16/DE
WP 242 rev.01

Leitlinien zum Recht auf Datenübertragbarkeit

angenommen am 13. Dezember 2016
zuletzt überarbeitet und angenommen am 5. April 2017

INHALTSVERZEICHNIS

Zusammenfassung

Durch Artikel 20 der DSGVO wird ein neues Recht auf Datenübertragbarkeit begründet, das mit dem Auskunftsrecht zwar eng verbunden ist, sich aber dennoch davon in vielerlei Hinsicht unterscheidet. Betroffene Personen sind demnach berechtigt, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten einem anderen Verantwortlichen zu übermitteln. Ziel dieses neuen Rechts ist es, die betroffene Person mit einer entsprechenden Befugnis auszustatten und ihr mehr Kontrolle über die sie betreffenden personenbezogenen Daten zu geben.

Da es die direkte Übermittlung personenbezogener Daten von einem Verantwortlichen an einen anderen ermöglicht, ist das Recht auf Datenübertragbarkeit auch ein wichtiges Werkzeug zur Unterstützung des freien Verkehrs personenbezogener Daten in der EU und zur Förderung des Wettbewerbs zwischen Verantwortlichen. Es erleichtert den Wechsel zwischen verschiedenen Dienstanbietern und wird daher die Entwicklung neuer Dienste im Kontext der Strategie für einen digitalen Binnenmarkt fördern.

Diese Stellungnahme dient als Orientierungshilfe für die Auslegung und Umsetzung des Rechts auf Datenübertragbarkeit, das durch die DSGVO eingeführt wurde. Sie soll das Recht auf Datenübertragbarkeit und seinen Anwendungsbereich erörtern. Es werden die Bedingungen geklärt, unter denen dieses neue Recht Anwendung findet, und zwar unter Berücksichtigung der Rechtsgrundlage für die Datenverarbeitung (entweder die Einwilligung der betroffenen Person oder die Erfordernis einer Vertragserfüllung) und der Tatsache, dass dieses Recht auf personenbezogene Daten beschränkt ist, die von der betroffenen Person bereitgestellt werden. Die Stellungnahme enthält zudem konkrete Beispiele und Kriterien, die veranschaulichen sollen, unter welchen Umständen dieses Recht gilt. Diesbezüglich ist die Datenschutzgruppe der Auffassung, dass sich das Recht auf Datenübertragbarkeit auf Daten erstreckt, die wissentlich und aktiv von der betroffenen Person bereitgestellt werden, sowie auf die personenbezogenen Daten, die durch ihre Aktivitäten erzeugt werden. Diese neue Recht darf nicht dadurch unterlaufen werden, dass es lediglich auf personenbezogene Daten angewendet wird, die die betroffene Person direkt (z. B. per Online-Formular) mitteilt.

Als bewährtes Verfahren sollten Verantwortliche Mittel zur Beantwortung von Anfragen zur Datenübertragbarkeit entwickeln (z.B. Download-Tools und Anwendungsprogrammierschnittstellen). Sie sollten gewährleisten, dass die personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format übermittelt werden, und sie sollten angehalten werden, die Interoperabilität des in Beantwortung einer Anfrage zur Datenübertragbarkeit bereitgestellten Datenformats sicherzustellen.

Die Stellungnahme enthält zudem erläuternde Ausführungen zu den Pflichten der Verantwortlichen sowie Empfehlungen für bewährte Verfahren und Tools, die die Einhaltung des Rechts auf Datenübertragbarkeit erleichtern. Abschließend wird in der Stellungnahme empfohlen, dass Branchenvertreter und Fachverbände auf der Grundlage gemeinsamer interoperabler Standards und Formate zusammenarbeiten sollten, um die Anforderungen des Rechts auf Datenübertragbarkeit zu erfüllen.

I. Einführung

Mit Artikel 20 der Datenschutz-Grundverordnung (DSGVO) wird das neue Recht auf Datenübertragbarkeit eingeführt. Betroffene Personen erhalten dadurch das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen zur Verfügung gestellt haben, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und diese Daten ohne Behinderung einem anderen Verantwortlichen zu übermitteln. Dieses Recht, das vorbehaltlich bestimmter Voraussetzungen gilt, fördert die Wahl- und Kontrollmöglichkeiten der Nutzer und die Selbstbestimmung der Verbraucher.

Personen, die von ihrem Auskunftsrecht gemäß der Datenschutzrichtlinie 95/46/EG Gebrauch machten, waren an das Format gebunden, das der Verantwortliche bei der Bereitstellung der angeforderten Daten vorgab. **Durch das neue Recht auf Datenübertragbarkeit soll betroffenen Personen größere Kontrolle über ihre personenbezogenen Daten gegeben werden, indem es ihnen einfacher gemacht wird, Daten ohne Weiteres von einer IT-Umgebung in eine andere zu verschieben, zu kopieren oder zu übertragen** - und dies unabhängig davon, ob es sich um ihre eigenen Systeme, die Systeme vertrauenswürdiger Dritter oder die Systeme neuer Verantwortlicher handelt.

Durch die Stärkung der Rechte und der Kontrolle des Einzelnen über seine personenbezogenen Daten eröffnet die Datenübertragbarkeit Möglichkeiten für ein neues Ausbalancieren des Verhältnisses zwischen betroffenen Personen und Verantwortlichen[1].

Das Recht auf Datenübertragbarkeit kann dem Wettbewerb unter den Anbietern förderlich sein, weil es den Anbieterwechsel vereinfacht. Dennoch ist die DSGVO kein Instrument zur Regulierung des Wettbewerbs, sondern zur Regulierung des Umgangs mit personenbezogenen Daten. So sieht Artikel 20 beispielsweise keine Begrenzung der Übertragbarkeit auf Daten vor, die für den Anbieterwechsel notwendig oder nützlich sind[2].

Auch wenn es sich bei der Datenübertragbarkeit um ein neues Recht handelt, gibt es sie bereits in anderer Form bzw. ist sie bereits Thema in anderen Bereichen der Rechtsetzung (z. B. im Zusammenhang mit der Beendigung eines Vertrags, beim Roaming von Kommunikationsdiensten oder beim grenzüberschreitenden Zugang zu Diensten)[3]. Aus diesen verschiedenen Formen der Übertragbarkeit könnten sich bei einer ganzheitlichen Herangehensweise gewisse Synergien und sogar Vorteile für den Einzelnen ergeben, auch wenn bei etwaigen Analogien Vorsicht geboten ist.

Diese Stellungnahme dient als Orientierungshilfe für Verantwortliche, damit diese ihre Praktiken, Prozesse und Richtlinien aktualisieren können, und klärt die Bedeutung von „Datenübertragbarkeit“, um betroffenen Personen die effiziente Nutzung ihres neuen Rechts zu ermöglichen.

---

[1] Vorrangiges Ziel der Datenübertragbarkeit ist die größere Kontrolle des Einzelnen über seine personenbezogenen Daten und seine aktive Mitwirkung im Daten-Ökosystem.

[2] Dieses Recht ermöglicht beispielsweise Banken, zusätzliche, der Kontrolle durch den Nutzer unterliegende Dienstleistungen anzubieten, bei denen auf personenbezogene Daten zurückgegriffen wird, welche ursprünglich im Rahmen einer Energieversorgungsdienstleistung erhoben wurden.

[3] Siehe Agenda für einen digitalen Binnenmarkt der Europäischen Kommission: https://ec.europa.eu/digital-agenda/en/digital-single-market, insbesondere die erste Säule der Strategie „Besserer Online-Zugang zu digitalen Waren und Dienstleistungen“.

II. Was sind die wesentlichen Elemente der Datenübertragbarkeit?

Das Recht auf Datenübertragbarkeit wird in Artikel 20 Absatz 1 der DSGVO wie folgt definiert:

> *Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln (...)*

- **Das Recht, personenbezogene Daten zu erhalten**

Zum einen gibt die Datenübertragbarkeit betroffenen Personen **das Recht, Teilsätze ihrer personenbezogener Daten zu erhalten**, die ein für sie zuständiger Verantwortlicher verarbeitet hat, und diese Daten zur weiteren persönlichen Verwendung zu speichern. Die Speicherung kann auf einem privaten Datenträger oder in einer privaten Cloud erfolgen und muss nicht unbedingt per Datenübermittlung an einen anderen Verantwortlichen erfolgen.

In diesem Sinne ergänzt die Datenübertragbarkeit das Auskunftsrecht. Eine Besonderheit der Datenübertragbarkeit liegt in der Tatsache begründet, dass sie betroffenen Personen eine einfache Möglichkeit zur eigenen Verwaltung und Wiederverwendung personenbezogener Daten bietet. Diese Daten sollten „*in einem strukturierten, gängigen und maschinenlesbaren Format*“ empfangen werden. So könnte eine betroffene Person beispielsweise Interesse daran haben, ihre aktuelle Wiedergabeliste (oder eine Verlaufsliste aller von ihr angehörten Musikstücke) bei einem Musik-Streaming-Dienst abzurufen, um in Erfahrung zu bringen, wie oft sie bestimmte Musikstücke angehört hat, oder um zu sehen, welche Musik sie auf einer anderen Plattform kaufen könnte. Außerdem möchte sie vielleicht die Kontakte aus ihrer Webmail-Anwendung abrufen, um eine Gästeliste für eine Hochzeit zu erstellen, oder sie möchte Informationen über Einkäufe mit verschiedenen Kundenkarten erhalten, um ihre individuelle CO_2-Bilanz zu überprüfen[4].

