



DAS RECHT AUF DATENPORTABILITÄT

RATGEBER FÜR UNTERNEHMEN

WAS IST DATENPORTABILITÄT?

Mit dem neuen europäischen Recht auf Datenübertragbarkeit (Art. 20 der EU-Datenschutz-Grundverordnung) haben die Bürger ab Mai 2018 das Recht, ihre personenbezogenen Daten von einem Dienstanbieter direkt zu erhalten oder unmittelbar zu einem neuen Dienstleister übertragen zu lassen. Alle Unternehmen sind demnach verpflichtet, auf Anfrage jeder natürlichen Person die sie betreffenden und von ihr bereitgestellten personenbezogenen Daten in einem strukturierten, maschinenlesbaren Format zu übermitteln. Das schafft Chancen für neue Geschäftsmodelle und Dienstleistungen, bringt aber auch Risiken bei der Umsetzung mit sich.

Bisher konnte man eine Datenübertragung vor allem als Umzugsservice beim Wechsel eines Bankkontos, beim Nachsendeauftrag der Post oder bei der Telefonnummer-Mitnahme. Demnächst gilt sie für alle Dienstanbieter, die mit personenbezogenen Daten ihrer Kunden umgehen.

Was ist vom Gesetzgeber bezweckt?

Die Idee hinter der neuen Regelung ist, Kunden den Wechsel zwischen unterschiedlichen Internetdiensten zu erleichtern. Der Gesetzgeber hofft, dass mit der Möglichkeit der Mitnahme „eigener“ Daten die Schwelle zum Wechsel von Anbietern digitaler Dienste sinkt und die



Verbraucher bessere Kontrollmöglichkeiten über ihre Daten erhalten. Es ist jedoch nicht auszuschließen, dass auch herkömmliche Dienstleistungen unter die neue Regelung fallen.

Durch dieses datenschutzrechtliche Instrument sollen außerdem Monopole aufgebrochen werden, sodass die Nutzer in dem einmal gewählten Dienst nicht „eingeschlossen“ werden. Die Datenportabilität soll damit sowohl die informationelle Selbstbestimmung der Bürger als auch den Wettbewerb in der digitalen Wirtschaft stärken.

Welche Unternehmen sind betroffen?

In der Entstehungsgeschichte des Rechts hatte der Gesetzgeber vor allem die großen sozialen Netzwerke vor Augen, bei denen ein Anbieterwechsel ohne Verlust eigener Daten oft nur schwer zu bewerkstelligen ist und daher nur selten vorgenommen wird.

Vom Recht des Verbrauchers auf die Datenübertragbarkeit ist jedoch jedes Unternehmen unabhängig von seiner Größe und seinem Geschäftsbereich gleichermaßen betroffen – vom Weltkonzern bis zum Start-up oder dem Friseursalon an der Ecke.



WELCHE DATEN SIND ZU ÜBERMITTELN UND WELCHE NICHT?

Zu übertragen sind:

