facebook

BLICK IN
DIE ZUKUNFT »

Datenübertragbarkeit und Datenschutz

Erin Egan
Vizepräsident und
Chief Privacy Officer, Richtlinie

September 2019

Inhaltsverzeichnis

Datenübertragbarkeit und Datenschutz

Immer mehr politische Entscheidungsträger in aller Welt sind sich einig darüber, dass die Datenübertragbarkeit – die Möglichkeit, die mit einem Dienst geteilten Daten an einen anderen zu übertragen – den Online-Wettbewerb und die Entwicklung neuer Dienste fördert. Wettbewerbs- und Datenschutzexperten stimmen überein, dass die Datenübertragbarkeit Nutzern trotz komplexer Sachverhalte dabei hilft, ihre Daten zu kontrollieren, und die Wahl des richtigen Online-Dienstanbieters vereinfacht.

Die Vorteile der Datenübertragbarkeit für Menschen und Märkte liegen auf der Hand. Deshalb hat unser CEO, Mark Zuckerberg, kürzlich Gesetze gefordert, die diese Datenübertragbarkeit garantieren.[1] Um zuverlässige und effektive Datenübertragungstools entwickeln zu können, müssen wir klare Regeln aufstellen, welche Arten von Daten übertragen werden dürfen und wer während der Übertragung für den Schutz dieser Daten verantwortlich ist.[2] Mit diesem Whitepaper möchten wir die Diskussion darüber vertiefen, wie diese Regeln aussehen sollten.

Dieses Paper soll Beteiligte weltweit zur Diskussion darüber anregen, wie datenschutzkonforme Produkte zur Datenübertragung entwickelt werden können und wie dabei gleichzeitig ein lebendiger Wettbewerb zwischen den Online-Diensten aufrechterhalten werden kann. Daraus soll ein Rahmen für die Datenübertragbarkeit entstehen, der die Produktentwicklung bei uns und anderen Unternehmen optimiert, die Zusammenarbeit in der Branche fördert und als mögliche Informationsquelle für künftige Gesetzgebungen dient.

Um dies zu erreichen, stellt das Paper fünf Fragen zu Datenschutz und Datenübertragbarkeit:

1. ### Was ist „Datenübertragbarkeit“?

   Sollten alle nutzergesteuerten Datenübertragungen an Dritte unter Datenübertragbarkeit zu verstehen sein? hould all user-directed data transfers to third parties be considered “data portability”?

2. ### Welche Daten sollten übertragbar sein?

   Sollten übertragbare Daten begrenzt sein auf solche, die eine Person einem Dienstanbieter zur Verfügung gestellt hat? (Und was bedeutet „zur Verfügung stellen“ in diesem Zusammenhang?)

3. ### Wessen Daten sollten übertragbar sein?

   Sollten die übertragenden Anbieter die Datenübertragbarkeit einschränken, wenn Daten mit mehr als nur einer Person verknüpft sind, was in sozialen Netzwerken oft der Fall ist? Wie können Anbieter sicherstellen, dass die Rechte jeder einzelnen Person gewahrt werden?

4. ### Wie sollten wir Daten im Rahmen der Datenübertragbarkeit schützen?

   What responsibilities, if any, should transferring providers have with respect to (1) requesting users, (2) others whose interests may be implicated by a transfer, and (3) potential recipients of the data?

5. ### Wer ist nach der Übertragung von Daten einer Person verantwortlich, falls die Daten missbräuchlich verwendet oder nicht ausreichend geschützt werden?

   Welche Verantwortlichkeiten sollten der übertragende und der empfangende Anbieter jeweils haben? Sollten Nutzer selbst für Probleme mit ihren Daten (oder denen ihrer Freunde) verantwortlich sein?

Von einigen wichtigen Akteuren liegen uns bereits Antworten auf diese Fragen vor, zum Beispiel die Empfehlung der EU-Datenschutzbehörden zum Recht auf Datenübertragbarkeit im Rahmen der europäischen Datenschutz-Grundverordnung („DSGVO“) aus dem Jahr 2017, zwei aktuelle Paper der Personal Data Protection Commission von Singapur, ein von der Generaldirektion „Wettbewerb“ der Europäischen Kommission beauftragter Bericht zum Thema „Wettbewerbspolitik für das digitale Zeitalter“ und ein Bericht zur Datenmobilität, der vom britischen Department for Digital, Culture, Media & Sport in Auftrag gegeben wurde. Wir sind jedoch der Meinung, dass weitere Diskussionen und Anregungen für die Branche nützlich wären.

Dieses Paper konzentriert sich auf Datenübertragbarkeit als Vorgang, zu dem sich einzelne Nutzer eines Dienstes entschließen. Es befasst sich nicht mit Datenübertragungen zwischen Unternehmen. Uns ist bewusst, dass auch diese Übertragungen hinsichtlich Auswahlmöglichkeit und Wettbewerb von zentraler Bedeutung sind. Deshalb suchen wir nach Möglichkeiten, Daten anderen Unternehmen zur Verfügung zu stellen, sodass diese sie beispielsweise zum Trainieren künstlicher Intelligenzen verwenden können. Die Datenschutzprobleme bei dieser Art von Übertragungen unterscheiden sich von Übertragungen, die einzelne Personen vornehmen. In diesem Paper befassen wir uns mit Datenübertragungen, die von einzelnen Personen angestoßen werden. Jedoch werden wir uns auch künftig mit Experten über die Datenübertragung zwischen Unternehmen austauschen.

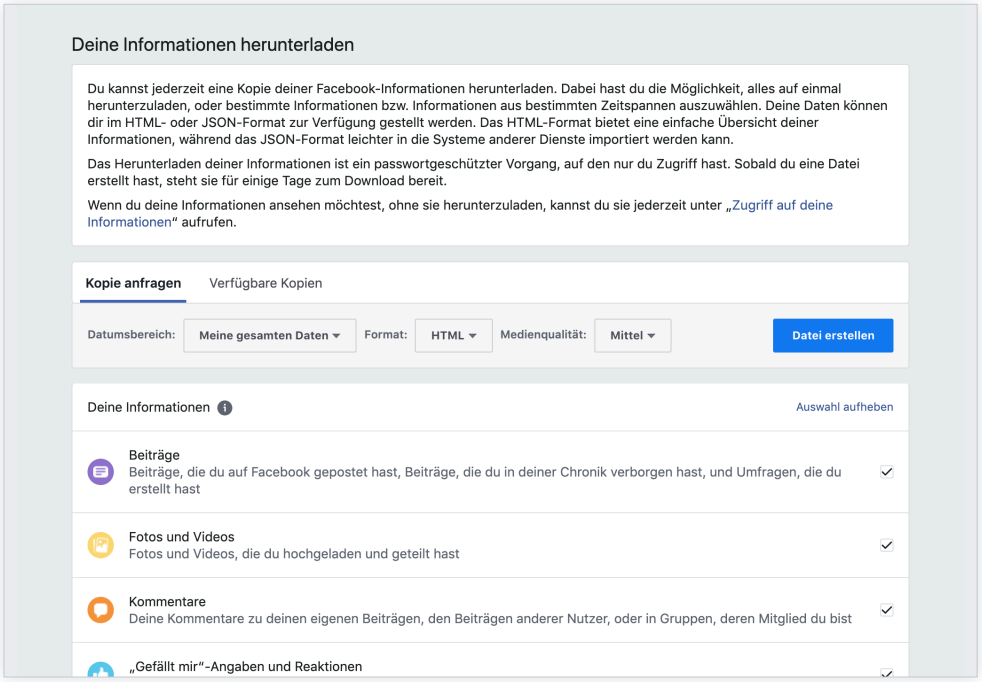
Vielen Dank im Voraus für die Teilnahme an dieser wichtigen Debatte! Wir freuen uns über Feedback von allen Beteiligten und sind gespannt auf unterschiedlichste Meinungen.

I. Die Herausforderung

Einer der Grundsätze des Datenschutzes bei Facebook ist, dass Nutzer stets in der Lage sein sollen, die Verwendung ihrer Informationen zu kontrollieren.[3] Ausgehend davon haben wir Tools entwickelt, die es unseren Nutzern u. a. ermöglichen, selbst zu bestimmen, welche Profilinformationen und Beiträge für andere Nutzer sichtbar sind. Außerdem geben die Tools Nutzern die Kontrolle über ihre Werbepräferenzen, sodass sie beeinflussen können, auf Basis welcher persönlicher Daten ihnen Werbung gezeigt wird.

Mit diesen Tools können die Nutzer also steuern, wie ihre Informationen auf Facebook genutzt werden. Wir sind uns bewusst, dass Kontrolle für Nutzer auch eine Stärkung der Auswahl und des Wettbewerbs bedeutet, indem Verbraucher in die Lage versetzt werden, ihre Daten von einem Anbieter zu einem anderen zu übertragen. Dadurch entsteht die Notwendigkeit, neue Produkte zu entwickeln, die die Datenportabilität vorantreiben.

Gesetze wie die DSGVO[4] und der California Consumer Privacy Act („CCPA“)[5] haben in manchen Regionen die Datenübertragbarkeit rechtlich verankert. Facebook hat jedoch bereits vor diesen Gesetzen nach Möglichkeiten gesucht, die Übertragung von Facebook-Nutzerdaten an andere Plattformen und Dienste zu optimieren. So bieten wir beispielsweise seit 2010 die Funktion „Deine Informationen herunterladen“. Sie wurde dafür konzipiert, dass Nutzer auf ihre Daten zugreifen und diese mit anderen Online-Diensten teilen können. Zeitgleich mit dem Inkrafttreten der DSGVO haben wir diese Funktion weiter an die Anforderungen der Datenübertragbarkeit angepasst, sodass die Nutzerinformationen jetzt im gängigen, strukturierten JSON-Format abrufbar sind.



