Countdown Data Act: 15 Kernpunkte zur Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung

10. Oktober 2024

Die Verordnung (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung, der sog. Data Act (hier abrufbar), ist ein wichtiger Bestandteil der EU-Digitalstrategie, der darauf abzielt, die Grundlagen für eine datengetriebene Zukunft in der EU zu schaffen. Zweck des Data Acts ist es, klare Regeln für den Zugang zu und die Nutzung von Daten zu schaffen. Im Kern geht es darum, einen freien Datenfluss innerhalb des Binnenmarktes zu fördern, innovative Geschäftsmodelle zu unterstützen und gleichzeitig die Privatsphäre und Datensicherheit zu gewährleisten. Die Auswirkungen des Data Acts sind daher sehr weitreichend und betreffen zahlreiche Sektoren. Angesichts der Komplexität und Neuartigkeit des Data Acts ist ein klares Verständnis für die verschiedenen Aspekte der Verordnung entscheidend. Hier setzt das folgende Q&A an, das darauf abzielt, die wichtigsten Fragen zum Data Act zu beantworten.

1. Ab wann muss der Data Act beachtet werden?

Der Data Act ist am 11. Januar 2024 in Kraft getreten. Die Regelungen des Data Acts sind gemäß Art. 50 Abs. 2 Data Act überwiegend **ab dem 12. September 2025** anwendbar.

2. Was sind die wesentlichen Regelungsbereiche des Data Act?

Der Data Act ist geprägt durch die folgenden, unterschiedlichen und teilweise nicht aufeinander aufbauenden Regelungsbereiche:

- Datenzugangsansprüche
- Missbräuchliche Vertragsklauseln zwischen Unternehmen
- Wechsel von Datenverarbeitungsdiensten
- Mindestanforderungen an die Interoperabilität von Daten

3. Auf welche Unternehmen ist der Data Act anwendbar?

Der Data Act ist mit seinen unterschiedlichen Regelungsbereichen auf folgende Unternehmen anwendbar:

a) Der Data Act verpflichtet **Hersteller von vernetzten Produkten** und **Anbieter von verbundenen Diensten** zur Bereitstellung von Daten.

Ein vernetztes Produkt ist ein Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und diese Daten übermitteln kann. Gemeint sind beispielsweise IoT-Geräte wie Smart Cars, Wearables, Smartphones, virtuelle Sprachassistenten, intelligente Sicherheitssysteme oder Navigationssysteme.

Ein verbundener Dienst ist ein digitaler Dienst, der so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen eines vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen. Zu diesen verbundenen Diensten können beispielsweise zusätzliche Beratungs-, Analyse- oder Finanzdienstleistungen sowie regelmäßige Reparatur- und Wartungsdienste gehören.

b) Daneben gilt der Data Act auch für **Dateninhaber** (unabhängig vom Ort ihrer Niederlassung), die Daten an Datenempfänger in der Union bereitstellen.

Dateninhaber bezeichnet dabei eine natürliche oder juristische Person, die nach dem Data Act, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat.

c) Darüber hinaus fallen Unternehmen, die mit anderen Unternehmen Datenzugangsvereinbarungen schließen, aber auch Anbieter von Datenverarbeitungsdiensten sowie Teilnehmer an europäischen Datenräumen in den Regelungsbereich des Data Acts.

4. Ist der Data Act auf Unternehmen mit Sitz außerhalb der EU anwendbar?

Der Anwendungsbereich des Data Act ist weit gefasst und legt das Marktortprinzip zu Grunde. Anknüpfungspunkt für den räumlichen Anwendungsbereich ist daher der Ort, an dem das vernetzte Produkt in Verkehr gebracht wird. Insofern kann der Data Act auch auf Unternehmen anwendbar sein, die nicht in der Union niedergelassen sind. Das können Unternehmen sein, die vernetzte Produkte herstellen, die in der Union in Verkehr gebracht werden, sowie Unternehmen, die verbundene Dienste in der Union anbieten.

5. Ist der Data Act auch auf kleinere und mittlere Unternehmen anwendbar?

Der Data Act ist auch auf kleinere und mittlere Unternehmen – sog. KMU – anwendbar, enthält aber einige Ausnahmen für Kleinst- und Kleinunternehmen, d.h. Unternehmen mit weniger als 50 Beschäftigten und maximal EUR 10 Mio. Jahresumsatz. Für diese gelten die folgenden Erleichterungen:

- Die Pflicht zur Bereitstellung von Produktdaten oder verbundenen Dienstdaten an Nutzer:innen oder einen Dritten gilt nicht, wenn das vernetzte Produkt von einem Kleinst- oder Kleinunternehmen hergestellt oder konzipiert wurde oder wenn ein solches Unternehmen die verbundenen Dienste erbringt. Diese in Art. 7 Abs. 1 Data Act geregelte Ausnahme gilt nicht, wenn das Kleinst- oder Kleinunternehmen ein Partnerunternehmen oder ein Konzernunternehmen hat, welches kein Kleinst- oder Kleinunternehmen ist oder wenn das Kleinst- oder Kleinunternehmen als Unterauftragnehmer mit der Herstellung oder Konzeption eines vernetzten Produktes oder der Erbringung des verbundenen Dienstes beauftragt wurde.