- **Recht zur Übermittlung personenbezogener Daten von einem Verantwortlichen an einen anderen**

Zum anderen überträgt Artikel 20 Absatz 1 betroffenen Personen das **Recht zur Übermittlung personenbezogener Daten von einem Verantwortlichen an einen anderen Verantwortlichen** „ohne Behinderung“. Zudem können auf Anfrage der betroffenen Personen deren personenbezogene Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist (Artikel 20 Absatz 2). Diesbezüglich sieht Erwägungsgrund 68 vor, dass die Verantwortlichen interoperable Formate entwickeln sollten, die die Datenübertragbarkeit ermöglichen[5], wobei die

[4] In derartigen Fällen gilt die von der betroffenen Person durchgeführte Datenverarbeitung als Haushaltstätigkeit, wenn die gesamte Verarbeitung unter ihrer alleinigen Kontrolle erfolgt; die Datenverarbeitung kann aber auch im Auftrag der betroffenen Person von einer anderen Partei durchgeführt werden. Im letztgenannten Fall gilt die andere Partei auch dann als Verantwortlicher, wenn lediglich eine Speicherung der Daten vorgenommen wird. Sie muss daher die in der DSGVO niedergelegten Grundsätze und Pflichten einhalten.

[5] Siehe auch Abschnitt V.

Verantwortlichen jedoch nicht verpflichtet werden sollten, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten[6]. Die DSGVO verbietet Verantwortlichen, die Übermittlung zu behindern.

Im Wesentlichen ermöglicht die Datenübertragbarkeit betroffenen Personen, die von ihnen bereitgestellten Daten nicht nur zu erhalten und wiederzuverwenden, sondern auch an einen anderen Diensteanbieter (derselben oder einer anderen Branche) zu übermitteln. Abgesehen davon, dass durch die Verhinderung des „Lock-in-Effekts" die Selbstbestimmung der Verbraucher gestärkt wird, besteht auch die Erwartung, dass durch das Recht auf Datenübertragbarkeit Innovationsmöglichkeiten und ein sicherer Austausch personenbezogener Daten zwischen Verantwortlichen unter der Kontrolle der betroffenen Person gefördert werden[7]. Die Datenübertragbarkeit kann den kontrollierten und begrenzten Austausch personenbezogener Daten zwischen Nutzern personenbezogener Daten in Organisationen begünstigen und so das Dienstleistungsangebot und die Kundenerfahrung bereichern[8]. Sie kann ferner die Übermittlung und die Wiederverwendung der personenbezogenen Daten von betroffenen Personen zwischen den für sie interessanten Diensten vereinfachen.

- **Kontrolle**

Durch das Recht auf Datenübertragbarkeit wird sichergestellt, dass betroffene Personen sie betreffende personenbezogene Daten empfangen und nach ihrem Belieben verarbeiten können[9].

Verantwortliche, die unter den Voraussetzungen gemäß Artikel 20 Anfragen zur Datenübertragbarkeit beantworten, haften nicht für die Verarbeitung, die durch die betroffene Person oder ein anderes Unternehmen erfolgt, das personenbezogene Daten erhält. Sie handeln jeweils im Namen der betroffenen Person; dies gilt auch für die direkte Übermittlung der personenbezogenen Daten an einen anderen Verantwortlichen. Dabei haftet der Verantwortliche nicht dafür, dass sich der die Daten empfangende Verantwortliche an die Datenschutzvorschriften hält, denn letzterer wird ja nicht von ihm selbst ausgewählt, sondern von der betroffenen Person. Nichtsdestotrotz sollte der Verantwortliche bestimmte Sicherheitsvorkehrungen treffen, durch die sichergestellt wird, dass er tatsächlich im Sinne der betroffenen Person vorgeht. Beispielsweise kann er durch geeignete Verfahren sicherstellen, dass wirklich nur diejenigen personenbezogenen Daten übermittelt werden, die die betroffene Person übermitteln möchte. Zu diesem Zweck kann er beispielsweise vor der Übermittlung oder bereits bei der ursprünglichen Zustimmung zur Datenverarbeitung bzw. beim Vertragsabschluss von der betroffenen Person eine entsprechende Bestätigung einholen.

---

[6] Daher sollte dem Format, in dem die Daten übertragen werden, besondere Beachtung geschenkt werden, denn es muss gewährleistet sein, dass die Daten von der betroffenen Person oder von einem anderen Verantwortlichen mit geringem Aufwand wiederverwendet werden können. Siehe auch Abschnitt V.

[7] Siehe mehrere versuchsweise Anwendungen in Europa, z. B. MiData im Vereinigten Königreich, MesInfos/SelfData durch FING in Frankreich.

[8] Bei den in den Bereichen „Quantified Self" und „Internet of Things (IoT)" tätigen Branchen hat sich gezeigt, welche Vorteile (und Risiken) sich aus der Vernetzung personenbezogener Daten zu verschiedenen Aspekten des individuellen Lebens (z. B. körperliche Fitness, Aktivität und Kalorienaufnahme) ergeben, bei denen es darum geht, ein möglichst umfassendes Gesamtbild des Lebens eines Einzelnen in einer einzigen Datei zu erhalten.

[9] Das Recht auf Datenübertragbarkeit ist nicht auf personenbezogene Daten begrenzt, die nützlich und relevant für ähnliche, von Mitbewerbern des Verantwortlichen angebotene Dienste sind.

Verantwortliche, die einer Portabilitätsanfrage nachkommen, unterliegen keiner spezifischen Pflicht zur Überprüfung der Datenqualität vor der Datenübermittlung. Selbstverständlich sollten derartige Daten stets sachlich richtig und auf dem neuesten Stand sein, wie es Artikel 5 Absatz 1 der DSGVO vorsieht. Durch das Recht auf Datenübertragbarkeit wird der Verantwortliche auch nicht verpflichtet, personenbezogene Daten länger als notwendig oder über einen etwaigen angegebenen Aufbewahrungszeitraum hinaus zu speichern[10]. Zudem ist er keineswegs verpflichtet, Daten über die ansonsten geltenden Vorhaltezeiten hinaus zu speichern, um etwaigen künftigen Portabilitätsanfragen nachkommen zu können.

Falls die angeforderten personenbezogenen Daten von einem Auftragsverarbeiter verarbeitet werden, muss der Vertrag nach Artikel 28 der DSGVO die Pflicht einschließen, dass der Auftragsverarbeiter den Verantwortlichen „nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der (...) Rechte der betroffenen Person nachzukommen". Daher sollte der Verantwortliche in Zusammenarbeit mit seinem Auftragsverarbeiter spezielle Verfahren zur Erledigung von Portabilitätsanfragen anwenden. Im Fall einer geteilten Kontrolle sollte die Aufteilung der Verantwortlichkeiten in Bezug auf die Verarbeitung von Portabilitätsanfragen auf die einzelnen Verantwortlichen mittels Vertrag klar geregelt werden.

Auch muss ein Verantwortlicher, der Daten erhält,[11] sicherstellen, dass die bereitgestellten portablen Daten für die neue Datenverarbeitung relevant und nicht exzessiv sind. Richtet beispielsweise eine betroffene Person eine Portabilitätsanfrage an einen Webmail-Dienst, um E-Mails abzurufen und diese an eine sichere Speicherplattform zu übermitteln, so ist es nicht erforderlich, dass der betreffende neue Verantwortliche die Kontaktdaten der Adressaten der Mails der betroffenen Person verarbeitet. Sind diese Daten für den Zweck der neuen Verarbeitung nicht erheblich, sollten sie nicht gespeichert und nicht verarbeitet werden. In jedem Fall sind Verantwortliche, die Daten erhalten, nicht verpflichtet, aufgrund einer Portabilitätsanfrage übermittelte Daten entgegenzunehmen und zu verarbeiten. Ebenso wenig muss in Fällen, in denen eine betroffene Person eine Anfrage zur Übermittlung von Einzelheiten ihrer Banktransaktionen an einen sie bei der Verwaltung ihrer Finanzen unterstützenden Dienst stellt, der Verantwortliche, dem die Daten übermittelt werden, nicht sämtliche Daten entgegennehmen oder sämtliche Einzelheiten der Transaktionen speichern, nachdem diese für diese Zwecke des neuen Dienstes markiert worden sind. Anders ausgedrückt: Es sollten ausschließlich solche Daten entgegengenommen und gespeichert werden, die erforderlich und erheblich für die Erbringung des betreffenden Dienstes durch den Verantwortlichen, der die Daten erhält, sind.

Eine Organisation, die Daten erhält, wird zu einem neuen Verantwortlichen für diese personenbezogenen Daten und ist verpflichtet, die in Artikel 5 der DSGVO genannten Grundsätze einhalten. Der „neue" Verantwortliche muss daher gemäß den in Artikel 14 niedergelegten Transparenzanforderungen[12] vor jeder Anfrage zur Übermittlung der portablen

[10] Wenn der Verantwortliche also im oben genannten Beispiel kein Verzeichnis der von einem Nutzer angehörten Lieder führt, so können diese personenbezogenen Daten auch nicht Gegenstand einer Anfrage zur Datenübertragbarkeit sein.

[11] D. h. ein Verantwortlicher, der personenbezogene Daten aufgrund einer Anfrage der betroffenen Person auf Übertragung der Daten an einen anderen Verantwortlichen erhält.

[12] Darüber hinaus sollte der neue Verantwortliche keine personenbezogenen Daten verarbeiten, die nicht erheblich sind, und die Verarbeitung ist auf die Daten zu beschränken, die für die neuen Zwecke erforderlich sind, auch wenn die personenbezogenen Daten Teil eines umfassenderen Datensatzes sind, der im Rahmen eines

Daten eindeutig und direkt angeben, zu welchem Zweck die neue Verarbeitung erfolgen soll. Bei allen sonstigen unter seiner Verantwortung durchgeführten Datenverarbeitungen sollte der Verantwortliche nach den in Artikel 5 niedergelegten Grundsätzen (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit und Rechenschaftspflicht[13]) verfahren.