Als Datenübertragungstool ist die Funktion „Deine Informationen herunterladen“ zwar solide, doch wir sind der Auffassung, dass wir die Auswahl- und Kontrollmöglichkeiten zusätzlich verbessern können, indem wir die Datenübertragung an andere Dienste weiter vereinfachen. Mark Zuckerberg schrieb erst kürzlich in einem Gastbeitrag, Datenübertragbarkeit solle nicht wie jetzt dem Herunterladen eines Archivs mit den Nutzerinformationen ähneln, sondern eher so funktionieren wie das Anmelden bei einer App mithilfe der Facebook-Plattform.[6] Kurz: Nutzer müssen in die Lage versetzt werden, ihre Informationen direkt an einen Anbieter ihrer Wahl zu übertragen, vergleichbar mit dem Facebook Login.

Um dieses Ziel zu erreichen, beteiligen wir uns am „Data Transfer Project“. Aufgabe dieses Open-Source-Softwareprojekts, an dem auch Google, Microsoft, Twitter, Apple und andere Unternehmen teilnehmen, ist es, gemeinsam wechselseitig kompatible Systeme zu entwickeln. Diese sollen es den Nutzern erleichtern, ihre Daten problemlos zwischen Anbietern von Online-Diensten zu übertragen.[7] Das durch die DSGVO begründete Recht auf Datenübertragbarkeit hat den Anstoß dafür gegeben. Sicherlich wird dieses Prinzip schon bald weltweit zur Norm. Im US-Bundesstaat Kalifornien wurde beispielsweise ein Gesetz verabschiedet, das ab 2020 die Datenübertragbarkeit regelt. Und auch in anderen Ländern wie Singapur, Australien, Indien, Hongkong usw. werden voraussichtlich schon bald ähnliche Gesetze eingeführt. Des Weiteren berücksichtigt die Europäische Kommission die Rolle von Portabilität bei der Wettbewerbspolitik im digitalen Zeitalter.[8]

Zweifellos hängt der Erfolg der Datenübertragbarkeit in hohem Maße auch von der Industrie ab. Ihre Aufgabe ist es, wie in dem vorliegenden Papier, grundlegende Fragen in puncto Datenschutz zu klären.[9] Zu einer Frage gibt es nur wenig Hilfestellung: Wie können oder sollen Anbieter die durch das Recht auf Datenübertragbarkeit entstehenden Vorteile, etwa Selbstbestimmung, Innovation und Wettbewerb abwägen gegen die einhergehenden Risiken in Bezug auf Datenschutz und Sicherheit?[10] Die Artikel-29-Datenschutzgruppe (Vorgänger des

Europäischen Datenschutzausschusses, der die von der Gruppe formulierten Leitlinien übernommen hat) hat zwar die von Datenübertragungstools ausgehenden Gefahren erkannt, doch lediglich darauf hingewiesen, dass die Sicherheitsmaßnahmen das Recht auf Datenübertragbarkeit nicht einschränken dürfen.[11] Außerdem hat die Datenschutzgruppe hervorgehoben, dass es möglich sein muss, das Recht auf Datenübertragbarkeit einer Person einzuschränken, wenn durch die Datenübertragung andere Personen benachteiligt werden könnten. Sie ist jedoch nicht genauer auf dieses Thema eingegangen.[12]

Hinzu kommt, dass sich einige Empfehlungen widersprechen, etwa zur Datenübertragbarkeit und zur Verantwortung der Unternehmen, dem Datenmissbrauch durch Dritte vorzubeugen, an die die Daten übertragen werden. Die für den Datenschutz zuständigen Behörden haben klargemacht, dass Plattformen wie die unsere zumindest bei einigen Beziehungen zu Dritten über Sicherheitsmaßnahmen verfügen müssen, um eventuelle, durch die Datenübertragung entstehende Risiken abzuwehren.[13] In Hinblick auf das Recht auf Datenübertragbarkeit befürwortet die Datenschutzgruppe jedoch die Übermittlung von Daten zwischen Nutzern und Drittanbietern.[14] Die Gruppe erklärt, dass der Datenverantwortliche nicht verantwortlich ist für die Einhaltung der Datenschutzgesetze seitens des empfangenen Datenverantwortlichen, da schließlich nicht der übermittelnde Datenverantwortliche den Empfänger ausgewählt hat.[15]

Mehrere Berichte rund um das Thema Wettbewerb im digitalen Zeitalter weisen auf die Bedeutung von Datenübertragbarkeit für Innovation hin. Dabei wird aber auch erwähnt, dass die potenziellen Risiken für den Datenschutz und die Sicherheit berücksichtigt werden müssen. So betont der Bericht des britischen Digital Competition Expert Panel, dass Konzepte der Datenübertragbarkeit konkrete Datenschutzmaßnahmen vorsehen müssen, denn nur so können die Privatsphäre der Nutzer geschützt und ihre Erwartungen erfüllt werden.[16] Wie diese Maßnahmen genau aussehen sollen, wird im Bericht jedoch nicht näher erläutert.

Da Datenübertragbarkeit bald schon die Norm sein wird, sind klare Regeln zu Portabilität, Datenschutz und Verantwortung für uns und andere Unternehmen von entscheidender Bedeutung.

II. Fünf Fragen zu Datenübertragbarkeit und Verantwortung

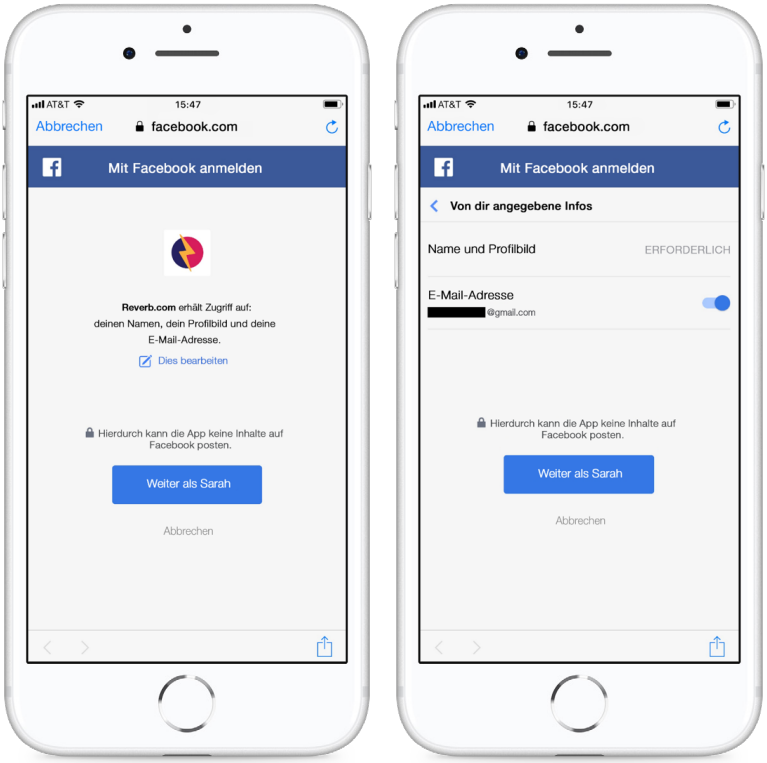
Wie oben erwähnt ist die Datenübertragbarkeit ein Instrument, mit dem Nutzer ihre Daten kontrollieren und die Dienste auswählen können, die am ehesten ihren Bedürfnissen entsprechen. Gleichzeitig stellt dies gewisse Herausforderungen in Bezug auf den Datenschutz dar. Mit dem Feedback und der Unterstützung vieler unterschiedlicher Stakeholder möchten wir diese Herausforderungen meistern und Portabilität so gestalten, das Nutzer die Kontrolle haben und gleichzeitig der Wettbewerb gestärkt wird, ohne dadurch das Vertrauen in die Online-Anbieter zu kompromittieren.[17] In diesem Abschnitt präsentieren wir fünf grundlegende Fragen. Die Antworten können als Ausgangspunkt dienen für die Entwicklung von Datenübertragungsprodukten der nächsten Generation. Wir möchten auch unsere eigenen Antworten auf diese Fragen vorstellen, um so der Diskussion über diese wichtigen Themen neue Impulse zu geben.

FRAGE 1: WAS IST DATENÜBERTRAGBARKEIT?

Betrachtet man die Literatur zu Datenübertragbarkeit, könnte man meinen, es gebe ein glasklares Konzept mit einer einstimmigen Definition. So beschreibt beispielsweise die Artikel-29-Datenschutzgruppe Datenübertragbarkeit im Rahmen der DSGVO als das Recht, personenbezogene Daten abzurufen und sie von einem Anbieter an einen anderen zu übermitteln.[18] Die Internationale Organisation für Normung definiert den Begriff „Datenübertragbarkeit" folgendermaßen: Die Möglichkeit, Daten von einem System auf ein anderes zu übertragen und zwar ohne erneute Dateneingabe. Bei dieser Definition liegt der Schwerpunkt auf der Einfachheit der Datenübermittlung.[19]

Jenseits dieser Debatten zum Thema Datenübertragbarkeit trifft man jedoch auf die unterschiedlichsten Ansichten. Dabei sehen wir unter anderem – sogar von ein und demselben Stakeholder – zweierlei Forderungen: mehr Übertragbarkeit zu ermöglichen und gleichzeitig die Möglichkeiten einzuschränken, Daten mit Dritten zu teilen. Die zweite Forderung hören wir besonders oft in Zusammenhang mit unserer App-Plattform für Verbraucher (kurz „Plattform"). Damit sind u. a. auch die Technologien gemeint, die wir Entwicklern zur Verfügung stellen, sodass Nutzer ihre Facebook-Informationen mit der App und umgekehrt teilen können. Das bekannteste Plattformtool ist Facebook Login. Nutzer verwenden es nicht nur für die Anmeldung, sondern auch um ihre Informationen mit Apps von Dritten zu teilen.