  Für mittlere Unternehmen (weniger als 250 Beschäftigte und bis zu EUR 50 Mio. Jahresumsatz) gelten die Bereitstellungspflichten hingegen ausnahmslos, allerdings erst ein Jahr nachdem (i) das vernetzte Produkt in Verkehr gebracht wurde oder (ii) ein Unternehmen die Schwellenwerte eines „mittleren Unternehmens" überschritten hat.

- Auch hinsichtlich der Pflicht zur Bereitstellung von Daten an öffentliche Stellen in Fällen außergewöhnlicher Notwendigkeit werden Kleinst- oder Kleinunternehmen privilegiert. An die außergewöhnliche Notwendigkeit werden gem. Art. 15 Abs. 2 Data Act bei Kleinst- oder Kleinunternehmen strengere Anforderungen gestellt. Außerdem steht ihnen nach Art. 20 Abs. 1 Data Act auch in den Fällen ein finanzieller Ausgleich für die Datenbereitstellung zu, in denen größere Unternehmen die Daten kostenfrei bereitzustellen haben.

6. Welche Datenzugangsansprüche ergeben sich aus dem Data Act für die Nutzer:innen?

Der Data Act regelt den Zugang zu Daten vernetzter Produkte oder damit verbundener Dienste. Im Ausgangspunkt steht die Idee, dass den Nutzer:innen Zugang zu sämtlichen Daten gewährt werden soll, an deren Erstellung die Nutzer:innen selbst beteiligt waren. Die Nutzer:innen sollen einerseits erfahren können, wie ihre Daten vom Dateninhaber genutzt werden und andererseits darüber entscheiden können, ob diese Daten mit Dritten geteilt werden. Dabei kann zwischen drei verschiedenen – gesetzlich einklagbaren – Zugangsrechten unterschieden werden:

- **Erste Konstellation**: Art. 3 Data Act verpflichtet Dateninhaber dazu, vernetzte Produkte so zu konzipieren und herzustellen, dass Nutzer:innen einen direkten Zugang zu Produktdaten

und verbundenen Dienstdaten erhalten. In den Fällen, in denen dieser direkte Zugriff nicht möglich ist, sind Dateninhaber nach Art. 4 Abs. 1 Data Act dazu verpflichtet, die Daten unverzüglich, unentgeltlich, in einem maschinenlesbaren Format sowie kontinuierlich und in Echtzeit bereitzustellen.

- **Zweite Konstellation**: Darüber hinaus sind Dateninhaber nach Art. 5 Abs. 1 Data Act dazu verpflichtet, auf Verlangen der Nutzer:innen Daten einem Dritten bereitzustellen. Eine Bereitstellung der Daten kann auch an Wettbewerber des Dateninhabers erfolgen. Handelt es sich bei dem Wettbewerber allerdings um ein Unternehmen, das in der Union als Torwächter im Sinne des Art. 3 Digital Markets Act (DMA) benannt worden ist, müssen die Daten nicht bereitgestellt werden.
- **Dritte Konstellation**: Ein dritter Datenzugangsanspruch ist in Art. 14 Data Act geregelt. Danach sind Dateninhaber dazu verpflichtet einer öffentlichen Stelle Daten bereitzustellen, wenn diese den Nachweis erbringen kann, dass im Hinblick auf die Erfüllung ihrer rechtlichen Aufgaben im öffentlichen Interesse die außergewöhnliche Notwendigkeit der Nutzung dieser Daten besteht. Der Datenzugangsanspruch ist vor allem für Fälle relevant, in denen die verlangten Daten zur Bewältigung eines öffentlichen Notstands erforderlich sind und nicht auf andere Weise rechtzeitig und wirksam beschafft werden können.

7. Welche Daten sind von den Zugangsansprüchen des Data Act erfasst?

Die Nutzer:innen können die Bereitstellung aller Produktdaten oder verbundenen Dienstdaten verlangen, die ohne Weiteres verfügbar sind. Nach Art. 1 Abs. 2 Data Act sind sowohl personenbezogene als auch nicht-personenbezogene Daten im Sinne der Datenschutz Grundverordnung („**DS-GVO**“) vom Anwendungsbereich erfasst. Zudem umfasst der Anwendungsbereich Daten, die von den Nutzer:innen bewusst aufgezeichnet werden oder die im Zusammenhang mit der Nutzung des vernetzten Produkts entstehen, andererseits aber auch Daten, die ohne Zutun der Nutzer:innen oder im ausgeschalteten Zustand des Produkts generiert werden.