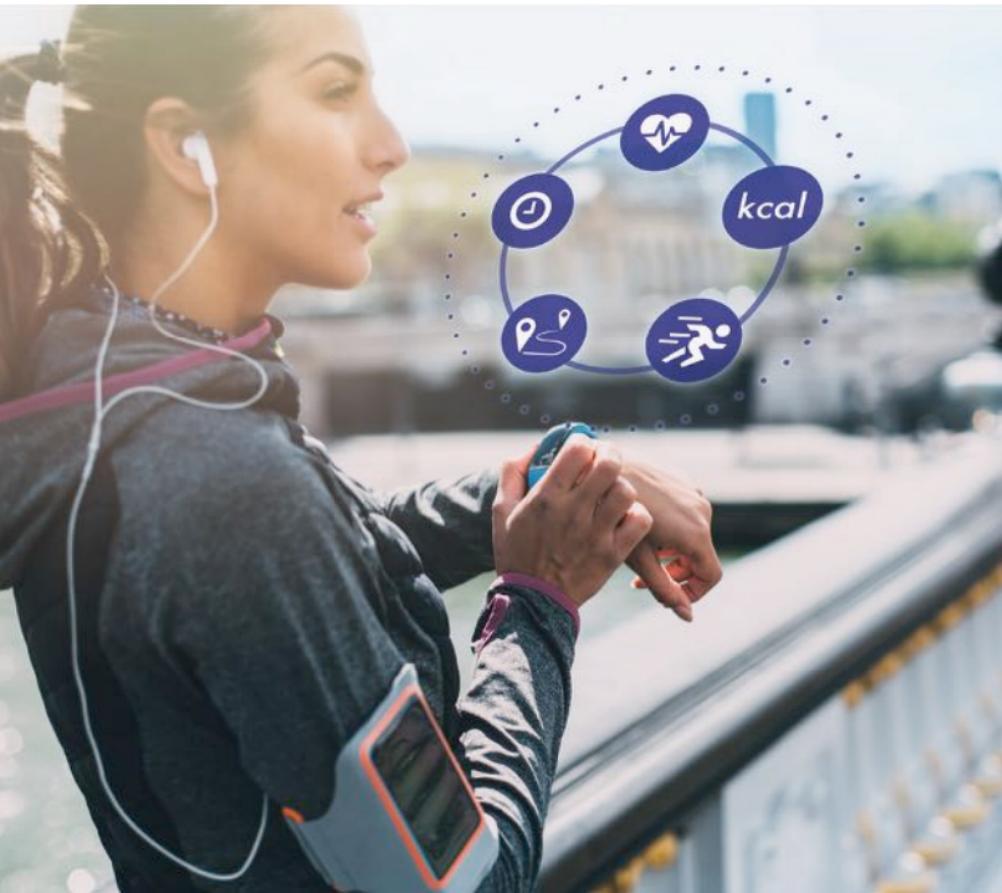
- **Direkt bereitgestellte personenbezogene Daten:**

Darunter fallen Bestandsdaten mit persönlichen Informationen über den Nutzer, die von ihm direkt bereitgestellt wurden.

Beispiel: Name, Geburtsdatum, Bild und Bankverbindung des Kunden, die im Formular eines Webshops angegeben wurden.

- **Indirekt bereitgestellte Daten:** Ebenfalls als „bereitgestellt“ gelten nach Auffassung der europäischen Datenschutzbehörden solche personenbezogenen Daten, welche vom Betroffenen durch die Nutzung eines Dienstes oder vernetzten Gerätes erzeugt und vom Anbieter beobachtet werden.

Beispiel: Individuell erstellte Playlisten bei einem Streaming-Dienst, zurückgelegte Strecken und Körperwerte bei einem Fitness-Tracker, das Fahrverhalten in einem vernetzten Auto.



Nicht übertragen werden müssen:

- „**Abgeleitete“ Daten:** Daten, welche vom Unternehmen über den Nutzer aufgrund seines Nutzungsverhalten erstellt und berechnet wurden. Da solche Datenerstellungen auf bestimmten Geschäftsmodellen und firmeninternen Algorithmen beruhen, kann deren Übertragung an Dritte möglicherweise Geschäftsheimnisse offenlegen oder geistiges Eigentum verletzen.
Beispiel: Nutzer-Bewertungen und -Profile, Informationen zur Personalisierung und Score-Werte.
- **Daten Dritter:** Daten, welche Informationen über andere Personen beinhalten und deren Übertragung daher deren informationelle Selbstbestimmung beeinträchtigen würde.
Beispiel: Die Mitnahme von Facebook-„Freunden“ zu Instagram oder Xing, Übertragung des Inhalts eines Chat zu einem anderen Messenger-Dienst.

Außerdem ist zu beachten:

- **Abgrenzung zur Auskunft:** Nicht all diejenigen Daten, die vom Auskunftsrecht (Art. 15 DSGVO) erfasst sind, fallen auch in den Anwendungsbereich des Rechts auf Datenübertragbarkeit. Dem Auskunftsrecht unterliegen auch Daten, die das Unternehmen aus anderen Quellen erlangt hat.
- **Übertragen heißt nicht Mitnehmen:** Daten, welche an den Nutzer oder neuen Anbieter übertragen werden, müssen von dem alten Anbieter nicht automatisch gelöscht werden. Der Anspruch auf Löschung muss vom Nutzer separat geltend gemacht werden.
- **Übertragenlassen heißt nicht Kündigen:** Der Antrag des Kunden auf Datenübertragbarkeit impliziert keine Kündigung eines bestehenden Vertrages (der neben einer Einwilligung die Datenspeicherung rechtfertigen kann). Wenn ein Vertrag besteht, so muss dieser vom Nutzer separat beendet werden.

WIE SOLLEN DIE DATEN ÜBERTRAGEN WERDEN?