Insbesondere im Zuge des Cambridge-Analytica-Vorfalls haben mehrere Stakeholder immer wieder eine Einschränkung der Daten gefordert, die über Facebook Login für Apps zugänglich werden. Außerdem sollten wir ihrer Meinung nach diese Apps strenger kontrollieren. Diesen Forderungen bedeuten, dass es einen Unterschied zwischen der Übertragung von Daten zwischen Plattformen und Apps einerseits und Übermittlungen andererseits gibt, die von „echter" Datenübertragbarkeit ermöglicht werden. Im Vergleich zwischen Facebook und der FTC aus dem Jahr 2019 werden beispielsweise Portabilität und andere Arten von Übertragungen unterschiedlich behandelt.[20]



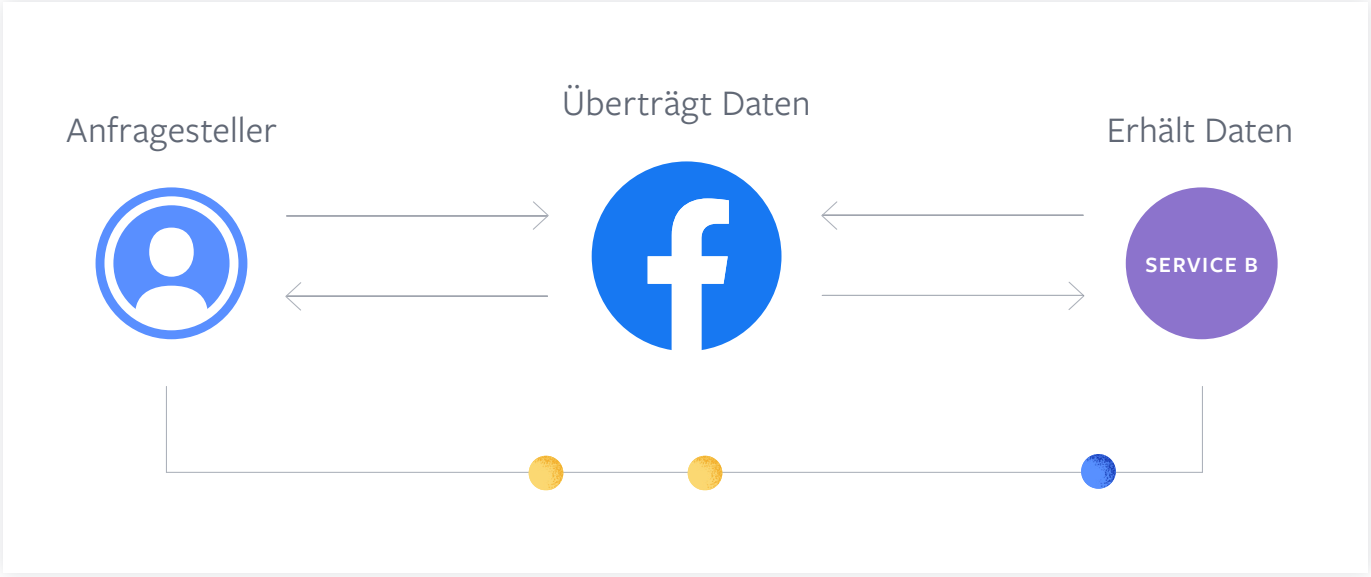
Gleichzeitig gibt es die Meinung, dass eben genau diese Datenübertragbarkeit den Cambridge-Analytica-Vorfall ermöglicht hat. Das heißt, auf Plattformen wie der unseren (und anderen wie iOS, Android, Twitter etc.) bestehen bereits Datenportabilitätsfunktionen, mit denen Nutzer der Plattform ihre Daten mit Apps teilen konnten.[21]

Diese Diskussionen werfen eine Frage auf: Wann ist eine Anfrage auf Datenübertragung eine Portabilitätsanfrage? Die Antwort ist ausschlaggebend, nicht zuletzt aufgrund der

gesetzlichen Rechte, die mit Portabilitätsanfragen einhergehen. Laut DSGVO muss Portabilitätsanfragen „ohne Behinderung“ nachgekommen werden. Dabei stellt sich die Frage, ob es Situationen gibt, in denen Anbieter eine Anfrage ablehnen, die angeforderten Daten einschränken oder verhindern können, dass Dritte die Daten nach der Übermittlung verwenden. Offensichtlich sind viele Stakeholder der Meinung, dass Plattformbetreiber für die Empfänger der Daten Nutzungseinschränkungen festlegen sollten. Dennoch bleibt die Frage offen, ob die Anbieter alternative Mechanismen zur Verfügung stellen müssen, für die keine Einschränkungen gelten. Falls ja, worin unterscheiden sich diese zwei Übertragungsarten?

Um diese Frage beantworten zu können, ist es wichtig zu verstehen, dass die meisten von Nutzern durchgeführten Übertragungen von Daten an Dritte sehr ähnlich sind. In der Regel sind drei Parteien beteiligt: der anfragende Nutzer, der für die Verarbeitung Verantwortliche und der Empfänger der Daten.[22]

Aus technischer Sicht besteht der erste Schritt bei der Datenübertragung darin, dass der Nutzer eine Anfrage stellt und das für die Verarbeitung verantwortliche Unternehmen veranlasst, seine Daten zu exportieren. Dieses Unternehmen übermittelt dann die betroffenen Daten entweder an den Anfragesteller (der die Daten nach Belieben nutzen oder an eine andere Partei weiterleiten kann) oder direkt an den Empfänger. Sobald der Empfänger die Daten erhalten hat, stehen sie dem Nutzer über den vom Empfänger angebotenen Dienst zu Verfügung.



Doch selbst wenn sich zwei Übertragungen aus technischer Sicht ähneln, können sich die Funktionsweisen unterscheiden. Ein Unterscheidungsmerkmal ist die Beziehung zwischen dem übertragenden Unternehmen und dem Empfänger-Unternehmen. Auch die unter Umständen geltenden Übertragungsregeln sind womöglich unterschiedlich. Zur Veranschaulichung kann man sich vorstellen, dass diese von Nutzern ausgehenden Übertragungen auf verschiedenen Punkten einer Skala liegen: je enger die Beziehung zwischen dem übertragenden Unternehmen

und dem Empfänger, umso mehr Einschränkungen gibt es (dabei lassen wir vorerst den Verwendungszweck der übertragenen Daten außen vor, denn damit befassen wir uns später). Wir können die Übertragungsarten in drei breitgefasste Kategorien einteilen:

1 Offene Übertragungen

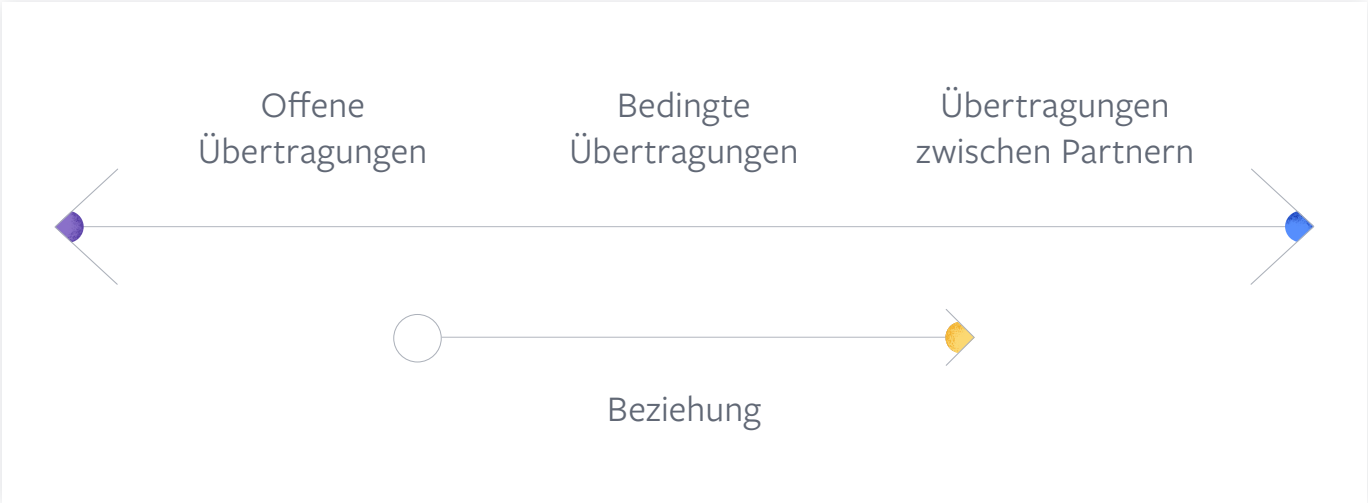
Anfragende Nutzer erhalten ihre Daten und können sie ganz ohne Behinderungen oder Einschränkungen an den Empfänger übermitteln. In diesem Fall kann entweder der Nutzer die Daten über sein eigenes Gerät (z. B. mit unserem Tool „Deine Informationen herunterladen“) an den Empfänger übertragen oder das für die Verarbeitung verantwortliche Unternehmen anweisen, die Daten direkt an den Empfänger zu senden. Abgesehen von der Zusammenarbeit bei der Übertragung der Daten besteht zwischen diesen beiden Unternehmen keine Beziehung. Dieses Szenario ähnelt am meisten dem in der DSGVO und in den Leitlinien der Datenschutzgruppe vorgesehenen Modell.

