternehmen mit der Herstellung oder dem Design des Produkts beauftragt werden.

**Europäisches Parlament:**

- Dateninhaber ist laut EP jede natürliche oder juristische Person, die [Art. 2 (6)]
  - auf Daten aus dem vernetzten Produkt zugegriffen hat oder die bei der Erbringung eines verbundenen Dienstes Daten erzeugt hat,
  - vertraglich berechtigt ist, diese Daten zu nutzen und
  - nach dem Data Act oder anderen Rechtsvorschriften verpflichtet ist, Daten bereitzustellen (rechtliche Kontrolle).
 Dateninhaber sind häufig die Hersteller vernetzter Produkte. Auftragsverarbeiter agieren grds. nicht als Dateninhaber, sofern sie nicht vom Verantwortlichen speziell damit beauftragt wurden. [EG 5, 21]
- Auch das EP will KKU von den Datenteilungspflichten ausnehmen, sofern sie keine größeren Partnerunternehmen oder verbundenen Unternehmen haben oder als Unterauftragnehmer mit der Herstellung oder dem Entwurf eines Produkts oder der Erbringung eines verbundenen Dienstes beauftragt werden [Art. 7(1)].

**Rat:**

- Der Rat präzisiert die Definition des Dateninhabers dahingehend, dass neben demjenigen, der die technische Gestaltung des Produkts bzw. Dienstes kontrolliert, auch derjenige als Dateninhaber gilt, der die Zugangsmöglichkeiten zu nicht-personenbezogenen Daten kontrollieren kann und so ebenfalls eine „faktische Kontrolle“ über diese Daten ausübt [Art. 2 (6)].
- Der Rat will zudem die Ausnahme für KKV auf mittlere Unternehmen ausnehmen, sofern diese den Schwellenwert als solches Unternehmen seit weniger als einem Jahr überschreiten oder, sofern das vernetzte Produkt des mittleren Unternehmens seit weniger als einem Jahr auf dem Markt ist [Art. 7 (1)].

► **Wer ist Nutzer eines vernetzten Produkts oder verbundenen Dienstes und hat daher ein Recht auf die vom Produkt erzeugten Daten?**

**Kommission:**

- Laut Kommission sind „Nutzer“ Unternehmen oder Verbraucher, die [Art. 2 (5), EG 18]
  - ein vernetztes Produkt besitzen, d.h. gekauft gemietet oder geleast haben oder
  - eine Dienstleistung in Anspruch nehmen.

**Europäisches Parlament:**

- Das EP will den Nutzerbegriff erweitern. Nutzer sollen nicht nur Unternehmen und Verbraucher, sondern auch öffentliche Stellen sein, die [Art. 2 (5), EG 14, 18]
  - ein vernetztes Produkt besitzen, d.h. gekauft gemietet oder geleast haben, oder
  - vom Eigentümer vertraglich zur Inanspruchnahme eines verbundenen Dienstes ermächtigt wurden.
 Zudem sollen auch alle betroffenen Personen, deren personenbezogene Daten das Produkt oder der verbundene Dienst verarbeitet, als „Nutzer“ gelten, auch wenn sie nicht Besitzer des Produkts sind.

**Rat:**

- Der Rat will den Nutzerbegriff ebenfalls auf Einrichtungen des öffentlichen Sektors erweitern. Als Nutzer gelten sollen zudem auch „betroffene Personen“, die ein Produkt besitzen, mieten oder leasen oder einen verbundenen Dienst nutzen [Art. 2 (5)].

► **Welche Daten müssen Dateninhaber teilen?**

**Kommission:**

- Laut Kommission müssen Dateninhaber die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes erzeugten Daten teilen [Art. 3 (1) 4 (1), 5(1), EG 14, 17].