Verantwortliche, die personenbezogene Daten besitzen, müssen in der Lage sein, ihren betroffenen Personen den Rückgriff auf ihr Recht auf Datenübertragbarkeit zu vereinfachen. Verantwortliche können Daten von betroffenen Personen entgegennehmen, sind dazu jedoch nicht verpflichtet.

- **Das Recht auf Datenübertragbarkeit gegenüber anderen Rechten betroffener Personen**

Macht jemand von seinem Recht auf Datenübertragbarkeit (oder einem anderen in der DSGVO verankerten Recht) Gebrauch, so tut er dies unbeschadet anderer Rechte. Eine betroffene Person kann die Dienste eines Verantwortlichen auch nach einem Datenübertragbarkeitsvorgang weiterhin nutzen und in Anspruch nehmen. Ein Datenübertragbarkeitsvorgang zieht nicht automatisch die Löschung der Daten aus den Systemen des Verantwortlichen nach sich[14] und wirkt sich auch nicht auf die ursprüngliche Speicherfrist für die übermittelten Daten aus. Die betroffene Person kann von ihren Rechten Gebrauch machen, so lange der Verantwortliche die Daten verarbeitet.

Ebenso kann die Datenübertragbarkeit, sofern die betroffene Person von ihrem Recht auf Löschung („Recht auf Vergessenwerden“ nach Artikel 17) Gebrauch machen möchte, von einem Verantwortlichen nicht als Mittel zur Verzögerung oder Verweigerung einer solchen Löschung verwendet werden.

Sollte eine betroffene Person feststellen, dass gemäß dem Recht auf Datenübertragbarkeit angeforderte personenbezogene Daten nicht in vollem Umfang ihrer Anfrage entsprechen, so ist jeder weiteren Anforderung personenbezogener Daten gemäß dem Auskunftsrecht des Artikels 15 der DSGVO in vollem Umfang nachzukommen.

Des Weiteren sind bei der Bearbeitung von Portabilitätsanfragen nach der DSGVO in Fällen, in denen eine einschlägige Rechtsvorschrift auf einem anderen Gebiet des Unionsrechts oder des Rechts der Mitgliedstaaten die Übertragbarkeit der betroffenen Daten vorsieht, auch die in diesen einschlägigen Rechtsvorschriften vorgesehenen Bedingungen zu berücksichtigen. Falls aus der Anfrage eindeutig hervorgeht, dass die betroffene Person nicht von ihren in der DSGVO niedergelegten Rechten, sondern ausschließlich von ihren in sektorspezifischen Rechtsvorschriften verankerten Rechten Gebrauch machen möchte, sind die

---

Übertragbarkeitsvorgangs übermittelt wird. Personenbezogene Daten, die für das Erreichen des Zwecks der neuen Verarbeitung nicht erforderlich sind, sollten so bald wie möglich gelöscht werden.

[13] Personenbezogene Daten, die gemäß dem Recht auf Datenübertragbarkeit übermittelt werden, können nach ihrem Eingang bei dem Verantwortlichen als von der betroffenen Person „bereitgestellt“ betrachtet werden und dürfen in Übereinstimmung mit dem Recht auf Datenübertragbarkeit weiterübermittelt werden, sofern die anderen mit diesem Recht verbundenen Bedingungen (u.a. in Bezug auf die Rechtsgrundlage der Verarbeitung) erfüllt sind.

[14] Siehe Artikel 17 der DSGVO.

Datenübertragbarkeitsbestimmungen der DSGVO auf diese Anfrage nicht anwendbar[15]. Falls sich die Anfrage hingegen auf Datenportabilität nach der DSGVO bezieht, wird die allgemeine Anwendung des Datenübertragbarkeitsgrundsatzes der DSGVO auf jeden Verantwortlichen durch die bloße Existenz dieser sektorspezifischen Vorschriften nicht berührt. Allerdings ist von Fall zu Fall zu prüfen, ob und wie sich diese sektorspezifischen Vorschriften auf das Recht auf Datenübertragbarkeit auswirken können.

III. Wann gilt das Recht auf Datenübertragbarkeit?

- **Welche Verarbeitungsvorgänge werden vom Recht auf Datenübertragbarkeit erfasst?**

Gemäß der DSGVO müssen Verantwortliche über eine eindeutige Rechtsgrundlage für die Verarbeitung personenbezogener Daten verfügen.

Nach Artikel 20 Absatz 1 Buchstabe a der DSGVO müssen Verarbeitungsvorgänge, **um in den Anwendungsbereich des Rechts auf Datenübertragbarkeit zu fallen**, auf Folgendem beruhen:

- auf der Einwilligung der betroffenen Person (gemäß Artikel 6 Absatz 1 Buchstabe a oder gemäß Artikel 9 Absatz 2 Buchstabe a, sofern es sich um besondere Kategorien personenbezogener Daten handelt)

- oder auf einem Vertrag, dessen Vertragspartei die betroffene Person gemäß Artikel 6 Absatz 1 Buchstabe b ist.

Buchtitel, die eine Person in einer Online-Buchhandlung gekauft hat, oder über einen Musik-Streaming-Dienst angehörte Musikstücke sind weitere Beispiele für personenbezogene Daten, die generell in den Anwendungsbereich des Rechts auf Datenübertragbarkeit fallen, da sie auf der Grundlage eines Vertrags verarbeitet werden, dessen Vertragspartei die betroffene Person ist.

Die DSGVO begründet kein allgemeines Recht auf Datenübertragbarkeit in Fällen, in denen die Verarbeitung personenbezogener Daten nicht aufgrund einer Einwilligung oder eines Vertrags erfolgt[16]. Beispielsweise sind Finanzeinrichtungen nicht verpflichtet,

[15] Stellt die Anfrage einer betroffenen Person beispielsweise speziell darauf ab, einem Kontoinformationsdienstleister zu den in der zweiten Zahlungsdiensterichtlinie vorgesehenen Zwecken Zugang zu ihrem Bankkontoverlauf zu erteilen, so sollte dieser Zugang nach Maßgabe dieser Richtlinie erteilt werden.

[16] Siehe Erwägungsgrund 68 und Artikel 20 Absatz 3 der DSGVO. In Artikel 20 Absatz 3 und in Erwägungsgrund 68 ist vorgesehen, dass das Recht auf Datenübertragbarkeit keine Anwendung findet, wenn die Datenverarbeitung zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung einer dem Verantwortlichen übertragenen öffentlicher Gewalt erfolgt, oder wenn ein Verantwortlicher in Erfüllung seiner öffentlichen Aufgaben oder einer rechtlichen Pflicht handelt. Es besteht für Verantwortliche daher keine Verpflichtung, in solchen Fällen die Übertragbarkeit zu gewährleisten. Es ist jedoch bewährte Praxis, Prozesse zur automatischen Beantwortung von Portabilitätsanfragen zu entwickeln, die den in Bezug auf das Recht auf Datenübertragbarkeit geltenden Grundsätzen folgen. Ein Beispiel hierfür wäre ein Behördendienst, der die Möglichkeit für das einfache Herunterladen früherer persönlicher Einkommensteuererklärungen bietet. Bezüglich der Datenübertragbarkeit als bewährter Praxis im Falle der Verarbeitung auf Basis des Rechtsgrunds der Notwendigkeit eines berechtigten Interesses und bestehender freiwilliger Programme siehe Seite 47 und 48 der Stellungnahme Nr. 6/2014 der Datenschutzgruppe bezüglich berechtigter Interessen (WP217).

Portabilitätsanfragen nachzukommen, die sich auf personenbezogene Daten beziehen, welche im Rahmen ihrer Pflicht zur Verhütung und Aufdeckung von Geldwäsche und anderen Formen der Finanzkriminalität verarbeitet wurden. Ebenso erstreckt sich das Recht auf Datenübertragbarkeit nicht auf berufliche Kontaktdaten, die im Rahmen einer Geschäftsbeziehung zwischen Unternehmen verarbeitet werden und bei denen die Verarbeitung nicht mit Einverständnis der betroffenen Person oder auf Grundlage eines Vertrags, dessen Partei diese Person ist, erfolgt.

In Bezug auf die Daten von Arbeitnehmern ist das Recht auf Datenübertragbarkeit normalerweise nur anwendbar, wenn die Datenverarbeitung auf der Grundlage eines Vertrags erfolgt, dessen Partei die betroffene Person ist. In viele Fällen wird davon ausgegangen, dass wegen des unausgewogenen Kräfteverhältnisses zwischen Arbeitgeber und Arbeitnehmer in diesem Zusammenhang keine freiwillige Zustimmung vorliegt[17]. Bestimmte Verarbeitungen von Personaldaten erfolgen gleichwohl auf Basis des Rechtsgrunds des legitimen Interesses oder sind für die Einhaltung einschlägiger rechtlicher Pflichten des Arbeitgebers erforderlich. In der Praxis berührt das Recht auf Datenübertragbarkeit zweifelsohne bestimmte Datenverarbeitungsvorgänge (beispielsweise im Zusammenhang mit Zahlungs- und Entschädigungsdiensten oder internen Einstellungen), doch in vielen anderen Situationen ist je nach Fall zu prüfen, ob sämtliche Bedingungen für die Anwendung des Rechts auf Datenübertragbarkeit erfüllt sind.

Auch gilt das Recht auf Datenübertragbarkeit nur dann, wenn die Datenverarbeitung „mit automatischen Mitteln erfolgt“; es erstreckt sich folglich nicht auf die meisten Dokumente in Papierform.