2 Bedingte Übertragungen

Anfragende Nutzer erhalten ihre Daten und können sie an Empfänger weiterleiten, die bestimmte von der anderen Partei festgelegte Bedingungen erfüllen. Zwischen den beiden Parteien gibt es keine Beziehung, und der Zweck der Zusammenarbeit besteht lediglich darin, der Nutzeranfrage nachzukommen. Dies ist, wie wir weiter unten sehen werden, ein gutes Beispiel dafür, wie wir uns Nutzeranfragen zur direkten Übertragung zwischen Anbietern vorstellen können. Das Data Transfer Project arbeitet schon an der Entwicklung der hierfür erforderlichen technischen Mittel.

3 Übertragungen zwischen Partnern

Anfragende Nutzer erhalten ihre Daten und leiten sie an einen Empfänger weiter. Sender und Empfänger unterhalten dabei eine fortlaufende Beziehung zur Ermöglichung solcher Übertragungen. Eventuell gelten bestimmten Bedingungen zur Datennutzung durch den Empfänger. Die Beziehung zwischen den beiden Parteien besteht in diesem Fall nicht nur, um den Portabilitätsanfragen von Nutzern nachzukommen, sondern auch um beispielswiese die von einer Partei angebotenen Funktionen in die Produkte der anderen Partei zu integrieren. Ein Beispiel für diese Kategorie sind die Übertragungen über die Facebook-



Wenn es um das Thema Datenübertragbarkeit geht, sollten diese Unterschiede zwischen den Übertragungskategorien berücksichtigt werden. Die Frage, die wir uns stellen müssen, lautet: Bei welcher Übertragungsart spielt das Recht auf Datenübertragbarkeit eine Rolle und welche Pflichten sollten je nach Modell die beteiligten Parteien erfüllen müssen? Offene Übertragungen kommen dem in der DSGVO und in anderen Quellen beschriebenen Konzept der Datenübertragbarkeit offensichtlich am nächsten, doch wie steht es mit bedingten Übertragungen, bei denen die für die Verarbeitung verantwortliche Partei einschränken kann, an welche Dritte die Daten übermittelt werden dürfen? Vertragen sich solche Einschränkungen mit dem Recht auf Datenübertragbarkeit? Gibt es überhaupt Fälle, in denen wir davon ausgehen können, dass Übertragungen zwischen Partnern (wie im Beispiel der Facebook Plattform) dem Konzept der Datenübertragbarkeit entsprechen?

Bisher haben unsere Diskussionen mit Stakeholdern gezeigt, dass die übertragende Partei einige grundlegende Einschränkungen zur Wahrung der Privatsphäre und des Datenschutzes bei der Datenübertragung vornehmen sollten – selbst wenn die Übertragung auf Nachfrage eines Nutzers geschieht. In späteren Abschnitten in diesem Paper werden wir jedoch sehen, dass die genauen Bedingungen noch geklärt werden müssen. Die auf Facebook Plattform geltenden Einschränkungen werden von einigen Personen als zu strikt und somit als nicht vereinbar mit dem Recht auf Datenübertragbarkeit eingestuft. Der kürzlich geschlossene Vergleich mit der FTC lässt darauf schließen, dass bestimmte Regulierungsbehörden zwischen Übertragungen ähnlich der Facebook Plattform und Portabilitäts-Übertragungen unterscheiden.[23] Wo genau die Linie zwischen diesen beiden Kategorien zu ziehen ist, wird in Zukunft die Unterscheidung zwischen Portabilität und anderen Übertragungsarten bestimmen.

FRAGE 2: WELCHE DATEN SOLLTEN ÜBERTRAGBAR SEIN?

Einer der wichtigsten Zwecke der Datenübertragbarkeit ist, den Nutzern die Kontrolle über ihre Daten zu überlassen. Doch was ist mit „ihre Daten“ eigentlich gemeint? Es leuchtet ein, dass Internetnutzer in der Lage sein sollten, Daten wie beispielsweise ihre hochgeladenen Fotos oder ihre Posts in sozialen Netzwerken von einem Ort an einen anderen zu übertragen. Auf welche anderen Daten sich dieses Recht auf Datenübertragbarkeit erstrecken soll, ist jedoch nicht ganz klar.

Sollten Internetnutzer solche Informationen exportieren können, die sie Anbietern während der Nutzung ihrer Funktionen bereitstellen, z. B. Suchverlaufsdaten, Standortdaten oder Aktivitätenprotokolle? Und wie sieht es mit Informationen aus, die der Anbieter anhand hochgeladener Daten oder dank Interaktionen mit dem Service gesammelt hat? Damit meinen wir beispielsweise aus Rückschlüssen erzeugte Daten zum Musikgeschmack oder zu relevanten Ereignissen und Anzeigen sowie Rückschlüsse, die auf möglicherweise betrügerische Aktivitäten hindeuten.

Sowohl die DSGVO als auch die Leitlinien der Datenschutzgruppe empfehlen, Einschränkungen festzulegen für die vom Recht auf Datenübertragbarkeit betroffenen Informationen. Gemäß der DSGVO fallen in den Anwendungsbereich des Rechts auf Datenübertragbarkeit alle Daten, die eine Person einem Datenverantwortlichen „bereitgestellt“ hat.[24] Die Empfehlung der Datenschutzgruppe lautet, dass Personen solche Daten übertragen können sollen, die sie einem Anbieter aktiv bereitgestellt haben oder die der Anbieter durch die Beobachtung des

Nutzerverhaltens erzeugt hat. Davon ausgeschlossen sind solche Informationen, die der Anbieter aus Rückschlüssen basierend auf dem Verhalten erzeugt hat.[25]

In puncto Nutzungsdaten stellt sich außerdem diese Frage: Inwiefern beeinflussen die Datenspeicherungspraktiken der Anbieter die Wahl der Datenkategorien, die portabel sein sollen? Es scheint weithin unumstritten, dass Anbietern keine Pflicht zur Datenspeicherung für Portabilitätszwecke auferlegt werden soll. Das hat zur Folge, dass bestimmte Daten gar nicht portabel sein können, da sie zum Zeitpunkt der Anfrage nicht mehr vorhanden sind. Wie sieht es aber mit solchen Daten aus, die zwar aus technischer Sicht verfügbar sind, aber bald gelöscht werden? Sollten Anbieter auch für den Export dieser Daten Tools entwickeln?

Außerdem stellt sich die Frage, ob es bestimmte Fälle gibt, in denen das Interesse des Nutzers am Datenexport einen komplexen Exportvorgang für Portabilitätszwecke überhaupt rechtfertigt? Die von einem Dienst erfassten Daten eines Nutzers umfassen beispielsweise alle Seiten oder Inhalte, die die Person innerhalb eines bestimmten Zeitraums aufgerufen hat, sowie alle angeklickten Links und erhaltenen Benachrichtigungen. Viele Anbieter führen auch Protokolle, in denen diese Informationen für einen bestimmten Zeitraum festgehalten werden. Diese Daten in ein portables Format zu verwandeln, wäre gar nicht so einfach. Und die Vorteile, die der Nutzer aus dem Datenexport zieht, lägen auch nicht immer auf der Hand. Wäre es wirklich nützlich, eine Liste mit allen auf Facebook innerhalb eines bestimmten Zeitraums angeklickten Links exportieren zu können? Oder ein Archiv, in dem alle im News Feed angesehenen Anzeigen enthalten sind?

Angesichts der Tatsache, dass Datenübertragbarkeit ein Mittel ist, um den Wettbewerb und die Entwicklung neuer Dienste zu fördern, sollten wir uns mit diesen Fragen auseinandersetzen und dabei den damit verbundenen betrieblichen Mehraufwand berücksichtigen, den auch Unternehmen mit weniger Ressourcen als Facebook betreiben müssten. Von diesem Standpunkt aus gesehen scheint es offensichtlich, dass die Pflichten der Anbieter bei der Freigabe von Daten, die durch Beobachtung des Nutzerverhaltens erzeugt wurden, eingeschränkt werden sollten. Um bestimmen zu können, wie diese Einschränkungen auszusehen haben und für welche Anbieter sie gelten sollen, müssen die Datenspeicherfristen und das Verhältnis zwischen den Vorteilen für die Nutzer und der zusätzlichen Arbeitslast für Anbieter einbezogen werden.[26] Wie dieses Abwiegen genau erfolgen und wer es durchführen soll, ist eine weitere zu beantwortende Frage.

FRAGE 3: WESSEN DATEN SOLLTEN ÜBERTRAGBAR SEIN?

Das Recht auf Datenübertragbarkeit ist ein Mittel, dass es Nutzern ermöglicht, ihre Daten zu kontrollieren. Doch wie sieht die Vorgehensweise in Situationen aus, in denen eine Person solche Daten übertragen möchte, die teilweise einer anderen Person gehören? Was wäre also, wenn Person A ihre Fotos von einem Dienst an einen anderen übertragen möchte, sich jedoch unter den Fotos auch Bilder von Person B befinden? Welche Kontrollmöglichkeiten hat Person B in diesem Szenario? Oder aber, wenn eine Person die Kontakte aus ihrem Adressbuch oder eine Liste mit den Geburtstagen dieser Kontakte an einen neuen Dienst übermitteln möchte? Sollten in diesem Fall die Kontakte, also die Personen, deren Daten mit dem neuen Dienst geteilt würden, mitbestimmen dürfen?