**Europäisches Parlament:**

- Laut EP müssen Dateninhaber Daten teilen, auf die sie über ein verbundenes Produkt zugreifen, oder die sie bei der Erbringung eines verbundenen Dienstes erzeugen, einschließlich aller hieraus abgeleiteten personenbezogenen Daten betroffener Personen. Dies umfasst auch Daten, die aus von einzelnen oder von einer Gruppe verbundener Sensoren gesammelten Rohdaten abgeleitet oder gefolgert werden, um sie als physikalische Größe oder deren Veränderung verständlich zu machen (z.B. Temperatur, Druck, Durchflussmenge, pH-Wert, Flüssigkeitsstand, Position, Beschleunigung oder Geschwindigkeit). [Art. 3(1), 4(1), 5(1), EG 24b, 24d]
- Die relevanten zugänglichen Daten sollen in sektorspezifischen Vorschriften genauer definiert und an die Besonderheiten des betreffenden Sektors angepasst werden. Dabei soll die Verfügbarkeit zumindest solcher Daten sichergestellt werden, die für die Reparatur oder Wartung der vernetzten Produkte und verbundenen Dienste wesentlich sind. [EG 24b, 24d]
- Metadaten, die zur Interpretation oder Nutzung der Daten notwendig sind, müssen mitgeliefert werden.

**Rat:**

- Der Rat will den Zugang zu den Daten, die bei der Nutzung eines vernetzten Produkts bzw. verbundenen Dienstes erzeugt werden, auf die Daten beschränken, die für den Dateninhaber leicht – d.h. ohne unverhältnismäßigem Aufwand – zugänglich sind. Das Zugangsrecht soll explizit auch die für die Interpretation und Nutzung der Daten erforderlichen Metadaten umfassen. [Art. 2 (1ae), 3(1), 4(1), 5(1), EG 14a]

► **Welche Daten müssen Dateninhaber nicht teilen?**

**Kommission:**

- Ausgenommen von der Teilungspflicht sind laut Kommission aus den Daten (mittels eines Softwareprozesses) abgeleitete oder gefolgerte Informationen bzw. Daten [EG 14, 17].

**Europäisches Parlament:**

- Ausgenommen von der Teilungspflicht sind laut EP alle Daten, die [Art. 2 (1), EG 15, 16, EG 24b, 24d]
  - mit Hilfe komplexer, eigentumsrechtlich geschützter Algorithmen aus den Daten abgeleitet oder gefolgert werden, insbesondere Daten, die durch eine Kombination der Messungen mehrerer Sensoren des Produkts (Sensorfusion) gewonnen werden [EG 24b];
  - für den Dateninhaber oder -empfänger nicht zugänglich sind; z.B. volatile, mit hoher Frequenz aufgezeichnete Werte, die ggf. nur für die Aktivierung einer spezifischen Funktion (Scheibenwischer, Scheinwerfer) erhoben und rasch wieder überschrieben werden und daher aus Kapazitäts- und Kostengründen nicht von dem Produkt gespeichert werden [EG 24d];
  - nicht in den bei der Erbringung eines verbundenen Diensten erzeugten Daten enthalten sind, sondern vom Dateninhaber oder -empfänger erst zeitlich nach erfolgtem Zugriff auf die vom vernetzten Produkt erzeugten nicht-personenbezogenen Daten aus diesen abgeleitet werden [EG 16], und
  - Inhalte oder Daten, die von dem vernetzten Produkt erlangt, erzeugt oder gesammelt werden, bzw. auf die von dem vernetzten Produkt zugegriffen wird, oder die im Auftrag Dritter zum Zwecke der Speicherung oder Verarbeitung an das vernetzte Produkt übermittelt werden, wie z.B. im Fall von Servern oder Cloud-Infrastrukturen, u. a. zur Nutzung durch einen Online-Dienst [Art. 2 (1), EG 15].
  - Nutzer können nicht verlangen, Daten, die aus dem vernetzten Produkt oder verbundenen Dienst im Zusammenhang mit der Erprobung anderer neuer, noch nicht auf dem Markt befindlicher Produkte, Stoffe und Verfahren gewonnen wurden, an Dritte weiterzugeben, es sei denn, Nutzer und Dateninhaber haben dies vertraglich vereinbart [Art. 5 (1a)].
- Zusätzliche Daten muss der Hersteller nicht auf dem Produkt speichern, wenn das in Bezug auf die erwartete Nutzung unverhältnismäßig wäre. Er kann dies mit dem Nutzer jedoch vereinbaren. Aktualisiert der Hersteller oder ein Dritter – z.B. im Rahmen eines Funktionsupdates – das Produkt und werden dadurch weitere oder weniger Daten zugänglich, muss der Nutzer aber hierüber informiert werden. [EG 19]
- Das EP will ein Vetorecht des Dateninhabers einführen. Er soll die Weitergabe von Daten ablehnen können, wenn der Zugang zu den Daten nach nationalem oder EU-Recht verboten ist. [Art. 3 (1a), Art. 4 (1a)]
- Der Dateninhaber soll zudem mit dem Nutzer vertraglich eine Beschränkung des Datenzugangs vereinbaren können, wenn der Zugang die vorgeschriebene Sicherheit des Produkts beeinträchtigen könnte [Art. 4 (1b)].