8. Kann der Dateninhaber für die Herausgabe der Daten eine Gegenleistung verlangen?

Die Pflicht zur Gegenleistung ist abhängig vom Datenempfänger:

- Die Bereitstellung von Daten **an die Nutzer:innen** muss immer kostenlos erfolgen.
- Die Bereitstellung von Daten **an einen Dritten**, der nicht Nutzer:in des vernetzten Produkts oder verbundenen Dienstes ist, richtet sich nach Art. 9 Data Act. Von einem Dritten darf eine Gegenleistung verlangt werden, wenn es sich um ein Unternehmen handelt. Diese Gegenleistung muss diskriminierungsfrei und angemessen sein. Sie darf auch eine Marge enthalten, wenn es sich bei dem Datenempfänger nicht um ein kleines oder mittleres Unternehmen handelt. Bei der Vereinbarung der Gegenleistung sollen die angefallenen Kosten für die Bereitstellung der Daten und die Investitionen in die Erhebung und Generierung der Daten berücksichtigt werden. Wenn es sich bei dem Dritten nicht um ein Unternehmen handelt, ist unklar, ob eine Gegenleistung verlangt werden kann. Der Data Act enthält hierzu keine ausdrückliche Regelung.

9. Welche Pflichten gelten für Datenempfänger?

Datenempfänger ist nach Art. 2 Nr. 14 Data Act ein Dritter, dem auf Verlangen der Nutzer:innen Produktdaten oder verbundene Dienstdaten bereitgestellt werden. Art. 6 Data Act regelt besondere Pflichten für Datenempfänger:

- Datenempfänger dürfen die ihnen bereitgestellten Daten nur zu den Zwecken und unter den Bedingungen nutzen, die sie mit den Nutzer:innen vereinbart haben. Grundsätzlich sind die Daten zu löschen, sobald sie für den vereinbarten Zweck nicht mehr benötigt werden. Handelt

es sich um personenbezogene Daten, müssen außerdem die Vorgaben der DS-GVO beachtet werden.

- Datenempfänger dürfen die ihnen bereitgestellten Daten nicht ohne die Zustimmung der Nutzer:innen an einen Dritten weitergeben.
- Datenempfänger dürfen die erhaltenen Daten nicht nutzen, um ein Produkt zu entwickeln, das mit dem vernetzten Produkt, von dem die Daten stammen, im Wettbewerb steht oder Daten zu diesem Zweck weitergeben.
- Datenempfänger dürfen Nutzer:innen, bei denen es sich um Verbraucher:innen handelt, nicht daran hindern, die erhaltenen Daten auch einer anderen Partei zur Verfügung zu stellen.

10. Darf der Dateninhaber den Nutzer:innen auch personenbezogene Daten bereitstellen?

Im Hinblick auf personenbezogene Daten überschneiden sich die Anwendungsbereiche von Data Act und DS-GVO. Die DS-GVO enthält ein Verbot mit Erlaubnisvorbehalt: Die Verarbeitung von personenbezogenen Daten ist untersagt, soweit die Verarbeitung nicht auf einen Erlaubnistatbestand nach Art. 6 Abs. 1 DS-GVO oder Art. 9 Abs. 2 DS-GVO gestützt werden kann. Die Bereitstellung von personenbezogenen Daten an Nutzer:innen oder einen Dritten ist eine Datenverarbeitung im Sinne der DS-GVO und somit nur zulässig, wenn diese Datenverarbeitung von einer Rechtsgrundlage gedeckt ist. Ob eine solche Rechtsgrundlage im Einzelfall zur Verfügung steht, hängt insbesondere von der Vorfrage ab, ob die Nutzer:innen zugleich Betroffene im Sinne von Art. 4 Nr. 1 DS-GVO sind:

- **Nutzer:innen sind zugleich Betroffene im Sinne der DS-GVO**: In der ersten Konstellation handelt es sich bei den herausverlangten personenbezogenen Daten um „eigene" Daten der Nutzer:innen. In diesem Fall wird man das Datenzugangsverlangen nach Art. 4 Abs. 1 Data Act oder Art. 5 Abs. 1 Data Act gleichzeitig auch als datenschutzrechtliche Einwilligung in die Datenverarbeitung ansehen müssen.
- **Nutzer:innen sind nicht zugleich Betroffene im Sinne der DS-GVO**: Problematischer ist der Fall, in dem die Nutzer:innen nicht zugleich Betroffene im Sinne der DS-GVO sind. Das kann beispielsweise der Fall sein, wenn ein Fahrzeug – etwa beim Carsharing – von mehreren Personen genutzt wird. In solchen Fällen ist die Bereitstellung der personenbezogenen Daten nur möglich, wenn eine datenschutzrechtliche Einwilligung sämtlicher Betroffener in die Herausgabe vorliegt, eine vertragliche Notwendigkeit für die Herausgabe besteht oder wenn eine Notwendigkeit zur Wahrung berechtigter Interessen vorliegt.