- **Welche personenbezogenen Daten sind einzubeziehen?**

Gemäß Artikel 20 Absatz 1 müssen Daten, um in den Anwendungsbereich des Rechts auf Datenübertragbarkeit zu fallen,

- personenbezogene Daten sein, die die betroffene Person selbst betreffen, und
- von der betroffenen Person einem Verantwortlichen *bereitgestellt* worden sein.

In Artikel 20 Absatz 4 wird außerdem ausgeführt, dass die Rechte und Freiheiten anderer Personen nicht durch die Einhaltung dieses Rechts beeinträchtigt werden dürfen.

Erste Bedingung: personenbezogene Daten, die die betroffene Person betreffen

Eine Portabilitätsanfrage kann sich ausschließlich auf personenbezogene Daten beziehen. Daten, die anonym sind[18] oder die betroffene Person nicht betreffen, kommen folglich nicht in Frage. Gleichwohl fallen pseudonymisierte Daten, die eindeutig mit der betroffenen Person in Zusammenhang gebracht werden können (z. B. indem diese die entsprechenden Informationen bereitstellt, die ihre Identifizierung ermöglichen, vgl. Artikel 11 Absatz 2), sehr wohl in den Anwendungsbereich.

In vielen Fällen verarbeiten Verantwortliche Daten, die die personenbezogenen Daten mehrerer betroffener Personen enthalten. In derartigen Fällen sollten Verantwortliche die Formulierung „der sie betreffenden personenbezogenen Daten“ nicht zu restriktiv auslegen.

[17] Siehe Stellungnahme Nr. 8/2001 der Datenschutzgruppe vom 13. September 2001 (WP48).
[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

In practice, the right to data portability in an HR context will undoubtedly concern someprocessing operations (such as pay and compensation services, internal recruitment)

So kann z.B. der Kontoverlauf eines Kunden zu dessen Telefongesprächen, per Nachrichtensystem übermittelten Nachrichten oder VoIP-Anrufen Angaben über Dritte enthalten, die an den ein- und abgehenden Anrufen beteiligt waren. Auch wenn in den betreffenden Aufzeichnungen mithin personenbezogene Daten mehrerer Personen erfasst sind, sollten die betreffenden Kunden die Möglichkeit haben, dass ihnen diese Aufzeichnungen im Rahmen einer Portabilitätsanfrage bereitgestellt werden. Wenn solche Aufzeichnungen dann allerdings an einen neuen Verantwortlichen übermittelt werden, sollte dieser neue Verantwortliche die Aufzeichnungen nicht für Zwecke verarbeiten, die die Rechte und Freiheiten der anderen Personen beeinträchtigen (siehe die dritte Bedingung).

Zweite Bedingung: Daten, die von der betroffenen Person bereitgestellt wurden

Durch die zweite Bedingung wird der Umfang der von der betroffenen Person „bereitgestellten" Daten eingeschränkt.

Es gibt viele Arten personenbezogener Daten, die wissentlich und aktiv von der betroffenen Person „bereitgestellt" werden, so beispielsweise Kontodaten (z. B. Postanschrift, Nutzername, Alter), die über Online-Formulare übermittelt werden. Allerdings sind manche von einer betroffenen Person „bereitgestellte" Daten auch das Ergebnis der Beobachtung ihrer Tätigkeit. Damit das neue Recht auf Datenübertragbarkeit seine volle Wirkung entfalten kann, sollten daher nach Auffassung der Datenschutzgruppe auch solche Daten, die aus der Beobachtung der Tätigkeiten eines Nutzers resultieren, unter die „bereitgestellten" Daten fallen - also beispielsweise Rohdaten, die in einem intelligenten Messgerät oder von anderen miteinander vernetzten Geräten[19], in Tätigkeitsprotokollen oder in Webseiten- bzw. Suchverläufen verarbeitet werden.

Zu dieser letztgenannten Datenkategorie zählen jedoch keine Daten, die der Verantwortliche (unter Verwendung erfasster oder direkt eingegebener Daten) erzeugt, beispielsweise ein Nutzerprofil auf Basis einer Analyse von mithilfe eines intelligenten Zählers erfassten Rohdaten.

Um zu entscheiden, ob sie unter das Recht auf Datenübertragbarkeit fallen, kann eine Unterscheidung zwischen verschiedenen Kategorien von Daten aufgrund ihrer Herkunft vorgenommen werden. Die folgenden Datenkategorien können als „von der betroffenen Person bereitgestellt" betrachtet werden:

- **aktiv und wissentlich von der betroffenen Person bereitgestellte Daten** (z.B. Postanschrift, Nutzername, Alter)
- **beobachtete Daten, die von der betroffenen Person durch die Nutzung des Dienstes oder des Geräts bereitgestellt werden** (z.B. Suchverlauf, Verkehrsdaten und Standortdaten, ebenso andere Rohdaten wie die von einem Trackinggerät aufgezeichnete Herzfrequenz);

im Gegensatz dazu werden aus Rückschlüssen erzeugte und abgeleitete Daten vom Verantwortlichen auf der Grundlage der „von der betroffenen Person bereitgestellten Daten" erzeugt. Beispielsweise können die Ergebnisse einer Bewertung des Gesundheitszustands

[19] Dank der Möglichkeit zur Abfrage der aus der Beobachtung ihrer Tätigkeit resultierenden Daten ist es der betroffenen Person auch möglich, sich ein besseres Bild der vom Verantwortlichen auf der Grundlage der erfassten Daten durchgeführten Anwendungen zu machen, sie kann somit besser entscheiden, welche Daten sie einem ähnlichen Dienst bereitstellen würde, und sie kann sich auf diese Weise einen Überblick darüber verschaffen, inwieweit ihr Recht auf Privatsphäre gewahrt bleibt.

eines Nutzers oder ein Risikoprofil, das im Zusammenhang mit dem Risikomanagement und Finanzvorschriften (beispielsweise zwecks Bonitätsbewertung oder zur Einhaltung von Geldwäschevorschriften) erstellt wurde, als solche nicht als von der betroffenen Person „bereitgestellt" betrachtet werden. Auch wenn solche Daten möglicherweise Teil eines Profils sind, das von einem Verantwortlichen gespeichert und anhand einer Analyse von Daten, die von der betroffenen Person (z.B. durch ihre Aktivitäten) bereitgestellt werden, aus Rückschlüssen erzeugt und abgeleitet wird, gelten diese Daten in der Regel nicht als „von der betroffenen Person bereitgestellt" und fallen daher nicht in den Anwendungsbereich dieses neuen Rechts[20].

Im Allgemeinen ist die Formulierung „von der betroffenen Person bereitgestellt" wegen der politischen Ziele des Rechts auf Datenübertragbarkeit weit auszulegen; ausgeschlossen werden sollten lediglich „aus Rückschlüssen erzeugte Daten" und „abgeleitete Daten", die personenbezogene Daten beinhalten, welche von einem Diensteanbieter erzeugt werden (z.B. algorithmische Ergebnisse). Ein Verantwortlicher kann diese aus Rückschlüssen erzeugten Daten ausschließen, sollte jedoch alle sonstigen personenbezogenen Daten berücksichtigen, die von der betroffenen Person durch technische Mittel bereitgestellt werden, die der Verantwortliche zur Verfügung stellt[21].

Daher schließt die Formulierung „bereitgestellt durch" auch personenbezogene Daten ein, die sich auf die Aktivität der betroffenen Person beziehen oder das Ergebnis einer Beobachtung des Verhaltens einer Person (jedoch nicht einer nachfolgenden Analyse dieses Verhaltens) sind. Im Gegensatz dazu gelten personenbezogene Daten, die vom Verantwortlichen im Rahmen der Datenverarbeitung (z.B. durch einen Personalisierungs- oder Empfehlungsprozess), durch Nutzerkategorisierung oder durch Profiling erzeugt werden, als Daten, die von den von der betroffenen Person bereitgestellten personenbezogenen Daten abgeleitet oder aus Rückschlüssen erzeugt wurden, und fallen folglich nicht unter das Recht auf Datenübertragbarkeit.

<u>Dritte Bedingung: keine Beeinträchtigung der Rechte und Freiheiten anderer Personen</u>

Bezüglich personenbezogener Daten, die andere betroffene Personen betreffen, gilt:

Durch die dritte Bedingung soll vermieden werden, dass Daten, die personenbezogene Daten anderer Personen (welche keine Einwilligung erteilt haben) enthalten, abgerufen und an einen neuen Verantwortlichen übermittelt werden können, wenn diese Daten mit hoher

[20] Nichtsdestotrotz kann die betroffene Person nach Maßgabe des (sich auf das Auskunftsrecht beziehenden) Artikels 15 der DSGVO von ihrem Recht Gebrauch machen, „von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten", sowie von ihrem Recht, Informationen über „das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und - zumindest in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person" anzufordern.

[21] Dazu gehören alle Daten, die in Bezug auf die betroffene Person während der Aktivitäten, zu deren Zweck die Daten erhoben werden, beobachtet werden (z.B. ein Transaktionsverlauf oder ein Zugriffsprotokoll). Daten, die im Wege der Nachverfolgung oder durch Aufzeichnung der betroffenen Person (beispielsweise von einer App, die die Herzfrequenz aufzeichnet, oder mithilfe einer Technologie, die das Browsingverhalten aufzeichnen kann) erhoben werden, sollten als von dieser Person „bereitgestellt" betrachtet werden, auch wenn die Daten nicht aktiv oder bewusst übermittelt werden.

Wahrscheinlichkeit in einer Weise verarbeitet werden, durch die die Rechte und Freiheiten anderer Personen beeinträchtigt werden (Artikel 20 Absatz 4 der DSGVO)[22].