Diese Beispiele zeigen, dass es in bestimmten Fällen gar nicht so einfach ist zu bestimmen, wessen Daten bei einer Portabilitätsanfrage übermittelt werden sollen.[27] Dies trifft insbesondere auf Facebook zu, denn eine der Hauptideen hinter dieser Plattform ist es, dass sich die Nutzer miteinander verbinden und gemeinsame Erlebnisse schaffen. Die Übertragung von Kontakt- oder sonstigen Daten von Freunden könnte also schwerwiegende datenschutzrechtliche Probleme mit sich bringen.[28]

Es wurden einige Vorschläge gemacht, dass im Falle einer Portabilitätsanfrage nur solche Daten übertragen werden sollten, die der anfragende Nutzer „besitzt".[29] Schließlich können sie mit ihren eigenen Daten, die sie einem Dienst bereitstellen, tun und lassen, was sie möchten – sie also auch an ein anderes Unternehmen übermitteln. Umgekehrt sollten Daten, die nicht Eigentum des anfragenden Nutzers sind, nicht portabel sein.

Daten als „Eigentum" zu klassifizieren, wird von manchen Personen als kontrovers betrachtet und es führt zu weiteren Fragen, die sich nicht nur auf das Thema Datenübertragbarkeit beschränken.[30] In der Praxis gibt es viele Arten von Informationen, die nicht nur einer Person gehören. Wenn Sie beispielsweise meine Telefonnummer in Ihrem Adressbuch gespeichert haben, gehört diese Telefonnummer dann Ihnen? In der EU beispielsweise spielt es beim Datenschutz (einem Grundrecht) keine Rolle, wem die betroffenen Daten gehören.[31]

Um bestimmen zu können, wessen Daten im Rahmen einer Portabilitätsanfrage zur Verfügung gestellt werden sollen, müssen wir uns auch damit befassen, wer die Daten bereitgestellt hat, ob der Anbieter die Daten einem bestimmten Nutzer zugeordnet hat und welchen Vertraulichkeitsgrad die Daten haben. Nehmen wir zur Veranschaulichung folgendes Szenario:

Person A lädt ein Video hoch, in dem sie selbst und drei Freunde (Personen B, C und D) zu sehen sind. Sie kennzeichnet die Personen auf keinerlei Weise (z. B. durch Taggen), sodass der Anbieter sie nicht identifizieren kann. Auf den ersten Blick scheint es unbestreitbar, dass Person A das Recht haben sollte, dieses Video an einen neuen Dienst zu übermitteln. Doch welche Rechte stehen den Personen B, C und D in Bezug auf dieses Video zu? Und welche der beiden Parteien, also Person A oder der Dienstanbieter, ist am ehesten in der Position, die Rechte dieser Personen einzufordern?

Sehen wir uns jetzt ein leicht abgewandeltes Szenario an: Person A lädt ein Video hoch und kennzeichnet darin die Personen B, C und D, die den Dienst ebenfalls nutzen. In diesem Szenario ist der Dienstanbieter möglicherweise berechtigt, die Personen B, C und D über die Portabilitätsanfrage zu informieren. Und nachdem er dies getan hat, sollten die anderen Personen Person A davon abhalten können, das Video zu übertragen?

Wie würden die Antworten lauten, wenn es sich statt um ein Video um die E-Mail-Adressen aus dem Kontaktbuch von Person A handelte? Sollte es einfacher oder schwieriger sein, solche Informationen anstelle von Videos zu übertragen? Und wo wir bereits beim Thema sind, wie sieht es mit den eigentlichen E-Mails aus, die ein Nutzer eventuell an einen neuen E-Mail-

Anbieter übermitteln möchte (beispielsweise bei einem Wechsel von Gmail zu Outlook)?

Wir glauben, dass ein Multifaktor-Ansatz, bei dem die obigen Fragen und Faktoren berücksichtigt werden, anderen Ansätzen vorzuziehen ist, bei denen der Fokus auf dem Dateneigentum liegt. Um entscheiden zu können, welche Daten portabel sein sollten, müssen wir wissen, wie wir diese Faktoren einbeziehen können – und dafür sind noch viele Diskussionen und Orientierungshilfen nötig.[32]

Bei der Frage, wessen Daten im Rahmen einer Portabilitätsanfrage übertragen werden sollten, verweisen Kommentatoren oftmals auf den „Social Graph" einer Person. Dabei handelt es sich um eine Übersicht der Verbindungen eines Nutzers mit anderen Personen und Unternehmen auf der Plattform des Dienstes. Einige Befürworter des Rechts auf Datenübertragbarkeit forderten, dass Dienstanbieter wie wir unseren Nutzern ermöglichen müssen, sowohl ihre eigenen Daten als auch die Daten aus ihrem Social Graph zu übertragen, da letztere unter anderem auch von anderen Social-Networking-Unternehmen genutzt werden können, um neue Produkte zu entwickeln.[33] Sie begründeten diese Forderung damit, dass der Wechsel von einem sozialen Netzwerk zu einem anderen ohne die Social-Graph-Daten für Nutzer nicht reibungslos funktionieren würde.

Wir glauben, dass beide Lager starke Argumente haben: Wenn sich das Recht auf Datenübertragbarkeit auch auf Social-Graph-Daten erstreckt, profitieren sowohl Innovation als auch Wettbewerb davon, doch dies würde auch viele wichtige Fragen zum Datenschutz aufwerfen. Dabei ist die wichtigste Frage, ob wir Wege finden können, diese Übertragung so umzusetzen, dass die Privatsphäre aller betroffenen Personen gewahrt wird. Im nächsten Abschnitt gehen wir näher auf diese Fragen ein.

FRAGE 4: WIE SOLLTEN WIR DATEN IM RAHMEN DER DATENÜBERTRAGBARKEIT SCHÜTZEN?

Bei den Fragen 1 bis 3 haben wir uns mit den Umständen vor der Datenübertragung befasst. Sobald wir wissen, (1) dass es sich um eine vom Nutzer angeforderte Datenübertragung handelt, (2) welche Arten von Daten übertragen werden sollen und (3) wessen Daten übertragen werden sollen, müssen wir in Erfahrung bringen, wie wir das Recht auf Datenübertragbarkeit bei gleichzeitigem Schutz der Privatsphäre umsetzen können.

Es gibt zwar Gesetze, die die Übertragung von Daten und das Recht auf Übertragbarkeit regeln, doch nur wenige Orientierungshilfen zum Schutz der Privatsphäre bei solchen Übertragungen. Stakeholder haben Bedenken wegen den Risiken für Privatsphäre und Datenschutz geäußert, die von Übertragungstools ausgehen, sowie wegen mangelnder Vorgaben von Politikern und Gesetzgebern dazu, was von den für die Verarbeitung verantwortlichen Unternehmen erwartet wird.[34]

Es ist besonders wichtig, bei diesen Punkten Klarheit zu schaffen, denn nur wenn sich die Nutzer darauf verlassen können, dass ihre Daten während und nach der Übertragung verantwortungsvoll gehandhabt werden, erfüllt das Recht auf Datenübertragbarkeit seine Funktion – den Nutzern mehr Kontrolle über ihre Daten zu geben. Bei der Suche nach Antworten auf diese Fragen rund um Datenschutz und Datenübertragbarkeit hat es sich für uns als hilfreich erwiesen, die Handlungen zwischen dem für die Verarbeitung Verantwortlichen und

folgenden Parteien einzubeziehen: (1) anfragende Nutzer, (2) nicht anfragende Nutzer, deren Daten von der Übertragung betroffen sind, und (3) Empfänger der Daten.

1 Anfragende Nutzer

Da es beim Recht auf Datenübertragbarkeit darum geht, den Nutzern mehr Kontrolle über ihre Daten zu geben, scheint es naheliegend, dass die für die Verarbeitung Verantwortlichen den Nutzern helfen, fundierte Entscheidungen zur Übertragung ihrer Daten zu treffen. Dafür ist es erforderlich, sicherzustellen, dass die anfragenden Nutzer genau wissen, an was für ein Unternehmen sie ihre Daten übermitteln. Politiker, Gesetzgeber und andere Stakeholder haben bisher jedoch versäumt, eine klare Antwort darauf zu geben, welche Informationen eine Person haben sollte und wie bzw. von wem diese bereitgestellt werden sollten.

In der Beurteilung des in der DSGVO begründeten Rechts auf Datenübertragbarkeit der Datenschutzgruppe haben die Mitglieder erklärt, dass zwar die Nutzer dafür verantwortlich sind, alle Sicherheitsmaßnahmen zu ergreifen, die bei der Übertragung an den Datenempfänger zum Schutz der Daten erforderlich sind, dass aber auch das für die Übermittlung verantwortliche Unternehmen die betroffene Person auf die richtigen Sicherheitsmaßnahmen aufmerksam machen muss.[35]

Im Vergleich dazu hat die Personal Data Protection Commission von Singapur in einem Bericht vorgeschlagen, dass der Verantwortliche einen Schritt weitergehen und dem betroffenen Nutzer auch diese Informationen zur Verfügung stellen sollte: wie der Empfänger die Nutzerdaten verwenden wird, Einzelheiten zum neuen Produkt oder Dienst, zu dem der Nutzer seine Daten überträgt, sowie Informationen zur Laufbahn, zum Ruf und zu den Datenverwaltungs- und -schutzpraktiken des Empfängers.[36] In einem im Mai 2019 veröffentlichten Konsultationsbericht riet die Commission außerdem dazu, einen für alle Unternehmen verbindlichen Verhaltenskodex zu entwerfen, in dem sie aufgefordert werden, den Nutzern alle relevanten Informationen mitzuteilen.[37]

Diese Vorschläge bilden eine gute Ausgangsbasis, doch unserer Meinung nach ist noch lange nicht ausreichend geklärt, wenn ja, welche Informationen den betroffenen Personen zur Verfügung gestellt werden sollten, wer diese Informationen bereitstellen sollte und in welchem Format.

