MENOLD BEZLER

10 Fragen und Antworten zum Data Act (DA)

1 Was regelt der Data Act?

Die „Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung“ (kurz: **Datengesetz** oder **Data Act**) **regelt den Zugang und die Nutzung von Daten,** die beim Einsatz von Produkten und verbundenen Diensten generiert werden. Es erfolgt jedoch keine Regelung in Bezug auf die Frage des Dateneigentums. Ziel des Gesetzes ist es den Datenaustausch zwischen Unternehmen über Branchen hinweg sowie zwischen Unternehmen und staatlichen Institutionen zu verbessern. Dadurch soll eine **funktionierende und wettbewerbsfähige Datenwirtschaft innerhalb der EU** entstehen.

2 Auf welche Produkte findet der Data Act Anwendung?

Der Data Act findet Anwendung auf **Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden**. Der Datenbegriff des Data Act ist sehr weit gefasst und beinhaltet j**egliche digitale Darstellung einer Information** unabhängig davon, ob die Information personenbezogenen oder nicht-personenbezogene ist. Betroffen sind nach dem Data Act **vernetzte Produkte**, wie etwa Haushaltsgeräte, Fahrzeuge oder Industriemaschinen, die mit dem Internet verbunden sind. Umfasst von der Regulierung sind auch **digitale Dienste**, ohne die ein Produkt seine Funktionen nicht ausführen könnte, wie beispielsweise die Software einer Fitnessuhr. Die Verordnung nimmt folglich Daten, die durch **IOT-fähige Geräte oder damit verbundene Cloud-Dienste** erzeugt werden, in den Fokus. Gerade diese Daten sind besonders wertvoll für die Entwicklung und Wartung neuer Produkte sowie das Training von selbstlernenden Algorithmen der Künstliche Intelligenz, werden jedoch derzeit vor allem von Herstellern solcher Produkte gespeichert und verwertet.

Wer ist vom DataAct betroffen?

Die Verordnung richtet sich insbesondere an **Unternehmen, die IOT-fähige Produkte und verbundenen Dienste entwickeln** und/oder vertreiben sowie **Cloud-Anbieter**. Für kleine und Kleinstunternehmen (KMU) gelten gewisse Ausnahmen bezüglich des Datenzugangsrechts. Adressiert sind zudem **private als auch unternehmerische Nutzer** von IOT-fähigen Geräten und verbundenen Diensten sowie in bestimmten Situationen zudem öffentliche Stellen. Wie bereits in der DSGVO kommt auch beim Data Act das **Marktortprinzip** zum Tragen, wonach auch **nicht-europäische Unternehmen**, wenn diese entsprechende IOT-fähige Produkte und verbundene Dienste innerhalb der EU anbieten, von den Regelungen erfasst werden.Regelungen erfasst werden.

Welche Pflichten müssen Unternehmen im Rahmen des Datenzugangs umsetzen?

Zentrale Regelung des Data Acts ist die Pflicht **Daten**, die bei der Nutzung von vernetzten Produkten und verbundenen Diensten entstehen, **sowohl im B2C als auch im B2C-Bereich zugänglich zu machen.** Die Produkte und verbundenen Dienste müssen zu diesem Zweck anhand der Vorgaben aus dem Data Act gestaltet werden („**Access by Design**").

Die Daten sollen den Nutzern idealerweise **durch direkten Zugriff** auf das vernetzte Produkt oder den verbundenen Dienst zur Verfügung gestellt werden. Die durch vernetzte Produkte erzeugten Daten müssen folglich hard- oder softwareseitig direkt zugänglich gemacht werden, was erfordert, dass Hersteller IOT-fähige Geräte entsprechend konstruieren oder anpassen. **Alternativ** müssen die Daten den Nutzern **„unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit"** zur Verfügung gestellt werden. Dies könnte durch Darstellung in einem über eine Website abrufbaren Dashboard, das kontinuierlich mit aktuellen Daten gespeist wird, realisiert werden.

Die Nutzer können den **Anspruch auf Datenzugang** mittels einfachen Verlangens auf elektronischem Weg **gegen den sogenannten Dateninhaber** geltend machen. Die Dateninhaberschaft wird durch die Kontrolle über die technische Konzeption des vernetzten Produktes und damit die tatsächliche Fähigkeit, Daten bereitzustellen, definiert. Neben dem Hersteller eines vernetzten Produktes kann auch ein Nutzer, dem Daten bereitgestellt wurden, seinerseits Dateninhaber werden, wenn es sich dabei um ein Unternehmen handelt, das beispielsweise im Vertriebsnetz des Herstellers dessen Produkte vertreibt.