11. Müssen Daten auch bereitgestellt werden, wenn durch die Bereitstellung Geschäftsgeheimnisse offengelegt werden?

Grundsätzlich müssen alle Daten offengelegt werden – also auch solche, die Geschäftsgeheimnisse enthalten. Der Dateninhaber kann allerdings technische und organisatorische Maßnahmen mit den Nutzer:innen vereinbaren, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren. Zu diesen Maßnahmen zählen beispielsweise die Verwendung von Mustervertragsklauseln, Vertraulichkeitsvereinbarungen und strengen Zugangsprotokollen. Ausnahmsweise kann die Bereitstellung der Daten verweigert werden, wenn zwischen dem Dateninhaber und den Nutzer:innen keine Vereinbarung über die erforderlichen Maßnahmen zum Schutz der Geschäftsgeheimnisse zustande kommt oder die Nutzer:innen die Umsetzung dieser Maßnahmen unterlassen. Ferner kann die Bereitstellung von Daten im Einzelfall verweigert werden, wenn der Dateninhaber trotz der getroffenen technischen und organisatorischen Maßnahmen durch die Offenlegung mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden erleiden wird. In beiden Fällen muss der Dateninhaber seine Entscheidung begründen, den Nutzer:innen unverzüglich schriftlich mitteilen und die zuständigen Aufsichtsbehörde informieren.

12. Können Datenzugangsansprüche der Nutzer:innen vertraglich abbedungen werden?
Nein. Nach Art. 7 Abs. 2 Data Act sind Vertragsklauseln, die Datenzugangsansprüche über die im Data Act festgelegten Grenzen zum Nachteil der Nutzer:innen einschränken oder ausschließen, nicht bindend. Es bedarf somit einer Einzelfallprüfung und -rechtfertigung, ob im Rahmen bestehender Verträge mit Nutzer:innen ein Zugangsanspruch – etwa aus der Notwendigkeit des Geschäftsgeheimnisschutzes – abgelehnt werden kann.

13. Zwei Unternehmen schließen einen Vertrag über den Datenzugang und die Datennutzung. Welche Anforderungen müssen bei der Vertragsgestaltung beachten?
Ist ein Dateninhaber verpflichtet, einem anderen Unternehmen Daten bereitzustellen, sind im Rahmen der zu treffenden Datenbereitstellungsvereinbarungen insbesondere folgende Aspekte zu beachten:

- Für B2B-Verträge, die einen Datenbezug aufweisen und einseitig auferlegt werden, ist eine Missbrauchskontrolle vorgesehen, vgl. Kapitel IV Data Act.
- Zudem müssen für bestimmte Datenbereitstellungsvereinbarungen sog. FRAND-Grundsätze berücksichtigt werden (vgl. Art. 8 Abs. 1 Data Act): Um vertragliche Ungleichgewichte zu verhindern, muss die Bereitstellung von Daten nach dem Data Act zu fairen, angemessenen und nichtdiskriminierenden Bedingungen in transparenter Art und Weise erfolgen.

14. Welche Regelungen enthält der Data Act für den Wechsel zwischen Datenverarbeitungsdiensten?
Die Bedingungen für den Wechsel zwischen Datenverarbeitungsdiensten sind nach Art. 25 Abs. 1 Data Act schriftlich festzulegen und vor Vertragsunterzeichnung in speicherbarer und reproduzierbarer Form bereitzustellen. Zudem gibt es eine Vielzahl von konkreten Anforderungen an die Wechselbedingungen, die es zu erfüllen gilt. Beispielsweise darf die Kündigungsfrist nicht länger als zwei Monate betragen. Außerdem müssen bestehende Wechselentgelte schrittweise abgeschafft werden.

15. Welche Sanktionen sieht der Data Act im Falle von Verstößen vor?
Durch Art. 40 Data Act werden die einzelnen Mitgliedstaaten dazu verpflichtet, Vorschriften über Sanktionen zu erlassen, die bei Verstößen gegen den Data Act zu verhängen sind und alle für die Anwendung dieser Sanktionen erforderlichen Maßnahmen zu treffen. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein und orientieren sich grundsätzlich an den aus der DS-GVO bekannten Geldbußen in Höhe von bis zu 4 % des weltweiten Jahresumsatzes.

***