Laut Gesetzgeber soll der Betroffene die Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“ erhalten. Außerdem sind „die Verantwortlichen dazu aufgefordert, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen“. Die betroffene Person darf alternativ verlangen, dass die Übermittlung direkt von einem Verantwortlichen zu dem anderen erfolgt, „soweit dies technisch machbar“ ist.

Im Einzelnen bedeutet das:

- „**Strukturiertes, gängiges und maschinenlesbares Format**“: Das Gesetz ist hier technologienutral und gibt keine bestimmten Formate oder Standards vor. Industrie und Wirtschaftsverbände sind aufgerufen, sich auf geeignete bestehende Formate und Standards selbst zu einigen oder neue zu entwickeln. Die Nutzung des – für den normalen Auskunftsanspruch ausreichenden – PDF-Formats, erfüllt die Bedingungen der Datenübertragbarkeit nicht.
- „**Soweit technisch machbar**“: Hierzu gibt es bislang keine objektiven Kriterien für die „Machbarkeit“. Es muss vielmehr im Einzelfall und unter der Berücksichtigung des Verhältnismäßigkeitsgrundsatzes eine Abwägung vorgenommen werden.
- **Keine Pflicht zur Annahme von Daten**: Neue Anbieter, welche auf Wunsch des Kunden die Daten von diesem selbst oder von dessen früheren Dienstanbieter erhalten sollen, sind zur Annahme oder Verarbeitung der Datensätze nicht verpflichtet.



DAS GEEIGNETE FORMAT

Sowohl für einfache als auch für komplexere Anforderungen kann auf bereits vorhandene Formate zurückgegriffen werden jedenfalls, wenn sie die Anforderungen zur Maschinenlesbarkeit und Interoperabilität erfüllen.

Hierfür ist beispielsweise das CSV-Format zu nutzen, dem eine einfache Beschreibung zur Anordnung im Datensatz hinzugefügt werden sollte.

Für umfangreichere Lösungen bieten sich XML oder JSON an. Eine Nutzung dieser bestehenden Formate erlaubt es, die zu portierenden Datensätze mittels bereits verbreiteter Standardsoftware zu verarbeiten, was die Wahrnehmung der Portabilitätsrechte insgesamt fördern und erleichtern sollte.

WAS MUSS ICH NUN KONKRET TUN?

Eine Checkliste für Ihr Unternehmen.

- **Bedarf klären:** Wie groß sind die Datenbestände, die ggf. zu übertragen sind? Mit welcher Anfrageintensität kann voraussichtlich gerechnet werden?
- **Bestand klären:** Welche von den Nutzern übertragenen personenbezogenen Daten liegen meinem Unternehmen vor? Werden von uns Nutzungsdaten gespeichert, die als „personenbezogen“ gelten können (auch bei Verwendung von Pseudonymen)?
- **Art der Speicherung klären:** Sind Datenbestände evtl. auf unterschiedlichen Servern verteilt? Können die Datenbanken für die Rohdaten so getrennt werden, dass der Datentransfer keine firmeninternen Informationen oder gar Geschäftsgeheimnisse beinhaltet?
- **Identifizierung/Authentifizierung ermöglichen:** Die Identität des anfragenden Kunden (und ggf. auch der empfangenden Stelle) ist zu überprüfen und nachweisbar sicherzustellen.



- **Weitergabeprozess definieren:** Welche Verfahren für die Datenportabilität sind für meinen Geschäftsbereich geeignet? Welche Formate kommen für mich in Frage?
- **Sichere Datenübertragung ermöglichen:** Insbesondere bei sensiblen Daten, z.B. durch standardmäßige Nutzung von Transportwegverschlüsselung.
- **Kosten analysieren:** Welche Umsetzungskosten habe ich? Wurden diese bereits in die Budgetplanung einbezogen?
- **Sich informieren:** Habe ich einen Datenschutzbeauftragten, der mir hilft? Gibt es innerhalb meiner Branche erste Lösungsansätze? Werden eventuell bereits branchenspezifische Lösungen angeboten? Gibt es ggf. Portabilitäts-Services von Drittanbietern?

Welche Bußgelder können mir drohen?

Bei Verletzung des Rechts auf Datenübertragbarkeit können Geldbußen von bis zu 20 Mio. Euro oder bis zu 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden (Art. 83 Absatz 5 DSGVO).