Zudem treffen Hersteller und Verkäufer vernetzter Produkte zukünftig **umfangreiche Informationspflichten**, insbesondere über Art und Umfang der Daten, die bei der Nutzung voraussichtlich erzeugt werden, und die Absicht sowie Zwecke, die Daten selbst zu nutzen oder Dritten zur Verfügung zu stellen. Diese Informationen müssen dem Nutzer vor Abschluss des Kauf-, Miet- oder Leasingvertrages für z.B. ein IoT-fähiges Produkt. mitgeteilt werden.

Der Dateninhaber darf die entstandenen Daten zudem selbst nur zu eigenen Zwecken nutzen, wenn dies mit dem Nutzer ausdrücklich vertraglich vereinbart wurde. Unternehmen müssen sich daher zukünftig von Beginn an **vertragliche Nutzungsrechte in Bezug auf die Daten der von ihnen vertriebenen vernetzten Produkte** einräumen lassen.

Die Vereinbarung über den Datenzugang sowie die eigene Datennutzung des Anbieters kann auch zukünftig auf Basis eines Vertrages erfolgen. Allerdings hat die Datenbereitstellung zu fairen, angemessenen und nichtdiskriminierenden Bedingungen zu erfolgen und es sind zukünftig die Bestimmungen über das **Verbot missbräuchlicher Klauseln** gemäß Art. 13 Data Act zu beachten.

Darüber hinaus erhalten auch **öffentliche Stellen** nach den neuen Vorschriften **in gewissen Ausnahmesituation**, z.B. Naturkatastrophen oder Pandemien, auf Verlangen **Zugang zu Daten**.

Welche Anforderungen sind hinsichtlich der Datenweitergabe zu beachten?

Auf Verlangen des Nutzers muss eine **Herausgabe der Daten auch an Dritte** erfolgen. Der Datenempfänger unterliegt ebenfalls gewissen Pflichten, insbesondere hinsichtlich Zweckbindung und Löschung der Daten. Der Eigentümer eines (vernetzten) Fahrzeugs (= Nutzer) kann zukünftig also beispielsweise verlangen, dass der Fahrzeughersteller (= Dateninhaber) die über den Nutzer generierten Daten an eine Reparaturwerkstatt weitergibt.

Wie bei der DSGVO werden Vorgaben für die Datenweitergabe in Länder außerhalb der EU gemacht. Es müssen **Schutzmaßnahmen bei der internationalen Datenübermittlung** getroffen werden, um den unberechtigten Zugriff von behördlichen Stellen außerhalb der EU auf Daten zu verhindern.

Was ist im Zusammenhang mit dem Wechsel zwischen Datenverarbeitungsdiensten und der Interoperabilität einzuhalten?

Nach dem Data Act müssen Datenverarbeitungsdienste, wie Cloud-Anbieter, den **einfachen Wechsel** zu einem anderen Anbieter ermöglichen. Dazu müssen entsprechende **Schnittstellen bereitgestellt** und **Interoperabilitätsstandards eingehalten** werden. Anbieter müssen den Kunden ermöglichen, alle digitalen Vermögenswerte inklusive Daten zu übertragen und deren Nutzung in der neuen Umgebung funktionaläquivalent ermöglichen. Das bedeutet, dass ein **Mindestfunktionsumfang nach dem Wechsel gewährleistet sein** muss, mit dem der Nutzer den Dienst bei dem gleichen Sicherheitsniveau, Betriebsstabilität und Dienstqualität fortführen kann. Um den Wechsel zu erleichtern, muss dem Kunden ermöglicht werden innerhalb von 30 Tagen den bestehenden Vertrag zu kündigen und der aktuelle Anbieter hat jegliche erforderliche Unterstützung und Hilfe anzubieten.

Welche Sanktionsmöglichkeiten und Rechtfolgen sieht der Data Act vor?

Den Berechtigten aus dem Data Act, also insbesondere den Nutzern von vernetzten Produkten und verbundenen Diensten, steht ein **Beschwerderecht** zu. Die verantwortlichen Behörden werden ermächtigt **Untersuchungsmaßnahmen** einzuleiten und **„abschreckende“ finanzielle Sanktion** zu verhängen. Es wird zum Teil auf die **Regelungen der DSGVO bezüglich der Bedingungen und Höhe von Bußgeldern** verwiesen.