**Rat:**

- Laut dem Rat müssen Dateninhaber keinen Zugang zu Daten gewähren, die [Art. 2 (1af), EG 14a, 15]
  - das Ergebnis von Verarbeitungen sind, die die Daten wesentlich verändern,
  - bei der Verwendung des Produkts für den Zugang zu anderen Softwareanwendungen als den damit verbundenen Diensten aufgezeichnet werden, oder die
  - vernetzte Produkte bei der Aufzeichnung, Übertragung, Anzeige oder Wiedergabe von Inhalten wie z.B. Text-, Audio- oder audiovisuellen Inhalten erzeugen, sowie zu diesen Inhalten selbst.

**► In welcher Form müssen die Daten bereitgestellt werden?****Kommission:**

- Laut Kommission müssen die Daten in der Form und dem Format bereitgestellt werden, in dem sie erzeugt werden, und „gegebenenfalls kontinuierlich und in Echtzeit“ [Art. 4 (1), 5 (1), EG 17].

**Europäisches Parlament:**

- Das EP will ebenfalls, dass die Daten in der Form bereitgestellt werden, in der sie vom vernetzten Produkt abgerufen oder vom verbundenen Dienst erzeugt wurden, und zwar, soweit relevant und technisch machbar, kontinuierlich und in Echtzeit [Art. 4 (1), 5 (1), EG 17, 19].
- Wie bei Art. 17 DSGVO soll der Dateninhaber die Daten in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format bereitstellen.
- Zudem muss der Dateninhaber die Daten – falls erforderlich – durch geringfügige Anpassungen für Dritte nutzbar machen.
- Sind die Daten verschlüsselt, muss der Nutzer sie entschlüsseln können.
- Sofern rechtlich nichts anderes bestimmt ist, sollten Daten auf der Verarbeitungsebene zugänglich sein, und zwar auch mithilfe der in dem vernetzten Produkt enthaltenen Software.

**Rat:**

- Der Rat will, dass die Daten standardmäßig und kostenlos in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format leicht, sicher und gegebenenfalls direkt für den Nutzer zugänglich

sind. Die Zugangsgewährung sollte, soweit relevant und angemessen, kontinuierlich und in Echtzeit erfolgen. [Art. 3 (1), 4(1), 5(1)]

► **Welche Dritten sind berechtigt, Daten zu empfangen („Datenempfänger“) und wer kann die Weitergabe der Daten an einen Datenempfänger verlangen?**

**Kommission:**

– Laut Kommission sind Datenempfänger alle Personen, die zu geschäftlichen oder beruflichen Zwecken handeln und keine Nutzer sind. Gatekeeper sind ausgenommen, an sie dürfen die Daten nicht weitergegeben werden. Der Nutzer oder eine in seinem Namen handelnde Partei kann die Weitergabe an Dritte verlangen. [Art. 2 (7), Art. 5 (1), (2) Art. 6 (2), EG 36]

**Europäisches Parlament:**

– Laut dem EP können Datenempfänger alle natürlichen oder juristischen Personen in der EU sein, die nicht Nutzer vernetzter Produkte oder verbundener Dienste sind, u.a. Unternehmen, Forschungseinrichtungen, gemeinnützige Organisationen sowie Datenvermittlungsdienste und datenaltruistische Organisationen i.S.d. Data Governance Act [Verordnung (EU) 2022/68 („DGA“), s. [cepAnalyse](#), vgl. Art. 2 (7) (20c), EG 29].