DIE DATENSCHUTZ-GRUNDVERORDNUNG IN KÜRZE

Ab 25. Mai 2018 gilt in der Europäischen Union ein neues Datenschutzrecht – die Europäische Datenschutz-Grundverordnung. Sie dient der Modernisierung von Regelungen zum Datenschutz und ihrer europaweiten Vereinheitlichung. Die wesentlichen Neuerungen der Grundverordnung sind:

- **Einführung des Marktortprinzips:** Das neue Datenschutzrecht gilt für alle Unternehmen, die ihre Dienstleistungen in der EU anbieten – auch für außereuropäische Unternehmen.
- **Erweiterung von Informations- und Auskunftspflichten:** Die Nutzer erhalten künftig eine größere Transparenz darüber, welche Daten über sie gesammelt und von wem sowie zu welchen Zwecken sie verarbeitet wurden.
- **Recht auf „Vergessenwerden“:** Beim Vorliegen eines berechtigten Löschungsanspruchs gegen einen Datenverarbeiter sind die Suchmaschinenbetreiber verpflichtet, Verweise und Links auf die ins Netz gestellten Daten zu löschen.
- **Recht auf Datenportabilität:** Personenbezogene Daten, die einem Datenverarbeiter vom Betroffenen bereitgestellt wurden, müssen ihm auf Wunsch wieder zur Verfügung gestellt oder an einen Drittanbieter übertragen werden.
- **Verbesserter Zugang zur Aufsicht:** Jeder hat künftig die Möglichkeit, sich an die Datenschutzbehörde vor Ort zu wenden – auch wenn die Datenverarbeitung von einem Unternehmen mit Niederlassung in einem anderen EU-Staat erfolgt.



KURZINTERVIEW: DREI FRAGEN AN FREDERICK RICHTER

Wo finde ich weitere Hilfe zum Thema?

Unsere aktuelle Studie hat gezeigt, dass wir mit der Datenportabilität absolutes Neuland betreten. Neben Ihren Datenschutzbehörden vor Ort, der Bundesbeauftragten Andrea Voßhoff oder den Verbraucherzentralen können Sie Ihre Fragen an Ihren Branchenverband adressieren.

Muss ich jede Anfrage beantworten und wie viel Zeit habe ich zur Bearbeitung?

Grundsätzlich müssen Sie alle Anfragen bearbeiten, die von Personen kommen, die Ihrem Unternehmen personenbezogene Daten mit einer Einwilligung oder im Rahmen einer vertraglichen Beziehung bereitgestellt haben. Auch für das Recht auf Datenübertragbarkeit gilt Art. 12 Absatz 3 DSGVO: Für die Antwort haben Sie einen Monat Zeit. Falls die Sache komplex ist, steht ein Vierteljahr zur Verfügung.

Wie schütze ich mich vor einer Anfrageflut und unberechtigten Ansprüchen von Dritten?

Vor einer Überflutung mit Anfragen soll Art. 12 Absatz 5 der DSGVO schützen. Danach brauchen Sie auf augenscheinlich unbegründete Anfragen nicht zu reagieren – oder Sie können (angemessene) Gebühren verlangen, was Sie bei berechtigten Portabilitätsanfragen nicht dürfen. Auf jeden Fall sollten Sie auch solche Fälle zur Sicherheit mit kurzer Begründung dokumentieren.

ÜBER DIE STIFTUNG DATENSCHUTZ

Die Stiftung Datenschutz wurde 2013 von der Bundesregierung gegründet. Aufgabe der unabhängigen Einrichtung ist die Förderung eines effizienten Privatsphärenschutzes. Die Bundesstiftung bringt als Diskussionsplattform zur Datenpolitik die unterschiedlichen Akteure in diesem Feld zusammen. Als Bindeglied zwischen Wissenschaft, Datenschutzaufsicht, Wirtschaft und Gesellschaft entwickelt sie Vorschläge für praxisgerechte Lösungen. Die Umsetzung der europäischen Datenschutzreform unterstützt die Stiftung als neutrale Informationsplattform. Im Bereich der Datenschutzzertifizierung verwaltet die Stiftung Datenschutz den Zertifizierungsstandard Trusted Cloud-Datenschutzprofil (TCDP).



Stiftung Datenschutz
Frederick Richter (V.i.S.d.P.)

Karl-Rothe-Straße 10–14
04105 Leipzig
T 0341 5861 555-0
F 0341 5861 555-9
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

gefördert durch das



Bundesministerium
des Innern