2 Nicht anfragende Nutzer

Bei einigen Portabilitätsanfragen könnten auch die Daten von anderen Personen als dem Antragsteller betroffen sein (also den sogenannten nicht anfragenden Nutzern). Wie bereits zuvor erwähnt, wird stark darüber diskutiert, ob die Daten dieser Nutzer überhaupt portabel sein sollten. Falls ja, müssen die Dienstanbieter das Recht auf Privatsphäre dieser Nutzer gewährleisten.

Einige Stakeholder haben vorgeschlagen, Einwilligungsfunktionen oder ähnliche Mittel einzuführen, sodass sich Nutzer gegenseitig die Zustimmung zum Export der bei einem bestimmten Dienst gespeicherten Daten geben können. Beispielsweise könnte so Nutzer A Nutzer B erlauben, die Daten von Nutzer A an einen neuen Verantwortlichen zu übertragen.[38] Da diese mögliche Lösung der Bereitstellung von Einwilligungsoptionen oft diskutiert wird, möchten wir näher auf dieses Thema eingehen und herausfinden, ob die Dienste nicht

anfragenden Nutzern hinreichend Mitentscheidung und Kontrolle geben können, und falls ja, wie sie das bewerkstelligen könnten. Wäre das Recht auf Übertragbarkeit zu stark eingeschränkt, wenn eine Einwilligung erforderlich wäre? Falls nein, wie könnte die Einwilligung eingeholt werden? Sollten nicht anfragende Nutzer die Möglichkeit haben, bei jeder einzelnen Anfrage von Freunden zu bestimmen, ob diese ihre Daten mit einer App teilen dürfen? Könnte dies zu einer Benachrichtigungsabnutzung führen?[39] Würde es sich für Nutzer eines bestimmten Dienstes lohnen, die relevanten Einstellungen immer auf „Ein" zu setzen, sodass ihre Freunde (oder Kontakte) alle oder bestimmte Kategorien von personenbezogenen Daten mit Dritten teilen können? Und welche Maßnahmen müssten für Personen eingeführt werden, die die Dienste nicht nutzen, deren Informationen aber an diese übertragen werden?

a. Übertragung von Social-Graph-Daten

Wie zuvor bereits erwähnt, sind viele Stakeholder der Meinung, dass die Übertragung der Social-Graph-Informationen (wie z. B. Kontaktlisten) jungen Social-Networking-Unternehmen bei der Entwicklung innovativer, neuer Dienste zugute kommt.[40] Darüber, wie der Export dieser Daten genau aussehen soll, wurden bereits viele Diskussionen geführt und auch einige konkrete Vorschläge gemacht. Einer der wohl vielversprechendsten Vorschläge ist die Idee, die einmaligen Nutzer- und Kontaktdaten in einem kryptografisch verschlüsselten (oder „gehashten") Format zu exportieren.[41]

Bei dieser Lösung werden die Nutzerkennungen (z. B. die E-Mail-Adressen) verborgen, doch die Social-Graph-Informationen der betroffenen Nutzer können mit einigen Ausnahmen vom Empfänger dennoch wiederhergestellt werden. Dies könnte eine Möglichkeit sein, um die mit der Übertragung der Daten von Freunden an Dritte verbundenen Datenschutzprobleme anzugehen – indem nicht betroffene personenbezogene Daten nicht offengelegt werden. Einige Experten sind jedoch der Meinung, dass durch die für diese Lösung erforderliche Zusammenarbeit auf technischer Ebene bislang unerwartete Privatsphäre- und Datenschutzrisiken sowie Compliance-Probleme auftreten könnten.[42] Nachfolgend beschäftigen wir uns mit zwei stark diskutierten Ansätzen zum Teilen gehashter Kontaktdaten und den möglicherweise dadurch entstehenden Herausforderungen.

Zunächst teilt ein Anbieter eine Liste gehashter Kennungen, die mit dem anfragenden Nutzer und dessen Kontakten übereinstimmen. Dies geht am einfachsten, indem er gehashte Versionen des Namens (dieser ist womöglich nicht einzigartig) oder der E-Mail-Adresse eines Kontakts teilt. Wenn sowohl Nutzer A als auch Nutzer B mit Nutzer C befreundet sind und gehashte Versionen ihrer Kontaktlisten einem Dienst zur Verfügung gestellt haben, weiß dieser Dienst, dass Nutzer A und Nutzer B mit Nutzer C verbunden sind. Sofern Nutzer C seine Daten nicht an den Dienst übermittelt hat, erfährt der entsprechende Anbieter jedoch nichts weiter über Nutzer C.

Eine weitere Möglichkeit besteht darin, solche Kennungen zu übermitteln, die nicht auf den Nutzer zurückführen, sondern auf die Beziehung zwischen den Nutzern. In diesem Fall kann der Dienst des neuen Anbieters anhand der Kontaktdaten von Nutzer A und Nutzer B, die beide mit Nutzer C befreundet sind, nicht wie im anderen Beispiel schlussfolgern, dass sich diese drei Nutzer kennen. Der Grund hierfür ist, dass sich die Kennung der Beziehung zwischen Nutzer A und Nutzer C von der Kennung der Beziehung zwischen Nutzer B und Nutzer C unterscheidet. Sollte Nutzer C jedoch beschließen, seine Kontaktliste mit diesem

Anbieter zu teilen, überträgt er so auch die Kennungen der Beziehung zu Nutzer A und Nutzer B. Nach einem Abgleich der Kennungen weiß der Anbieter dann, dass Nutzer A, B und C befreundet sind.

Beide Ansätze bergen Risiken, die weiter zu diskutieren sind. Beim ersten Ansatz kann der Empfänger schon anhand der Informationen zur Beziehung zwischen den Nutzern A, B und C weitere Daten über Nutzer C in Erfahrung bringen. Wenn beispielsweise Nutzer A und Nutzer B Arbeitskollegen sind oder derselben politischen Partei angehören, kann der Datenempfänger diese Informationen auch mit Nutzer C in Verbindung bringen und mit wenigen weiteren Daten die Identität von Nutzer C aufdecken. Dieses Risiko besteht beim zweiten Ansatz zwar nicht, doch der Nutzen bei dieser Vorgehensweise ist für den Empfänger beschränkt, denn die Beziehung zwischen Nutzern ist für den Dienst nur dann sichtbar, wenn beide ihre Informationen teilen.

Eine weitere Herausforderung beim Teilen von Social-Graph-Informationen besteht darin, ein einheitliches Datenmodell zu wählen, das für alle Dienste geeignet ist und sich jeder Situation anpasst. Es gibt beispielsweise soziale Netzwerke, in denen Nutzer nur ein Konto haben können, und andere Netzwerke, in denen ein Nutzer mehrere Konten erstellen kann. Wenn also Nutzer A mit nur einem der Konten von Nutzer B verknüpft ist, wie sollte dann diese Beziehung beim Teilen von Kontaktlisten mit einem Dienst gehandhabt werden, bei dem pro Nutzer nur ein Konto erlaubt ist? Ein weiteres Risiko entsteht dann, wenn Nutzer ihre Daten aus einem sozialen Netzwerk, in dem es nicht erforderlich ist, seinen echten Namen anzugeben, in ein anderes Netzwerk übertragen, das Echtnamen erfordert. Der Empfänger (oder auch der anfordernde Nutzer) wäre in der Lage, anhand von gemeinsamen Merkmalen eine Verknüpfung zwischen einem pseudonymen Nutzer und der realen Person aus der Kontaktliste herzustellen.

Hinzu kommt, dass das Teilen von Social-Graph-Daten zunehmend komplizierter wird, da die Menge der sozialen Interaktionsebenen immer weiter zunimmt. Gehen wir einmal davon aus, dass ein Beitrag von Nutzer A, den Nutzer B kommentiert oder mit „Gefällt mir“ markiert hat, in ein neues soziales Netzwerk übertragen wird. Unter welchen Umständen sollte der Kommentar sichtbar sein, wer sollte ihn sehen können und wie sollte Nutzer B auf der neuen Plattform identifiziert werden, wenn überhaupt? Die Antworten auf all diese Fragen hängen nicht nur von den Kontrollfunktionen ab, die den Nutzern des neuen Dienstes zur Verfügung stehen, sondern auch davon, wie die Kontakte an den neuen Anbieter übertragen und von ihm identifiziert werden.

3 Mögliche Empfänger von personenbezogenen Daten

Im Laufe des vergangenen Jahres haben viele Stakeholder von Dienstanbietern gefordert, zusätzliche Anstrengungen zu unternehmen, um dem Datenmissbrauch durch bestimmte Dritte vorzubeugen.[43] Doch wie sollten diese Anstrengungen im Kontext der Datenübertragbarkeit aussehen?