– Ausgenommen sind laut EP neben Gatekeepern auch Empfänger außerhalb der EU, es sei denn, der Nutzer verlangt dies oder EU-Recht oder nationales Umsetzungsrecht bestimmt es [Art. 1 (4b)]. Auch ein Datenvermittlungsdienst i.S.d. DGA kann im Namen des Nutzers die Weitergabe verlangen [Art. 5 (1), EG 28].

**Rat:**

– Laut dem Rat sind Datenempfänger Unternehmen, Forschungseinrichtungen, gemeinnützige Organisationen und Einrichtungen, die in ihrer beruflichen Eigenschaft handeln [EG 29].

– Auch der Rat will, dass Datenvermittlungsdienste nach dem DGA Nutzer und Dritte bei der Herstellung einer Geschäftsbeziehung zur Datenweitergabe unterstützen dürfen, etwa indem sie im Namen eines Nutzers handeln [EG 29].

► **Wie werden Geschäftsgeheimnisse geschützt?**

**Kommission:**

– Laut Kommission müssen Dateninhaber gegenüber Nutzern Geschäftsgeheimnisse nur offenlegen, wenn diese alle erforderlichen Schutzvorkehrungen getroffen haben, um deren Vertraulichkeit – insbesondere gegenüber Dritten – zu wahren. Dateninhaber können mit Nutzern Maßnahmen zur Wahrung der Vertraulichkeit der Daten vereinbaren, etwa in einem Non-Disclosure-Agreement (NDA) [Art. 4 (3); 5 (8)].

– Auch gegenüber Dritten müssen Dateninhaber ggf. Geschäftsgeheimnisse offenlegen, soweit

- dies unbedingt erforderlich ist, um den zwischen Nutzern und Dritten vereinbarten Zweck zu erfüllen, und
- der Dritte alle mit Dateninhabern (vertraglich) – z.B. in einem NDA – vereinbarten und erforderlichen Maßnahmen zur Wahrung ihrer Vertraulichkeit getroffen hat.

**Europäisches Parlament:**

– Das EP präzisiert, dass der Nutzer vorab alle erforderlichen Schutzvorkehrungen nach der EU-Richtlinie über Geschäftsgeheimnisse getroffen haben muss. Der Dateninhaber oder der abweichende Inhaber der Geheimnisse muss die Geschäftsgeheimnisse aber als solche bestimmen. [Art. 4 (3), 5 (8)]

– Ferner präzisiert das EP die technischen und organisatorische Maßnahmen („TOMs“), die der Dateninhaber oder ein anderer Inhaber des Geschäftsgeheimnisses mit dem Nutzer oder dem Dritten vereinbaren kann (z.B. Mustervertragsbestimmungen, NDAs, strenge Zugangsprotokolle, technische Standards und die Anwendung von Verhaltenskodizes), aber auch Haftungsregeln. Setzt der Nutzer oder der Dritte die Maßnahmen nicht um oder untergräbt er die Vertraulichkeit der Geschäftsgeheimnisse, soll der Dateninhaber die Weitergabe dieser Daten aussetzen können; die zuständige Behörde („Datenkoordinator“) soll dann über den Streit entscheiden [Art. 4 (3), 5 (8)].