Eine solche Beeinträchtigung läge beispielsweise vor, wenn Dritte durch die Übermittlung von Daten von einem Verantwortlichen an einen anderen im Rahmen des Rechts auf Datenübertragbarkeit davon abgehalten würden, ihre Rechte als betroffene Personen gemäß der DSGVO auszuüben (wie das Recht auf Information, Auskunft usw.).

Die betroffene Person, die die Übertragung ihrer Daten an einen anderen Verantwortlichen veranlasst, erteilt dem neuen Verantwortlichen entweder eine Einwilligung für die Verarbeitung oder schließt einen Vertrag mit diesem. Enthält der Datensatz personenbezogene Daten anderer Personen, muss eine andere Rechtsgrundlage für die Verarbeitung ermittelt werden. Beispielsweise kann der Verantwortliche ein berechtigtes Interesse nach Artikel 6 Absatz 1 Buchstabe f verfolgen, insbesondere wenn der Zweck, den er verfolgt, darin besteht, der betroffenen Person einen Dienst bereitzustellen, der es letzterer ermöglicht, personenbezogene Daten ausschließlich zu persönlichen oder familiären Tätigkeiten zu verarbeiten. Sofern der Verantwortliche keine Entscheidungen bezüglich der Verarbeitungsvorgänge trifft, die die betroffene Person im Zusammenhang mit ihrer persönlichen Tätigkeit in die Wege geleitet hat, und die Dritte betreffen und diese möglicherweise beeinträchtigen, ist die betroffene Person für etwaige derartige Beeinträchtigungen verantwortlich.

Beispielsweise kann ein Webmail-Dienst die Erstellung eines Verzeichnisses mit den Kontakten, Freunden, Verwandten, Familienangehörigen und dem weiteren Umfeld der betroffenen Person ermöglichen. Da sich diese Daten auf die bestimmbare Person beziehen, die ihr Recht auf Datenübertragbarkeit ausüben möchte (und von dieser erstellt werden), sollten Verantwortliche das gesamte Verzeichnis der ein- und ausgehenden E-Mails an die betroffene Person übertragen.

Ebenso kann das Bankkonto einer betroffenen Person personenbezogene Daten enthalten, die sich sowohl auf Transaktionen des Kontoinhabers beziehen als auch auf Transaktionen anderer Personen (welche beispielsweise Geld auf das Konto des Kontoinhabers überwiesen haben). Es ist unwahrscheinlich, dass die Rechte und Freiheiten anderer Parteien im Fall einer Portabilitätsanfrage durch die Übermittlung der Kontoinformationen an den Kontoinhaber beeinträchtigt werden, sofern die Daten in den beiden Beispielen für denselben Zweck verwendet werden (d. h. als Kontaktadresse, die ausschließlich von der betroffenen Person verwendet wird, bzw. als Kontoverlauf des Bankkontos der betroffenen Person).

Im Gegensatz dazu liegt eine Verletzung der Rechte und Freiheiten Dritter vor, wenn der neue Verantwortliche die personenbezogenen Daten für andere Zwecke verwendet (und diese beispielsweise zusammen mit personenbezogenen Daten von Kontakten aus dem Adressbuch der betroffenen Person für Vermarktungszwecke verwendet).

Um eine Beeinträchtigung der beteiligten Dritten zu verhindern, ist die Verarbeitung von personenbezogenen Daten dieser Art durch einen anderen Verantwortlichen nur in dem Umfang zulässig, in dem die Daten unter der alleinigen Kontrolle des anfragenden Nutzers bleiben und ausschließlich für persönliche oder familiäre Zwecke verwaltet werden. Ein

[22] „Ist im Fall eines bestimmten Satzes personenbezogener Daten mehr als eine betroffene Person tangiert, so sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen.“ (Erwägungsgrund 68).

„neuer“ Verantwortlicher, der Daten erhält und an den die Daten auf Anfrage des Nutzers übermittelt werden können, darf die übermittelten Daten Dritter nicht für seine eigenen Zwecke verwenden, um diesen anderen Personen z. B. Marketingprodukte und Dienste anzubieten. Beispielsweise dürfen diese Informationen nicht dazu verwendet werden, das Profil des von der Datenverarbeitung betroffenen Dritten ohne dessen Wissen und Zustimmung zu verfeinern und seine soziale Umgebung neu aufzubauen[23]. Auch dürfen sie nicht dazu verwendet werden, Informationen über derartige Dritte abzufragen und spezifische Profile zu erstellen. Dies gilt auch dann, wenn ihre personenbezogenen Daten dem Verantwortlichen bereits vorliegen. Anderenfalls ist eine solche Verarbeitung mit hoher Wahrscheinlichkeit unrechtmäßig und unfair, insbesondere wenn die betroffenen Dritten nicht darüber informiert werden und nicht von ihrem Recht als betroffene Personen Gebrauch machen können.

Ein bewährtes Verfahren für sämtliche Verantwortlichen, die personenbezogene Daten erhalten oder übermitteln, besteht darin, Tools einzusetzen, die den betroffenen Personen ermöglichen, diejenigen Daten, die sie erhalten und übermitteln möchten, auszuwählen und etwaige Daten anderer Personen auszuschließen. Auf diese Weise können die Risiken für Dritte, deren personenbezogene Daten möglicherweise mitübertragen werden könnten, weiter verringert werden.

Darüber hinaus sollten die Verantwortlichen Einwilligungsmechanismen für andere beteiligte Personen einführen, um die Datenübertragung in den Fällen zu vereinfachen, in denen solche Dritte bereit sind, ihre Einwilligung zu erteilen, weil sie beispielsweise ihre Daten an einen anderen Verantwortlichen übertragen möchten. Ein solcher Fall könnte sich beispielsweise bei einem sozialen Netzwerk ergeben, doch es ist Sache der Verantwortlichen, die maßgeblichen Vorgehensweisen festzulegen.

Für Daten im Zusammenhang mit Rechten an geistigem Eigentum und Geschäftsgeheimnissen gilt:
Die Rechte und Freiheiten anderer Personen werden in Artikel 20 Absatz 4 angesprochen. Obschon kein direkter Bezug zur Datenportabilität hergestellt wird, kann davon ausgegangen werden, dass auch Geschäftsgeheimnisse und geistiges Eigentum (und insbesondere das geistige Eigentum an Software) unter die betroffenen Daten fallen. Auch wenn diese Rechte im Vorfeld einer Portabilitätsanfrage berücksichtigt werden sollten, „darf dies jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.“ Zudem darf der Verantwortliche eine Portabilitätsanfrage nicht wegen eines Verstoßes gegen ein anderes Vertragsrecht (wie eine ausstehende Schuld oder ein geschäftlicher Konflikt mit der betroffenen Person) zurückweisen.

Das Recht auf Datenübertragbarkeit berechtigt eine Person nicht, die Informationen in der Form zu missbrauchen, dass dies als unlautere Praxis eingestuft werden könnte oder dass dies eine Verletzung von Rechten an geistigem Eigentum begründen würde.

Ein potenzielles Geschäftsrisiko kann jedoch nicht per se als Grund dafür dienen, eine Portabilitätsanfrage zurückzuweisen, denn die für die Verarbeitung Verantwortlichen können die von betroffenen Personen bereitgestellten personenbezogenen Daten so übermitteln, dass

[23] Ein Betreiber eines sozialen Netzwerks darf personenbezogene Daten, die ihm eine betroffene Person in Ausübung ihres Rechts auf Datenübertragbarkeit übermittelt, nur dann zur Verfeinerung des Profils seiner Nutzer verwenden, wenn er dem Transparenzgrundsatz Rechnung trägt und sicherstellt, dass diese spezifische Datenverarbeitung auf geeigneter Rechtsgrundlage erfolgt.

keine unter das Geschäftsgeheimnis fallenden oder durch Rechte an geistigem Eigentum geschützten Informationen offengelegt werden.

IV. Inwiefern gelten die allgemeinen Regeln für die Ausübung der Rechte der betroffenen Person für die Datenübertragbarkeit?

- **Welche vorherigen Informationen sollten der betroffenen Person mitgeteilt werden?**

Um dem neuen Recht auf Datenübertragbarkeit Genüge zu tun, müssen die Verantwortlichen die betroffenen Personen über das Bestehen dieses neuen Rechts unterrichten. Erfolgt die Erhebung der personenbezogenen Daten von der betroffenen Person auf direktem Wege, hat diese Belehrung „zum Zeitpunkt der Erhebung dieser Daten" zu erfolgen. Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so hat der Verantwortliche die in Artikel 13 Absatz 2 Buchstabe b und in Artikel 14 Absatz 2 Buchstabe c genannten Informationen mitzuteilen.

Für den Fall, dass die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, sieht Artikel 14 Absatz 3 vor, dass diese Informationen „innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats", „spätestens zum Zeitpunkt der ersten Mitteilung an sie" oder „spätestens zum Zeitpunkt der ersten Offenlegung" gegenüber Dritten[24] erteilt werden.

Bei der Erteilung der erforderlichen Informationen müssen die Verantwortlichen sicherstellen, dass das Recht auf Datenübertragbarkeit von anderen Rechten abgegrenzt wird. Die Datenschutzgruppe empfiehlt daher insbesondere, dass Verantwortliche klar und deutlich den Unterschied zwischen den verschiedenen Arten von Daten darlegen, die eine betroffene Person erhalten kann, wenn sie von ihrem Auskunftsrecht oder von ihrem Recht auf Datenübertragbarkeit Gebrauch macht.

Zusätzlich empfiehlt die Gruppe den Verantwortlichen, vor jeder etwaigen Kontoschließung Informationen über das Recht auf Datenübertragbarkeit zur Verfügung zu stellen. Dadurch wird den Nutzern die Möglichkeit gegeben, sich einen Überblick über ihre personenbezogenen Daten zu verschaffen und die Daten auf einfache Weise auf ihre eigenen Geräte oder an einen anderen Anbieter zu übermitteln, bevor ein Vertrag beendet wird.