Nur wenige Experten haben sich hierzu geäußert. In den Leitlinien der Datenschutzgruppe zur DSGVO steht lediglich: „der Verantwortliche hat all die Sicherheitsmaßnahmen zu ergreifen, die erforderlich sind, um eine sichere Übertragung der personenbezogenen Daten (z. B. durch Verschlüsselung) an den richtigen Bestimmungsort (z. B. durch Verwendung zusätzlicher Authentifizierungsangaben) zu gewährleisten“.[44] In den Leitlinien wird also empfohlen,

Maßnahmen zur Risikominimierung wie zusätzliche Authentifizierungsangaben einzusetzen oder die Übertragung auszusetzen bzw. anzuhalten, wenn es Anzeichen dafür gibt, dass ein Konto kompromittiert wurde. Es ist allerdings auch vermerkt: „solche Sicherheitsmaßnahmen dürfen ihrem Wesen nach kein Hindernis darstellen und Nutzer nicht davon abhalten, ihre Rechte auszuüben[.]“[45]

Abgesehen von diesen grundlegenden Orientierungshilfen macht die Datenschutzgruppe keine weiteren Vorschläge dazu, was Dienstanbieter gegen Datenmissbrauch durch Dritte unternehmen könnten. Stakeholder haben in Gesprächen mit uns immer wieder darauf hingewiesen, dass die für die Verarbeitung Verantwortlichen die Einführung zusätzlicher Kontrollmaßnahmen in Erwägung ziehen sollten, um so sicherzustellen, dass die Daten vom Empfänger in Übereinstimmung mit den Privatsphäre- und Datenschutzvorschriften verarbeitet werden. Sie schlugen beispielsweise vor, es für Datenempfänger verpflichtend zu machen, (1) den Verwendungszweck und die Verarbeitungsmethode der gemäß der Portabilitätsanfrage erhaltenen Daten offenzulegen und (2) die Einhaltung aller anwendbaren Gesetze und Datenschutzvorschriften zu bestätigen. Andere sind der Meinung, dass die für die Verarbeitung Verantwortlichen die Verarbeitung der Daten durch den Empfänger überwachen und bei Verstößen gegen die anwendbaren Gesetze und Datenschutzvorschriften Maßnahmen gegen sie einleiten sollten. Das Problem ist nur, dass eine solche Überwachung wenn überhaupt nur schwer umsetzbar und offenbar gemäß den Anforderungen an die Datenübertragbarkeit in der DSGVO nicht erforderlich ist.

Andererseits sind einige Stakeholder darüber besorgt, dass solche Voraussetzungen nicht mit dem Prinzip „echter“ Datenübertragbarkeit vereinbar sind. Wenn Nutzer ihre Daten an ein bestimmtes Unternehmen übertragen möchten, darf sich der bisherige Anbieter dann wirklich einmischen und vom Empfänger Einzelheiten zur Datenverarbeitung und zur Einhaltung der Gesetze fordern? Und was geschieht in Fällen, in denen der alte und der neue Datenverantwortliche die Gesetze jeweils anders auslegen? Hat dann der neue Verantwortliche das letzte Wort? Die Due-Diligence-Pflichten des für die Verarbeitung verantwortlichen Unternehmens haben ihre Grenzen und beschränken sich in der Regel auf die sichere Durchführung der Übertragung. Werden diese Grenzen überschritten, könnte dadurch möglicherweise das Recht der Nutzer eingeschränkt werden, zu Wettbewerbern zu wechseln.

Einigen Vorschlägen zufolge könnte man mit einem Zertifizierungssystem diese Einwände ausräumen.[46] Durch die Einführung eines solchen Systems könnte man es potenziellen Empfängern von Nutzerdaten ermöglichen, sich von einer unabhängigen Zertifizierungsstelle akkreditieren zu lassen, um so zu beweisen, dass sie die Datenschutz- und-verarbeitungsstandards aus der DSGVO oder anderen Vorschriften einhalten.[47] Für die Identifizierung solcher Unternehmen kämen Datenschutzsiegel und -prüfzeichen zum Einsatz, die zum Nachweis dienen, dass die Unternehmen für das Empfangen von Daten berechtigt sind. Die Aufgabe der unabhängigen Stelle (möglicherweise in Zusammenarbeit mit den zuständigen Regulierungsbehörden) wäre es, die Einhaltung dieser Standards zu überwachen und Unternehmen, die dagegen verstoßen, die Zertifizierung abzuerkennen.

Es gibt eine weitere mögliche Lösung, die für die Datenübertragbarkeit die Erstellung eines Verhaltenskodex vorsieht, dessen Einhaltung von einer unabhängigen Organisation überwacht werden soll. Dieser Vorschlag ist vor allem für Unternehmen aus solchen Ländern attraktiv,

in denen es keine umfassenden Datenschutzgesetze gibt.[48] Im Verhaltenskodex könnte beispielsweise festgelegt werden, dass Unternehmen bestimmte Privatsphäre- und Datenschutzkontrollen einführen müssen, bevor sie die Daten eines Nutzers, der eine Portabilitätsanfrage gestellt hat, empfangen dürfen. Die unabhängige Organisation wäre dafür zuständig, die Durchsetzung der Vorschriften aus dem Kodex zu überwachen und möglichen Verstößen nachzugehen. Es stellt sich jedoch eine wichtige Frage: Welche Folgen gäbe es für Unternehmen, die sich zwar der Einhaltung des Kodex verschrieben haben, aber gegen die Vorschriften verstoßen, oder die den Kodex gar nicht erst akzeptieren? Selbst wenn ein Nutzer seine Daten per Portabilitätsanfrage an einen solchen Dienst übertragen will, muss dem nachgekommen werden. Doch die Information über Nichteinhaltung des Kodex (oder über die Verweigerung, diesen zu akzeptieren) ist ein klares Anzeichen dafür, wie in dem jeweiligen Unternehmen der Schutz der Privatsphäre und der Daten von Nutzern gehandhabt wird.

FRAGE 5: WELCHE PARTEI TRÄGT NACH DER ÜBERTRAGUNG DIE VERANTWORTUNG UND HAFTET FÜR MISSBRAUCH UND UNZUREICHENDEN SCHUTZ DER DATEN?

Sowohl Nutzer als auch Dienstanbieter müssen genau wissen, wer vor, während und nach der angeforderten Übertragung von Nutzerdaten für die Verarbeitung und den Schutz verantwortlich ist. Der Meinung einiger Regulierungsbehörden zufolge könnte die Verantwortung auch nach bestimmten angeforderten Übertragungen bei Plattformbetreibern wie Facebook liegen. Doch gilt das auch bei Portabilitätsanfragen?

In den Leitlinien der Datenschutzgruppe zum Recht auf Datenübertragbarkeit, das in der DSGVO begründet ist, steht klar geschrieben, wer die Verantwortung trägt, wenn ein Dienstanbieter auf Anfrage eines Nutzers dessen Daten an eine andere Partei überträgt.[49] Bei der Übertragung werden nicht nur Daten verschoben, sondern auch die Verantwortung und Haftung. Vor und während des Vorgangs ist der aktuelle Dienstanbieter dafür verantwortlich, der Anfrage des Nutzers nachzukommen, die Daten auf sicherem Weg an den richtigen Empfänger zu senden und alle damit verbundenen Risiken zu minimieren. Die Pflicht des Empfängers ist es, sicherzustellen, dass ausschließlich für den Dienst erforderliche und relevante Daten übertragen werden.

Sobald die Übertragung abgeschlossen ist, trägt der übermittelnde Dienstanbieter keine Verantwortung mehr für die Verarbeitung der Daten durch die betroffene Person oder den Empfänger (schließlich wählt die betroffene Person den Empfänger aus und der Anbieter befolgt nur ihre Anweisungen). Laut der Datenschutzgruppe liegt die Verantwortung dann also beim Empfänger. Es ist seine Aufgabe, die personenbezogenen Daten gemäß den Vorschriften der DSGVO zu verarbeiten und zu schützen.

Die Personal Data Protection Commission von Singapur schlägt in ihrem Diskussionspapier ein Haftungsmodell vor, das das für die Verarbeitung verantwortliche Unternehmen von jedweder Haftung für Schäden freispricht, die aufgrund des Datenmissbrauchs durch den Empfänger entstehen. Sie erachtet dieses Modell als angemessen, da es schier unmöglich wäre, alle potenziellen Empfänger zu überprüfen. In dem Papier steht außerdem, dass der für die Verarbeitung Verantwortliche nicht für Ansprüche bezüglich der Richtigkeit und Qualität der übertragenen Daten haftbar zu machen ist, sofern nicht nachgewiesen werden kann, dass

die Daten in dessen Obhut beschädigt wurden.[50] Im neuesten Konsultationspapier der Commission wird das Thema Haftung zwar nicht besprochen, doch die Verantwortung des für die Übertragung Verantwortlichen nach Abschluss des Prozesses eingeschränkt. Demzufolge ist diese Partei nur dafür zuständig, zu überprüfen, ob die Daten erhalten wurden, und eventuelle Fragen zu den Daten zu beantworten.[51]

Ganz offensichtlich gibt es aber auch Fälle, in denen Politiker und Mitarbeiter der zuständigen Aufsichtsbehörden die Verantwortung selbst nach der Übertragung beim übertragenden Unternehmen sehen. Um diese Meinungen mit denen der Datenschutzgruppe und der Personal Data Protection Commission zu vereinheitlichen, muss die genaue Art der Übertragung bestimmt werden, also ob es sich um eine offene, bedingte oder eine Übertragung zwischen Partnern (siehe Abschnitt II. A.) handelt. Anhand dieser Information können die Pflichten des Dienstanbieters einfacher geklärt werden. Sollten beispielsweise Anbieter bei Übertragungen zwischen Partnern (wie z. B. im Fall der Facebook-Plattform) mehr Verantwortung tragen, da die Beziehung zur empfangenden Partei enger ist und der Zweck der Übertragung über die Erfüllung der Nutzeranfrage hinausgeht?