**Rat:**

– Der Rat will den Schutz von Geschäftsgeheimnissen ausweiten. So soll der Dateninhaber die Möglichkeit erhalten, Nutzer und Datenempfänger zum Schutz der Geschäftsgeheimnisse zu verpflichten, auch durch technische Maßnahmen. Diese können strenger ausfallen, wenn die Durchsetzbarkeit des Geheimnisschutzes schwierig ist, etwa wenn die Daten in Drittstaaten verarbeitet werden. Der Dateninhaber soll verpflichtet sein, Daten, die als Geschäftsgeheimnis geschützt sind, explizit zu kennzeichnen. [Art. 4 (3), EG 28a]

– Der Rat will Dateninhabern zudem das Recht einräumen, „in Ausnahmefällen“ Datenzugangsansprüche verweigern zu können. Dieses Recht sollen Dateninhaber nur dann erhalten, wenn die Schutzvorkehrungen

nicht ausreichen und die Preisgabe der Geschäftsgeheimnisse „mit hoher Wahrscheinlichkeit“ einen „schweren Schaden“ entstehen lässt. Als „schwere Schäden“ gelten etwa potenziell zu erwartende „erhebliche wirtschaftliche Verluste“, die die Existenz des Dateninhabers gefährden. Der Dateninhaber muss die Verweigerung explizit begründen und seiner zuständigen nationalen Behörde melden. [Art. 4 (3a), EG 28a]

### ► Wie dürfen Dateninhaber, Nutzer und Dritte die Daten nutzen?

#### **Kommission:**

- Laut Kommission dürfen Dateninhaber nicht-personenbezogene Daten, die bei der Nutzung eines vernetzten Produkts bzw. eines verbundenen Dienstes erzeugt werden, nur „auf der Grundlage“ eines Vertrags mit dem Nutzer nutzen [Art. 4 (6), EG 24].

#### **Europäisches Parlament:**

- Das EP schränkt die Nutzung durch den Dateninhaber weiter ein. Er soll nicht personenbezogene Daten nur zur Erfüllung seiner Pflichten gegenüber dem Nutzer an Dritte weitergeben, also nicht z.B. frei an Dritte verkaufen dürfen. Sofern der Nutzer ihm die Nutzung vertraglich erlaubt, soll er nicht personenbezogene Daten nur nutzen dürfen, um [Art. 4 (6a), (6b)]
  - die Funktionsweise des vernetzten Produkts oder des verbundenen Dienstes zu verbessern,
  - neue Produkte oder Dienste zu entwickeln, oder
  - aus den Daten durch Anreicherung, Manipulation oder Zusammenführung mit anderen Daten abgeleitete Datensätze zu erstellen und an Dritte zu verkaufen oder weiterzugeben. Datenelemente einzelner Nutzer dürfen für den Empfänger aus dem abgeleiteten Datensatz jedoch nicht abrufbar oder ermittelbar sein.

#### **Rat:**

- Der Rat unternimmt insoweit keine Änderungen am Vorschlag der Kommission.

#### **Kommission:**

- Laut Kommission dürfen Nutzer die Daten nicht zur Entwicklung von Produkten nutzen, die mit dem vernetzten Produkt im Wettbewerb stehen [Art. 4 (4)].

#### **Europäisches Parlament:**

- Das EP beschränkt dieses Verbot auf Konkurrenzprodukte, die in direktem Wettbewerb mit dem Produkt stehen, verbietet aber bereits die Entwicklung konkurrierender Produktteile [Art. 4 (4)].
- Laut dem EP darf der Nutzer alle nicht-personenbezogenen Daten, die er direkt vom Produkt abrufen oder über ein Verlangen vom Dateninhaber erhält, an einen Dritten (Datenempfänger) verkaufen oder zu nicht-kommerziellen Zwecken weitergeben. Die Weitergabe kann durch den Nutzer, den Dateninhaber oder über einen Datenvermittlungsdienst i.S.d. DGA erfolgen. Für den Vertrag zwischen Nutzer und Datenempfänger sollen die FRAND-Bestimmungen des Kapitels IV Data Act entsprechend gelten [Art. 4 (4b)].
- Ferner dürfen Nutzer die Daten auch zum Reverse Engineering nutzen, soweit die Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen dies erlaubt (EG 28).
- Geschäftliche Nutzer sollen gegenüber Dateninhabern oder -empfängern gegen angemessene Vergütung vertraglich auf ihr Recht zur eigenen Nutzung oder Weitergabe der Daten verzichten können. Die Dateninhaber oder Datenempfänger dürfen die Erbringung eines verbundenen Dienstes oder die Bedingungen dieser Erbringung einschließlich des Preises aber nicht von einem solchen Verzicht abhängig machen oder den Nutzer durch Zwang oder Täuschung zum Verzicht bewegen [Art. 4 (6c)].