Schließlich empfiehlt die Datenschutzgruppe als bewährtes Verfahren für Verantwortliche, „die Daten erhalten", dass diese die betroffenen Personen umfassend über die Art der personenbezogenen Daten informieren, die für die Erbringung ihrer Leistungen erheblich sind. Dies ist nicht nur im Sinne einer fairen Datenverarbeitung, sondern ermöglicht den Nutzern zudem, etwaige Risiken für Dritte zu beschränken und unnötige Vervielfältigungen personenbezogener Daten zu vermeiden, selbst wenn keine weiteren betroffenen Personen beteiligt sind.

[24] In Artikel 12 ist vorgeschrieben, dass Verantwortliche „alle Mitteilungen (…) in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache (…) übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten."

- **Wie kann der Verantwortliche die betroffene Person identifizieren, bevor er ihrer Anfrage nachkommt?**

Die DSGVO enthält keine Vorschriften darüber, wie die betroffenen Personen zu authentifizieren sind. Gleichwohl ist in Artikel 12 Absatz 2 der DSGVO festgelegt, dass der Verantwortliche sich nicht weigern darf, tätig zu werden, wenn er eine Anfrage einer betroffenen Person erhält, die von ihren Rechten (einschließlich des Rechts auf Datenübertragbarkeit) Gebrauch machen möchte - es sei denn, die Verarbeitung personenbezogener Daten soll zu einem Zweck erfolgen, für den die Identifizierung einer betroffenen Person nicht erforderlich ist, und er kann nachweisen, dass es ihm nicht möglich ist, die betroffene Person zu identifizieren. Allerdings kann die betroffene Person gemäß Artikel 11 Absatz 2 weitere Informationen bereitstellen, um ihre Identifizierung zu ermöglichen. Darüber hinaus ist in Artikel 12 Absatz 6 vorgesehen, dass ein Verantwortlicher, der begründete Zweifel an der Identität einer betroffenen Person hat, weitere Informationen verlangen kann, die die Identität der betroffenen Person bestätigen. Stellt eine betroffene Person zusätzliche Informationen zur Verfügung, die ihre Identifizierung ermöglichen, darf sich der Verantwortliche nicht weigern, ihrer Anfrage nachzukommen. In Fällen, in denen online erhobene Informationen und Daten mit Pseudonymen oder eindeutigen Kennungen verknüpft sind, können Verantwortliche geeignete Verfahren einführen, die es einer Person ermöglichen, eine Portabilitätsanfrage einzureichen und die sie betreffenden Daten zu erhalten. In jedem Fall müssen Verantwortliche ein Authentifizierungsverfahren einführen, um die Identität der betroffenen Person, die ihre personenbezogenen Daten anfordert oder allgemein die ihr durch die DSGVO übertragenen Rechte ausüben möchte, sicher festzustellen.

In vielen Fällen bestehen derartige Verfahren bereits. Oftmals werden die betroffenen Personen vom Verantwortlichen identifiziert, bevor ein Vertrag abgeschlossen oder ihre Zustimmung zu der Datenverarbeitung eingeholt wird. Die personenbezogenen Daten, die für die Registrierung der von der Datenverarbeitung betroffenen Personen verwendet werden, können daher auch für die Authentifizierung dieser Personen bei Portabilitätsanfragen verwendet werden[25].

In derartigen Fällen kann es für die vorherige Identifizierung der betroffenen Person erforderlich sein, eine Anfrage zum Nachweis ihrer rechtlichen Identität vorzunehmen. Die diesbezügliche Überprüfung kann jedoch nicht erheblich für die Bewertung der Verbindung zwischen den Daten und der betroffenen Person sein, da die Verbindung in keinem Zusammenhang mit der amtlichen oder rechtlichen Identität steht. Im Wesentlichen darf die dem Verantwortlichen offenstehende Möglichkeit, zusätzliche Informationen anzufordern, um die Identität einer Person überprüfen zu können, nicht zu exzessiven Datenanfragen führen oder die Erhebung personenbezogener Daten nach sich ziehen, die nicht erheblich oder nicht notwendig für eine nähere Ermittlung der Verbindung zwischen der Person und den angeforderten personenbezogenen Daten sind.

In vielen Fällen sind solche Authentifizierungsverfahren bereits eingerichtet. Beispielsweise werden Nutzernamen und Passwörter häufig verwendet, um Einzelnen den Zugriff auf ihre Daten in ihren E-Mail-Konten, in ihren Nutzerkonten bei sozialen Netzwerken oder in ihren

[25] Wenn die Datenverarbeitung in Verbindung mit einem Nutzerkonto erfolgt, können beispielsweise das Login und das Passwort für die Identifizierung der betroffenen Person ausreichen.

für sonstige Dienste genutzten Konten zu ermöglichen, zu deren Nutzung sich manche Personen ohne Angabe ihres vollständigen Namens und ihrer Identität entschieden haben.

Ist die Übertragung über das Internet aufgrund der Größe der von der betroffenen Person angeforderten Daten problematisch, muss der Verantwortliche unter Umständen, statt von einer verlängerten Frist von maximal drei Monaten zur Beantwortung der Anfrage[26] Gebrauch zu machen, auch alternative Mittel zur Bereitstellung der Daten in Erwägung ziehen, beispielsweise Streaming-Verfahren, die Speicherung auf einer CD, DVD oder einem anderen physischen Medium oder die direkte Übermittlung an einen anderen Verantwortlichen (gemäß Artikel 20 Absatz 2 der DSGVO, sofern technisch machbar).

- **Welche Frist gilt für die Beantwortung einer Anfrage zur Datenübertragbarkeit?**

In Artikel 12 Absatz 3 ist vorgesehen, dass der Verantwortliche der betroffenen Person Informationen über die ergriffenen Maßnahmen „unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang" der Anfrage zur Verfügung stellt. Die Frist von einem Monat kann in komplexen Fällen auf bis zu drei Monate verlängert werden, sofern die betroffene Person innerhalb eines Monats nach Eingang der Anfrage über die Fristverlängerung und die Gründe für die Verzögerung unterrichtet wird.

Verantwortliche, die Dienste der Informationsgesellschaft betreiben, sind technisch zumeist besser in der Lage, Anfragen innerhalb kürzester Fristen zu bearbeiten. Um den Erwartungen der Nutzer gerecht zu werden, empfiehlt es sich, die Fristen festzulegen, binnen derer Portabilitätsanfragen üblicherweise beantwortet werden können, und diese den betroffenen Personen mitzuteilen.

Verantwortliche, die es ablehnen, einer Anfrage zur Datenübertragbarkeit nachzukommen, haben die betroffene Person gemäß Artikel 12 Absatz 4 spätestens innerhalb eines Monats nach Eingang der Anfrage „über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen" zu unterrichten.

Verantwortliche müssen sich auch dann, wenn sie sich weigern, tätig zu werden, an die Pflicht halten, innerhalb der vorgegebenen Fristen zu antworten. Anders ausgedrückt: Der Verantwortliche kann, wenn er eine Portabilitätsanfrage erhält, nicht schweigen.

- **In welchen Fällen kann eine Anfrage zur Datenübertragbarkeit abgelehnt oder ein Entgelt berechnet werden?**

Gemäß Artikel 12 ist es dem Verantwortlichen untersagt, ein Entgelt für die Bereitstellung der personenbezogenen Daten zu berechnen, es sei denn, er kann nachweisen, dass die Anfragen offenkundig unbegründet oder „*insbesondere im Fall von häufiger Wiederholung*" exzessiv sind. Dienste der Informationsgesellschaft, die sich auf die automatische Verarbeitung personenbezogener Daten spezialisieren und dabei auf automatisierte Systeme wie Programmierschnittstellen (API)[27] zurückgreifen, können den Austausch mit der betroffenen

[26] Diesbezüglich sieht Artikel 12 Absatz 3 vor: „Der Verantwortliche stellt der betroffenen Person Informationen über die (...) ergriffenen Maßnahmen (...) zur Verfügung."

[27] Eine API ist eine Schnittstelle einer Anwendung oder eines Webdienstes, die von einem Verantwortlichen zur Verfügung gestellt wird, damit andere Systeme oder Anwendungen an sein Systemen angebunden werden können.

Person vereinfachen und somit einem durch Mehrfachanfragen entstehenden Mehraufwand entgegenwirken. Selbst bei einer großen Zahl von Portabilitätsanfragen dürfte es mithin nur sehr wenige Fälle geben, in denen der Verantwortliche eine Bereitstellung der angeforderten Informationen zu Recht verweigern kann.

Des Weiteren dürfen die Gesamtkosten für die zur Beantwortung von Datenübertragbarkeitsanfragen eingerichteten Prozesse bei der Beurteilung, ob eine Anfrage als exzessiv zu betrachten ist, keine Rolle spielen. Artikel 12 bezieht sich auf konkrete Anfragen einer einzelnen betroffenen Person, nicht auf die Gesamtzahl der bei einem Verantwortlichen eingehenden Anfragen. Daher dürfen die Gesamtkosten der Systemimplementierung weder den betroffenen Personen in Rechnung gestellt noch als Rechtfertigung für die Weigerung, einer Anfrage zur Datenübertragbarkeit nachzukommen, herangezogen werden.

V. Wie müssen die portablen Daten bereitgestellt werden?

- Mit welchen Mitteln sollen Verantwortliche die Daten bereitstellen?