8 In welchem Verhältnis steht der Data Act zum Datenschutzrecht?

Der Data Act findet **neben den Regelungen zum Datenschutz** wie der DSGVO und dem TTDSG Anwendung, soll diese ergänzen und den Datenschutz in keinem Fall schwächen. Dies führt zu einem gewissen **Spannungsverhältnis**: Ziel des Data Acts ist es einen fairen Datenzugang und die faire Datennutzung zu ermöglichen, während die Datenschutzgesetze einen möglichst umfassenden Schutz natürlicher Personen bei der Verarbeitung deren **personenbezogener Daten** gewährleisten sollen. Der Data Act sieht einige Regelungen vor, um diesen Widerspruch in Einklang zu bringen. Handelt es sich bei den Daten um personenbezogene Daten dürfen diese etwa **nur an die betroffene Person** und an Dritte nur **bei Vorliegen einer datenschutzrechtlichen Rechtsgrundlage** herausgegeben werden. Der Data Act selbst kann jedoch nicht als Rechtsgrundlage für die Datenverarbeitung herangezogen werden. Bei dem Datenzugang sowie der Datenweitergabe sollen **technische und organisatorische Schutzmaßnahmen** eingesetzt werden.

9 Ab wann gilt der Data Act?

Der Data Act tritt am 11. Januar 2024 in Kraft. Der Data Act wird im Grundsatz nach einer Übergangfrist von 20 Monaten nach Inkrafttreten **ab dem 12.09.2025 unmittelbar in allen EU-Mitgliedstaaten anwendbar** sein. Ab diesem Tag sind die Datenbereitstellungspflichten zu erfüllen sowie das „Daten-AGB-Recht" gültig. Für die folgenden Regelungen sind jedoch abweichende Anwendungsfristen vorgesehen: Die Vorgabe zum sog. „Access by Design", das bedeutet die Pflicht zur Gestaltung von Produkten und verbundenen Diensten unter Berücksichtigung der Möglichkeit des Datenzugriffs, greift erst nach weiteren 12 Monaten zum 13.09.2026. Die Anforderungen an vertragliche Klauseln sollen für bestehende Verträge unter bestimmten Bedingungen erst weitere 2 Jahr nach der Übergangfrist ab dem 12.09.2027 gelten.

10 Was sollten Unternehmen bereits tun?

Unternehmen sollten nun prüfen, in welcher Rolle sie im Rahmen ihrer Geschäftstätigkeit von dem Data Act erfasst sind. Insbesondere der Anspruch auf Datenzugang sowie die Bestimmungen zur Datenweitergabe und Interoperabilität erfordern die **Berücksichtigung bei der Konzeption und Herstellung von Produkten und der verbundenen Dienste.** Es müssen daher bereits bei der Planung von Produktionszyklen der Datenzugang by Design in der Produktentwicklung berücksichtigt werden. Zudem sind die **Verträge mit Kunden auf Einhaltung der Vorgaben des Data Act zu überprüfen**, insbesondere daraufhin, ob missbräuchliche Klauseln verwendet wurden, und gegebenenfalls anzupassen. Nicht nur wegen der Ähnlichkeit mancher Regelungsinhalte, sondern auch aufgrund der zahlreichen Pflichten, die der Data Act für betroffene Unternehmen vorsieht, dürften dessen Auswirkungen mit der DSGVO, vergleichbar sein. Mit Blick auf die Erfahrungen mit der praktischen Implementierung der Vorgaben der DSGVO, ist daher eine **rechtzeitige Beschäftigung mit den notwendigen Umsetzungen** zu empfehlen.

Autorin: Varinia Iber

Unser Team aus dem Bereich IT- / Internet- und Datenschutzrecht

Dr. Jörg Schneider-Brodtmann, LL. M
Partner, Rechtsanwalt
joerg.schneider-brodtmann
@menoldbezler.de
Tel.: +49 711 86040 350

Dr. Carsten Ulbricht M.C.L.
Partner, Rechtsanwalt
carsten.ulbricht@menoldbezler.de
Tel.: +49 711 86040 025

Carolin Nemec, LL.M. (UCC)
Rechtsanwältin
carolin.nemec@menoldbezler.de
Tel.: +49 711 86040 791

Varinia Iber
Rechtsanwältin,
Fachanwältin für IT Recht
varinia.iber@menoldbezler.de
Tel.: +49 711 86040 025

Jessica Hawighorst
Rechtsanwältin
jessica.hawighorst@menoldbezler.de
Tel.: +49 711 86040 760