#### **Rat:**

- Der Rat übernimmt den Vorschlag der Kommission. Er ergänzt, dass auch der Nutzer die Daten nicht an Dritte weitergeben darf, damit diese ein Konkurrenzprodukt entwickeln. Ob die betroffenen Produkte auf demselben Markt miteinander konkurrieren, bestimmt das EU-Wettbewerbsrecht. [Art. 4 (4), EG 28]

#### **Kommission:**

- Laut Kommission dürfen Datenempfänger die Daten u.a. nicht an andere Dritte weitergeben, außer dies ist zur Erbringung des vom Nutzer gewünschten Dienstes erforderlich [Art. 6 (2), EG 35].

#### **Europäisches Parlament:**

- Das EP stellt nun klar, dass Datenempfänger die eingeräumten Datenzugangsrechte aber dann (entgeltlich) auf andere Dritte übertragen dürfen, wenn der Nutzer klar hierauf hingewiesen wird und ausdrücklich vertraglich zustimmt [Art. 6 (2) lit. c, EG 29, 33].
- Ist der Nutzer zugleich die betroffene Person i.S.d. Datenschutzgrundverordnung (DSGVO), darf der Dritte die Daten für die vom Nutzer angegebenen Zwecke verarbeiten, z.B. [Art. 5 (1)]

- zur Erbringung von Anschlussdiensten (z.B. Wartung, Reparatur), wobei das EP nun auch im Gesetzestext klarstellt, dass diese Dienste – nicht aber vom Dritten mit den Daten entwickelte vernetzte Produkte – mit dem Produkt oder einem verbundenen Dienst des Dateninhabers „in Wettbewerb stehen“ dürfen,
- um dem Nutzer die Aktualisierung der Software des vernetzten Produkts oder des verbundenen Dienstes zu ermöglichen, oder wenn
- der Dritte ein anerkannter Datenvermittlungsdienst oder eine datenaltruistische Organisation i.S.d. DGA ist.
- Das EP will Dritten ausdrücklich die Verantwortung auferlegen, für die Sicherheit und den Schutz der vom Dateninhaber erhaltenen Daten zu sorgen [Art. 6 (2a)].
- Das EP will ferner regeln, dass (1) Dateninhaber nicht gegenüber Nutzern und (2) Nutzer oder Datenempfänger nicht gegenüber Dritten für Schäden aus den bereitgestellten bzw. weitergegebenen Daten haften, sofern sie den Data Act einhalten, die Daten rechtmäßig verarbeiten sowie die einschlägigen Cybersicherheitsanforderungen und die TOMs zur Wahrung ihrer Vertraulichkeit erfüllen [Art. 4 (1c)].

**Rat:**

- Der Rat übernimmt den Vorschlag der Kommission. Er ergänzt, dass Datenempfänger die Daten auch dann nicht an andere Dritte weiterreichen dürfen, wenn diese nicht die notwendigen Maßnahmen getroffen haben, um die Vertraulichkeit der Geschäftsgeheimnisse des Dateninhabers zu wahren. [Art. 6 (2) lit. c)]

► **Welche Vergütung ist für die Datenbereitstellung zu zahlen?****Kommission:**

- Laut Kommission können Dateninhaber, die gesetzlich verpflichtet sind, Daten bereitzustellen, von geschäftlich handelnden Datenempfängern – nicht aber von den Nutzern – eine „angemessene Gegenleistung“ für die Bereitstellung der Daten verlangen. Ist der Empfänger ein KMU, darf die Vergütung die unmittelbaren Bereitstellungskosten nicht übersteigen und nicht diskriminierend sein [Art. 9 (1), (2), Art. 8 (3), EG 42, 31].