Die betroffene Person hat nach Artikel 20 Absatz 1 das Recht, die sie betreffenden personenbezogenen Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

Eine solche Behinderung lässt sich als jedwede rechtliche, technische oder finanzielle Hürde charakterisieren, durch die ein Verantwortlicher den Datenzugriff, die Datenübertragung oder die Datenwiederverwendung vonseiten der betroffenen Person oder eines anderen Verantwortlichen verlangsamen oder verhindern möchte. Sie liegt beispielsweise vor, wenn Gebühren für die Datenbereitstellung erhoben werden, wenn keine Dateninteroperabilität geboten wird bzw. kein Zugriff auf ein Datenformat, keine Programmierschnittstelle oder nicht das bereitgestellte Format angeboten wird, wenn übermäßige Verzögerungen auftreten oder die Abfrage des vollständigen Datensatzes zu kompliziert ist, wenn Daten absichtlich verschleiert werden, oder wenn spezifische, überzogene oder nicht gerechtfertigte sektorspezifische Normungs- oder Akkreditierungsanforderungen aufgestellt werden[28].

Nach Artikel 20 Absatz 2 ist der Verantwortliche verpflichtet, die portablen Daten auf Wunsch auf direktem Wege an einen anderen Verantwortlichen zu übermitteln, „soweit dies technisch machbar ist".

Inwieweit es technisch machbar ist, personenbezogene Daten unter der Kontrolle der betroffenen Person von einem Verantwortlichen an einen anderen Verantwortlichen zu übermitteln, ist von Fall zu Fall zu prüfen. Bezüglich der Grenzen des technisch Machbaren heißt es in Erwägungsgrund 68: „Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten."

[28] Gleichwohl können bestimmte legitime Hindernisse auftraten, insbesondere im Zusammenhang mit den Rechten und Freiheiten anderer Personen (Artikel 20 Absatz 4) oder im Zusammenhang mit der Sicherheit der Systeme des Verantwortlichen. In solchen Fällen hat der Verantwortlich zu begründen, inwieweit derartige Hindernisse legitim sind und keine Behinderung im Sinne von Artikel 20 Absatz 1 darstellen.

Vom Verantwortlichen wird erwartet, dass er die personenbezogenen Daten in einem interoperablen Format übermittelt. Gleichwohl sind andere Verantwortliche deshalb keineswegs verpflichtet, diese Formate zu unterstützen. Eine direkte Datenübermittlung von einem Verantwortlichen an einen anderen Verantwortlichen kann daher erfolgen, wenn eine sichere Kommunikation[29] zwischen den beiden Systemen möglich und das empfangende System technisch in der Lage ist, die übermittelten Daten entgegenzunehmen. Falls eine direkte Datenübermittlung aufgrund technischer Hindernisse nicht möglich ist, muss der Verantwortlich die betroffenen Personen über die Hindernisse informieren. Andernfalls käme sein Vorgehen einer Weigerung, einer Portabilitätsanfrage einer betroffenen Person nachzukommen, gleich (Artikel 12 Absatz 4).

Verantwortliche sollten auf technischer Ebene zwei unterschiedliche, einander ergänzende Verfahren analysieren und bewerten, durch die portable Daten an betroffene Personen oder andere Verantwortliche übermittelt werden können:

- direkte Übermittlung des vollständigen Datensatzes (oder mehrerer Auszüge von Teilen des Datensatzes)
- Einsatz eines automatisierten Werkzeugs, das die Extrahierung der relevanten Daten ermöglicht.

Das zweite Verfahren dürfte vom Verantwortlichen bei komplexen und umfangreichen Datensätzen vorzuziehen sein, denn es ermöglicht ihm, genau jene Teile des Datensatzes zu extrahieren, die für die betroffene Person laut deren Anfrage relevant sind. Dies kann zur Risikominimierung beitragen und auch die Nutzung von Datensynchronisierungsverfahren[30] (beispielsweise im Rahmen der regelmäßigen Kommunikation zwischen Verantwortlichen) ermöglichen. Dieses Verfahren eignet sich vielleicht besser, um die Vorschrifteneinhaltung des „neuen“ Verantwortlichen sicherzustellen und kann als bewährtes Verfahren zur Verringerung von Datenschutzrisiken bei der Datenverarbeitung aufseiten des ursprünglichen Verantwortlichen gelten.

Zur Implementierung dieser beiden unterschiedlichen, im Idealfall einander ergänzenden Verfahren für die Übermittlung relevanter portabler Daten könnten die betreffenden Daten auf verschiedenen Wegen (z.B. sichere E-Mail, SFTP-Server, sichere Web-Schnittstelle oder Web-Portal) bereitgestellt werden. Betroffenen Personen sollte der Rückgriff auf einen persönlichen Datenspeicher, ein persönliches Informationsmanagementsystem[31] oder andere vertrauenswürdige Dritte ermöglicht werden, damit sie die personenbezogenen Daten vorhalten und speichern und gegebenenfalls Verantwortlichen die Erlaubnis erteilen können, auf die personenbezogenen Daten zuzugreifen und sie zu verarbeiten.

- **Welches ist das erwartete Dateiformat?**

Die DSGVO verpflichtet Verantwortliche, die von der Person angeforderten personenbezogenen Daten in einem Format bereitzustellen, das mit einer Weiterverwendung vereinbar ist. Insbesondere in Artikel 20 Absatz 1 der DSGVO wird ausgeführt, dass die

[29] Per Authentisierungsverfahren mit geeigneter Datenverschlüsselung.
[30] Synchronisierungsverfahren können die Einhaltung der allgemeinen Pflicht nach Artikel 5 der DSGVO erleichtern, wonach personenbezogene Daten „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein“ müssen.
[31] Siehe diesbezüglich beispielsweise die Stellungnahme Nr. 9/2016 des Europäischen Datenschutzbeauftragten: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf

personenbezogenen Daten „in einem strukturierten, gängigen und maschinenlesbaren Format“ bereitgestellt werden müssen. Erwägungsgrund 68 enthält diesbezüglich die Präzisierung, dass dieses Format „interoperabel“ sein sollte. Interoperabilität ist nach dem EU-Recht[32]

> *die Fähigkeit verschiedener und unterschiedlicher Organisationen zur Interaktion zum beiderseitigen Nutzen und im Interesse gemeinsamer Ziele; dies schließt den Austausch von Informationen und Wissen zwischen den beteiligten Organisationen durch von ihnen unterstützte Geschäftsprozesse mittels Datenaustausch zwischen ihren jeweiligen IKT-Systemen ein.*

Die Begriffe „strukturiert“, „gängig“ und „maschinenlesbar“ bezeichnen bestimmte Mindestanforderungen, durch die die Interoperabilität des vom Verantwortlichen bereitgestellten Datenformats ermöglicht werden soll. Sie stellen somit Leistungsvorgaben für die Mittel dar, und Interoperabilität ist das gewünschte Ergebnis.

Gemäß Erwägungsgrund 21 der Richtlinie 2013/37/EU[33,34] gilt ein Dokument als „maschinenlesbar“,

> *wenn es in einem Dateiformat vorliegt, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten, einschließlich einzelner Sachverhaltsdarstellungen und deren interner Struktur, einfach identifizieren, erkennen und extrahieren können. In Dateien verschlüsselte Daten, die in maschinenlesbarem Format strukturiert sind, sind maschinenlesbare Daten. Maschinenlesbare Formate können offen oder geschützt sein; sie können einem formellen Standard entsprechen oder nicht. Dokumente, die in einem Dateiformat verschlüsselt sind, das eine automatische Verarbeitung einschränkt, weil die Daten nicht oder nicht ohne Weiteres aus ihnen extrahiert werden können, sollten nicht als maschinenlesbar gelten. Dokumente, die in einem Dateiformat verschlüsselt sind, das eine automatische Verarbeitung einschränkt, weil die Daten nicht oder nicht ohne Weiteres aus ihnen extrahiert werden können, sollten nicht als maschinenlesbar gelten.*

Angesichts des breiten Spektrums an potenziellen Datentypen, die von einem Verantwortlichen verarbeitet werden könnten, sind in der DSGVO keine speziellen Empfehlungen zum Format der bereitzustellenden personenbezogenen Daten vorgesehen. Das am besten geeignete Format wird je nach Sektor unterschiedlich sein, und geeignete Formate existieren bereits, sollten jedoch stets so gewählt werden, dass sie die Voraussetzung der Lesbarkeit erfüllen und eine weitreichende Portabilität der Daten der betroffenen Person ermöglichen. Formate, für die kostspielige Lizenzbeschränkungen gelten, werden nicht als geeigneter Ansatz betrachtet.

---

[32] Artikel 2 des Beschlusses Nr. 922/2009/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über Interoperabilitätslösungen für europäische öffentliche Verwaltungen (ISA) (ABl. L 260 vom 3.10.2009, S. 20).

[33] Zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors.

[34] Im EU-Glossar (http://eur-lex.europa.eu/eli-register/glossary.html) werden nähere Erläuterungen zu den Erwartungen im Zusammenhang mit den in der Richtlinie verwendeten Begriffen wie *„maschinenlesbar“, „Interoperabilität“, „offenes Format“, „Standard“* oder *„Metadaten“* gegeben.

Zudem wird in Erwägungsgrund 68 präzisiert: „*Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten.*“ **Ziel der Übertragbarkeit ist es daher, nicht kompatible, sondern interoperable Systeme zu schaffen**[35].