**Europäisches Parlament:**

- Laut EP soll dies auch für Forschungseinrichtungen gelten, die die Daten gemeinnützig nutzen [EG 42, 44].
- Das EP ergänzt, dass eine angemessene Gegenleistung (außer bei KMU und Forschungseinrichtungen) neben den Kosten und den nötigen Investitionen für die Bereitstellung der Daten auch eine Marge umfassen kann [EG 42a]. Zu den Kosten und Investitionen können gehören:
  - Technische Kosten, z.B. für die Reproduktion, elektronische Verbreitung und Speicherung,
  - Kosten für die zur Bereitstellung erforderlichen Verarbeitung,
  - Kosten für die Erleichterung von Anfragen zur gemeinsamen Datennutzung,
  - nicht aber Kosten der Datensammlung oder -produktion.
- Die Höhe der Gegenleistung darf je nach Vereinbarung variieren, z.B. bei langfristigen oder regelmäßigen Transaktionen (Daten-Abonnements) niedriger sein [EG 42a].
- In der Marge dürfen auch die Datenerhebungskosten berücksichtigt werden; ferner kann die Höhe der Marge je nach der geplanten Nutzung durch den Empfänger und nach Menge, Format und Art der Daten sowie Angebot und Nachfrage variieren. Sie kann etwa bei erheblichen Investitionen in die Datenerhebung höher oder – wenn die Tätigkeit des Dateninhabers nicht eingeschränkt wird oder Daten durch den Nutzer als Besitzer eines vernetzten Produkts miterzeugt werden – niedriger ausfallen [EG 42a].
- Die Kommission soll in Leitlinien konkretisieren, wann Bedingungen „nichtdiskriminierend“ sind und wann die Gegenleistung angemessen ist [Art. 9(2a), EG 41, 42].
- Der Dateninhaber soll nur dann beweispflichtig sein, dass eine Vertragsklausel oder die vereinbarte Vergütung nichtdiskriminierend sind, wenn der Datenempfänger „begründete Bedenken“ hat, dass er diskriminiert wird [Art. 8 (3)].

**Rat:**

- Der Rat will, dass die Regeln zur Gegenleistung für die Datenbereitstellungen nur für Beziehungen zwischen Unternehmen (B2B) gelten. Er verlangt wie Kommission und EP, dass die Gegenleistung „angemessen“ sein muss. Der Rat erlaubt jedoch explizit, dass sie eine Marge enthalten kann. [Art. 9 (1)]
- Zudem konkretisiert er, dass eine Gegenleistung von der „Menge, dem Format und der Art der Daten“ abhängen kann und dass die „angefallenen Kosten und erforderlichen Investitionen“ – etwa für die Formatierung und Speicherung – sowie „Investitionen in die Datenerhebung und -produktion“ eine Rolle spielen dürfen. [Art. 9 (1a)]
- Laut dem Rat darf die vereinbarte Gegenleistung bei Datenempfängern, die KMU sind, jedoch nur die „angefallenen Kosten und erforderlichen Investitionen“ umfassen, nicht aber die „Investitionen in die Datenerhebung und -produktion“ [Art. 9 (2)].

► **Welche Transparenzpflichten gelten?**

**Kommission:**

- Laut Kommission müssen Nutzer bereits vor dem Erwerb des vernetzten Produkts oder verbundenen Dienstes u.a. klar über die erzeugten Daten und die Zugriffsmöglichkeiten informiert werden [Art. 3 (2)].

**Europäisches Parlament:**

- Das EP begrenzt die Transparenzpflichten auf zugängliche Daten, fordert aber zugleich die Angabe weiterer Informationen wie Format und Erhebungsfrequenz der Daten, Speicherkapazität des Geräts sowie eine Beschreibung der technischen Mittel für den Datenzugriff (z.B. Software Development Kits oder Anwendungsprogrammierschnittstellen) sowie deren Nutzungsbedingungen und die Dienstqualität. Angegeben werden muss auch, ob der Zugriff auf die Daten Geschäftsgeheimnisse berührt und wer deren Inhaber ist. [Art. 3 (2), EG 23].
- Das EP stellt zudem klar, dass die Transparenzpflichten erfüllt werden können, indem der Hersteller/Dateninhaber die erforderlichen Informationen im Internet bereithält und der Hersteller oder der Verkäufer diese vor Abschluss des Kaufvertrags per Weblink oder QR-Code einsehbar macht. Der Nutzer muss die Informationen speichern und auch nachträglich einsehen können [EG 23].

**Rat:**

- Der Rat behält die Transparenzvorgaben weitgehend bei. Er legt nun explizit fest, dass der Dateninhaber die Transparenzpflichten erfüllen muss. Auch wenn der Dateninhaber nicht der Verkäufer, Vermieter bzw. Leasinggeber des Produkts, ist er dafür verantwortlich, dass die Nutzer die Informationen erhalten. Ähnlich wie das EP schlägt der Rat vor, dass Dateninhaber die Informationen per Weblink oder QR-Code bereitstellen und die Verkäufer, Vermieter bzw. Leasinggeber vertraglich verpflichten, diese an die Nutzer weiterzugeben. Auch der Rat fordert, dass Nutzer die Informationen speichern können müssen. [Art. 3 (2), EG 23]
- Der Rat konkretisiert ferner, dass Dateninhaber die Nutzer informieren müssen, wenn sich die Informationen während der Lebensdauer des vernetzten Produkts ändern [EG 23].

► **Welche Unternehmen schützt der Data Act vor missbräuchlichen Vertragsklauseln?**

**Kommission:**

- Laut Kommission schützt der Data Act KMU, denen [Art. 13 (1), (5), EG 5, 51, 52]
  - eine Vertragsklausel in Bezug auf den Datenzugang und die Datennutzung oder in Bezug auf die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten
  - einseitig auferlegt wurde, die
  - missbräuchlich ist.
- Missbräuchliche Vertragsklauseln sind für KMU nicht bindend. Eine Vertragsklausel ist missbräuchlich, wenn [Art. 13 (2), (3), (4) EG 55]
  - sie unter eine „schwarze Liste“ stets missbräuchlicher Vertragsklauseln fällt oder
  - ihre Missbräuchlichkeit nach einer „grauen Liste“ vermutet wird, oder wenn
  - ihre Verwendung „gröblich von der guten Geschäftspraxis beim Datenzugang und der Datennutzung“ abweicht und gegen „Treu und Glauben“ und den „redlichen Geschäftsverkehr“ verstößt.

**Europäisches Parlament:**

- Laut EP sollen diese Regeln nicht nur zugunsten von KMU gelten, sondern alle Unternehmen egal welcher Größe schützen. Zudem will das EP die graue Liste der Klauseln erweitern, bei denen die Missbräuchlichkeit vermutet wird. [Art. 13 (1), (2), (4)]
- Ferner sollen Vertragsklauseln zusätzlich auch dann missbräuchlich sein, wenn sie [Art. 13 (2)]
  - die Fähigkeiten des Vertragspartners objektiv beeinträchtigen, sein berechtigtes Interesse an den Daten zu schützen, oder wenn sie
  - ein erhebliches Ungleichgewicht zwischen den Rechten und Pflichten der Vertragsparteien schaffen.
- Schließlich will das EP, dass Unternehmen auch bestehende Verträge innerhalb von drei Jahren prüfen und ggf. an diese Regeln anpassen müssen. [Art. 13 (8a)].

**Rat:**

- Der Rat will ebenfalls erreichen, dass die Regeln zum Schutz vor missbräuchlichen Vertragsklauseln für alle Unternehmen egal welcher Größe gelten [Art. 13 (1)].
- Zusätzlich soll die Missbräuchlichkeit auch bei Klauseln vermutet werden, die darauf abzielen, die Haftung des Unternehmens zu erweitern, dem die Klausel auferlegt wurde [Art. 13 (4)].