Personenbezogene Daten sollten in Formaten bereitgestellt werden, die über ein sehr hohes Abstraktionsniveau gegenüber internen oder proprietären Formaten verfügen. Die Datenübertragbarkeit als solche setzt voraus, dass die Verantwortlichen einen zusätzlichen Datenverarbeitungsschritt einfügen, um Daten von der Plattform zu extrahieren und personenbezogene Daten, für die die Übertragbarkeit nicht gilt (z.B. abgeleitete oder sich auf die Systemsicherheit beziehende Daten), herauszufiltern. Verantwortliche sollen so dazu bewegt werden, vorab zu ermitteln, welche Daten in ihren Systemen portabel sind. Diese zusätzliche Datenverarbeitung ist im Verhältnis zur eigentlichen Datenverarbeitung als nachrangig zu betrachten, da damit kein neuer, vom Verantwortlichen festgelegter Zweck verfolgt wird.

Gibt es für eine gegebene Branche oder für einen gegebenen Kontext keine gängigen Formate, **sollten die Verantwortlichen personenbezogene Daten in gemeinhin verwendeten offenen Formaten (wie XML, JSON oder CSV) zusammen mit** sachdienlichen **Metadaten in der bestmöglichen Granularitätsstufe bereitstellen,** dabei aber ein hohes Abstraktionsniveau beibehalten. Dabei sollte der Inhalt der übermittelten Informationen mit geeigneten Metadaten genau beschrieben werden. Diese Metadaten sollten umfangreich genug sein, um die Nutzung und Wiederverwendung der Daten zu ermöglichen, ohne Geschäftsgeheimnisse offenzulegen. PDF-Fassungen eines E-Mail-Eingangsfachs einer betroffenen Person dürften mithin weder strukturiert genug noch hinreichend beschreibend sein, um ohne Weiteres die Wiederverwendung der Daten des Posteingangs zu ermöglichen. Um eine effektive Wiederverwendung der Daten zu ermöglichen, sollten E-Mail-Daten daher in einem Format bereitgestellt werden, bei dem sämtliche Metadaten beibehalten werden. Der Verantwortliche sollte bei der Wahl eines Datenformats, in dem die personenbezogenen Daten bereitgestellt werden, berücksichtigen, wie dieses Format das Recht des Einzelnen auf Wiederverwendung der Daten beeinträchtigen oder seine Ausübung verhindern würde. In Fällen, in denen der Verantwortliche der betroffenen Person hinsichtlich des bevorzugten Formats Wahlmöglichkeiten bieten kann, sollte eine eindeutige Erklärung dazu geliefert werden, welche Auswirkungen die jeweilige Wahl hat. Jedoch stellt jede Verarbeitung zusätzlicher Metadaten, die einzig für den Fall erfolgt, dass diese erforderlich oder erwünscht sein könnten, um Portabilitätsanfragen nachzukommen, keinen rechtmäßigen Grund für eine solche Verarbeitung dar.

Die Datenschutzgruppe empfiehlt nachdrücklich, dass Interessenvertreter der Branche und Fachverbände auf der Grundlage gemeinsamer interoperabler Standards und Formate zusammenarbeiten sollten, um die Anforderungen des Rechts auf Datenübertragbarkeit zu erfüllen. Dieses Thema wurde auch vom Europäischen Interoperabilitätsrahmen (EIF) aufgegriffen, einem gemeinsamen Konzept für die Interoperabilität von Organisationen, deren Ziel die gemeinsame Erbringung öffentlicher

[35] In ISO/IEC 2382-01 wird Interoperabilität folgendermaßen definiert: „Interoperabilität ist die Fähigkeit, zwischen verschiedenen Funktionseinheiten zu kommunizieren, Programme auszuführen oder Daten zu übertragen, und zwar in einer Weise, dass der Nutzer über wenig oder keine Kenntnisse über die eindeutigen Merkmale dieser Einheiten verfügen muss.“

Dienstleistungen ist. Innerhalb seines Anwendungsbereichs gibt dieser Rahmen eine Reihe gemeinsamer Elemente wie Vokabular, Konzepte, Grundsätze, Richtlinien, Leitfäden, Empfehlungen, Standards, Spezifikationen und Praktiken vor[36].

- **Wie ist bei einer großen oder komplexen Sammlung personenbezogener Daten zu verfahren?**

In der DSGVO ist nicht näher ausgeführt, wie auf Anfragen zu reagieren ist, wenn eine große Datensammlung, eine komplexe Datenstruktur oder andere technische Probleme vorliegen, die den Verantwortlichen oder den betroffenen Personen Schwierigkeiten bereiten könnten.

In jedem Fall ist es sehr wichtig, dass der Einzelne in die Lage versetzt wird, Definition, Schema und Struktur der personenbezogenen Daten, die vom Verantwortlichen bereitgestellt werden könnten, zu erfassen. Beispielsweise könnten Daten zunächst unter Verwendung von Dashboards zusammengefasst werden, was der betroffenen Person ermöglichen würde, Teilmengen der personenbezogenen Daten zu übertragen anstelle des gesamten Katalogs. Der Verantwortliche sollte eine Übersicht „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ (Artikel 12 Absatz 1 der DSGVO) übermitteln, damit die betroffene Person über präzise Informationen darüber verfügt, welche Daten sie für einen gegebenen Zweck herunterladen oder an einen anderen Verantwortlichen übermitteln kann. Beispielsweise müssen betroffene Personen spezifische Daten ohne Weiteres mit Softwareanwendungen identifizieren, erkennen und verarbeiten können.

Wie bereits gesagt, besteht für den Verantwortlichen eine praktische Möglichkeit, Portabilitätsanfragen nachzukommen, darin, eine ausreichend gesicherte und dokumentierte Anwendungsprogrammierschnittstelle (API) anzubieten. Auf diese Weise kann betroffenen Personen ermöglicht werden, ihre personenbezogenen Daten über eigene Software oder über Fremdsoftware beim Verantwortlichen anzufordern oder Dritten (einschließlich anderer Verantwortlicher) die Erlaubnis zu erteilen, dies (wie in Artikel 20 Absatz 2 der DSGVO ausgeführt) in ihrem Auftrag zu tun. Der Zugriff auf Daten über eine von außen zugängliche API kann auch die Möglichkeit eines ausgefeilteren Zugriffssystems bieten, das es erlaubt, mehrfach hintereinander Daten (in Form eines vollständigen Download oder als Deltafunktion mit lediglich den Änderungen seit dem letzten Download) anzufordern, ohne dass dem Verantwortlichen dadurch zusätzlicher Aufwand entsteht.

- **Wie könnten portable Daten gesichert werden?**

Allgemein sollten Verantwortliche gemäß Artikel 5 Absatz 1 Buchstabe f der DSGVO die „angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“.

Jedoch wirft die Übertragung personenbezogener Daten unter Umständen auch Sicherheitsfragen auf.

[36] Quelle: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

Wie kann der Verantwortliche sicherstellen, dass personenbezogene Daten sicher an die richtige Person übermittelt werden?

Da das Ziel der Datenübertragbarkeit darin besteht, personenbezogene Daten aus dem Informationssystem des Verantwortlichen zu erhalten, könnte die Übertragung dieser Daten mit Risiken behaftet sein (insbesondere in Bezug auf Verstöße gegen die Datenschutzbestimmungen bei der Übertragung). Der Verantwortliche ist verpflichtet, alle erforderlichen Sicherheitsvorkehrungen zu treffen, damit die personenbezogenen Daten (mittels Ende-zu-Ende-Verschlüsselung) sicher übertragen werden können und die in seinem System verbleibenden Daten weiterhin geschützt sind, und er muss über transparente Verfahren für das Vorgehen bei etwaigen Verstößen gegen die Datenschutzvorschriften verfügen[37]. Daher sollten Verantwortliche die spezifischen Risiken, die im Zusammenhang mit der Datenübertragbarkeit bestehen, ermitteln und geeignete Maßnahmen zu ihrer Minderung ergreifen.

Beispiele für geeignete Risikominderungsmaßnahmen: (falls eine Authentisierung der betroffenen Person erforderlich ist:) Erforderlichmachung zusätzlicher Authentisierungsinformationen (Geheimnis oder andere Authentisierungsmöglichkeit wie ein einmaliges Passwort); (falls der Verdacht besteht, dass das Konto kompromittiert wurde:) Aussetzung oder Einfrieren der Datenübertragung; (bei direkten Datenübertragungen zwischen Verantwortlichen:) Authentisierung per Mandat (z.B. mit Token).

Derartige Sicherheitsmaßnahmen dürfen ihrem Wesen nach kein Hindernis darstellen und dürfen Nutzer nicht davon abhalten, ihre Rechte auszuüben (z.B. durch Auferlegung von Zusatzkosten).

Wie können Nutzer bei der sicheren Speicherung ihrer personenbezogenen Daten in ihren eigenen Systemen unterstützt werden?

Beim Abruf ihrer personenbezogenen Daten von einem Online-Dienst besteht stets das Risiko, dass die Nutzer die Daten in einem weniger gut gesicherten System als dem des Dienstes abspeichern. Jede betroffene Person ist selbst dafür verantwortlich, die von ihr angeforderten personenbezogenen Daten auf geeignete Weise in ihrem eigenen System sicher zu verwahren. Daher sollten betroffene Personen stets auf diese Pflicht hingewiesen werden, damit sie geeignete Maßnahmen zum Schutz der abgerufenen Daten ergreifen. Als bewährtes Verfahren können Verantwortliche beispielsweise auch geeignete Formate, Verschlüsselungstools und sonstige Sicherheitsmaßnahmen empfehlen, die der betroffenen Person dabei helfen, dieses Ziel zu erreichen.

* * *

Geschehen zu Brüssel am 13. Dezember 2016.

Für die Datenschutzgruppe
Die Vorsitzende
Isabelle FALQUE-PIERROTIN

[37] Gemäß der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netzen und Informationssystemen in der Union.

zuletzt überarbeitet und angenommen am 5. April 2017

Für die Datenschutzgruppe
Die Vorsitzende
Isabelle FALQUE-PIERROTIN