Bei offenen Übertragungen wäre es womöglich ausreichend, wenn der Dienstanbieter den Nutzern dabei hilft, selbst die Verantwortung für die mit der Übertragung verbundenen Risiken zu übernehmen. Und nachdem sie abgeschlossen wurde, ist allein der Empfänger für den Schutz der Daten verantwortlich. Dienstanbieter haben die Option, Tools einzuführen, die den Nutzern die Sicherheitsrisiken aufzeigen und ihnen die Verwendung von Protokollen für die heruntergeladenen Daten erklären. Außerdem könnten sie ihren Nutzern Tipps geben, wie sie herausfinden können, ob der Empfänger für Datenmissbrauch oder unzulängliche Sicherheitsmaßnahmen bekannt ist. Einige Tipps könnten sein, die Authentizität des Empfängers zu überprüfen (also dass es wirklich das Unternehmen ist, das es zu sein ausgibt), die Sicherheitsmaßnahmen auf der Website des Empfängers zu prüfen (z. B. ob sie das Protokoll HTTP oder HTTPS verwendet), das Gerät während des Datendownloads zu sichern (z. B. kein öffentliches WLAN-Netzwerk zu nutzen) und die Richtlinien des Empfängers auf Angemessenheit zu überprüfen (z. B. in der Datenschutzlinie nachzulesen, ob das Unternehmen die erhaltenen Daten weiterverkauft).

Die Vorgehensweise bei bedingten Übertragungen könnte sein, dass der Dienstanbieter vor der Übertragung eine Zertifizierungsbestätigung vom Empfänger anfordert, die von einer Normungsorganisation ausgestellt wurde. Alternativ könnte der Empfänger bestätigen, dass er an einen relevanten Verhaltenskodex gebunden ist oder die Daten in Übereinstimmung mit den anwendbaren Gesetzen und Datenschutzvorschriften verarbeitet. Nachdem der Empfänger die Zertifizierung präsentiert bzw. die erforderlichen Zusicherungen gemacht hat, würde der übertragende Anbieter von jeglicher Verantwortung (und Haftung) für anschließend entstandene Probleme freigestellt.

Bei Übertragungen zwischen Partnern wäre es angebracht, dem für die Verarbeitung Verantwortlichen selbst nach Abschluss der Übertragung ein gewisses Maß an Verantwortung zuzusprechen. Sofern möglich sollte diese Partei selbst nach Ende des Übertragungsprozesses die Verarbeitung der Nutzerdaten durch den Empfänger überwachen.

Zu guter Letzt bleibt die Frage, wer die Verantwortung für Daten einer anderen Person trägt, die im Rahmen einer Portabilitätsanfrage ebenfalls übermittelt werden. In den Leitlinien der

Datenschutzgruppe steht, dass bei der Übertragung von Datensätzen, die die personenbezogenen Daten anderer Personen enthalten, der anfordernde Nutzer auch für die Verarbeitung dieser Daten verantwortlich ist (soweit die Art der Verarbeitung nicht vom Datenverantwortlichen bestimmt wird), es sei denn die Daten sind Gegenstand eines rein häuslichen oder privaten Zusammenhangs.[52] Indem den anfordernden Nutzern bei solchen Übertragungen auch Verantwortung (und Haftung) auferlegt wird, könnte das Nutzerinteressente an der Übermittlung von Daten im Allgemeinen und an Social-Graph-Informationen im Besonderen abgeschreckt werden. Wäre es vielleicht effektiver, die Haftung der anfordernden Nutzer auf solche Fälle zu beschränken, in denen ihnen unvernünftiges oder fahrlässiges Verhalten nachgewiesen werden kann, wie beispielsweise bei einer Übertragung von Kontaktdaten an Unternehmen, die nachweislich Datenmissbrauch betrieben haben oder schlechte Datenschutzmaßnahmen aufweisen?

III. Wie geht es weiter?

Mit dem Recht auf Datenübertragbarkeit soll Nutzern ein bisher beispielloses Maß an Kontrolle über ihre Informationen gegeben werden und zusätzlich Innovation und Online-Wettbewerb angefacht werden. Im Zuge des Inkrafttretens der DSGVO und anderer Gesetze wurden bereits große Investitionen in Übertragungstools gemacht. Mit diesem Paper und den zukünftigen Debatten möchten wir einen Beitrag zur Förderung der Datenübertragbarkeit leisten. Ziel dabei ist, die Probleme aufzuzeigen und Antworten auf komplexe Fragen darüber zu finden, wie das Recht auf Datenübertragbarkeit datenschutzkonform umgesetzt werden kann. Wir sind davon überzeugt, dass diese Herausforderung gemeinsam zu bewältigen ist, und freuen uns bereits darauf, in den kommenden Monaten mit diversen Stakeholdern an der Entwicklung neuer Lösungen zu arbeiten.

Datenübertragbarkeit und Datenschutz: Blick in die Zukunft

1. *Siehe* Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas*, Washington Post (30. März 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.6247ef86cd32.
2. Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas*, Washington Post (30. März 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.6247ef86cd32.
3. Facebook-Datenschutzgrundsätze, Facebook, https://www.facebook.com/about/basics/privacy-principles (zuletzt aufgerufen am 16. Aug. 2019).
4. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Datenschutz-Grundverordnung], Artikel 20 (EU).
5. Zivilgesetzbuch des US-Bundesstaates Kalifornien § 1798.100(d).
6. Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas*, Washington Post (30. März 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.49b1d969ff54.
7. *Siehe* Data Transfer Project: About Us, https://datatransferproject.dev/.
8. *Siehe* Jacques Crémer, et al., *Competition Policy for the digital era*, Generaldirektion „Wettbewerb" (2019), http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.
9. *Siehe Unlocking Digital Competition: Report of the Digital Competition Expert Panel*, (März 2019 um 09:00 Uhr), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf („There may be situations where opening up some of the data held by digital businesses and providing access on reasonable terms is the essential and justified step needed to unlock competition. Any remedy of this kind would need to protect personal privacy and consider carefully whether the benefits justified the impact on the business holding the data.")
10. *Siehe u. a.* Datum Future: „Data Portability: What is at stake?" (Juli 2017), https://www.datumfuture.org/wp-content/uploads/2019/07/Datum-Future-Data-Portability-July-2019.pdf.
11. *Siehe* Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 19:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
12. *Siehe* Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 11:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
13. *Siehe u. a.* Information Commissioner's Office, Monetary Penalty Notice (24. Okt. 2018), https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf; Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2019-002 (25. Apr. 2019), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/; FTC-Entscheidung, In re Facebook, Inc., C-4365 (24. Juli 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.
14. *Siehe* Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 19:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
15. *Siehe* Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 6:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (Unterstreichung hinzugefügt).
16. *Unlocking Digital Competition: Report of the Digital Competition Expert Panel*, (März 2019 um 08:00 Uhr), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.
17. Diese Herausforderungen gehen weiter als die herkömmlichen Datensicherheitsfragen, die rund um den Zugriff auf personenbezogene Daten über technische Kanäle aufgetaucht sind (wobei auch diese Fragen durchaus komplex sind). Je mehr solche Kanäle es gibt, umso höher ist das Risiko von Datenlecks oder Datenverlust. Durch die Einführung der für die Datenübertragung erforderlichen komplexen, unabhängigen Systeme kommen unweigerlich weitere Kanäle für den Zugriff auf Daten und kontrollierte Dienste hinzu. Für Nutzer können die Sicherheitsrisiken dadurch steigen. *Siehe* John Palfrey und Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (2010).
18. *Siehe* Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 05:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
19. Internationale Organisation für Normung, *ISO/IEC 19941:2017, Information Technology – Cloud Computing – Interoperability and Portability* (2017), https://www.iso.org/obp/ui/#iso:std:66639:en.
20. *Siehe* Decision and Order, In re Facebook, Inc., C-4365 (F.T.C 24. Juli 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.
21. *Siehe u. a.* Ben Thompson, *The Bill Gates Line Follow-up, Twitter and the Bill Gates Line, Data Portability and Facebook*, Stratechery (29. Mai 2018), https://stratechery.com/2018/the-bill-gates-line-follow-up-twitter-and-the-bill-gates-line-data-portability-and-facebook/ („...acknowledging that ‚forced data portability and interoperability' would ‚return[] Facebook to the state it was with the original social graph API', which is what prompted Cambridge Analytica"); Ben Thompson, *The Facebook Brand*, Stratechery (19. März 2018), https://stratechery.com/2018/the-facebook-brand/ („... noting that Facebook Graph API allowed users to ‚give away everything about their friends' and ‚this is exactly how the researcher implicated in the Cambridge Analytica story' gained access to Facebook user data"); Paul Przemyslaw Polanski, *Some*

Thoughts on Data Portability in the Aftermath of the Cambridge Analytica Scandal, EuCML (2018) (in seinem Artikel schreibt er, dass der Cambridge-Analytica-Vorfall die Folge einer fehlerhaften API-Implementierung war, und fordert ein Recht auf Datenübertragbarkeit mit strengen Vorschriften).

22. Es gibt einige technische Hilfsmittel für die Übertragung. Außerdem werden momentan multilaterale Modelle entwickelt, die es den Nutzern erleichtern sollen, die Daten zu verwalten und einen Speicherort zu wählen. Mit Personal Information Management-Systemen (PIMS) beispielsweise können Nutzer ihre Daten entweder lokal oder in einer Cloud speichern und genauestens bestimmen, wie und für welche Zwecke ihre personenbezogenen Daten verwendet werden dürfen. Siehe Europäischer Datenschutzbeauftragter, *Stellungnahme 9/2016, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM)* (20. Okt. 2016 um 07:00 Uhr), https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf. Auch das MIT versucht im Rahmen des Projekts „Solid" dezentralisierte soziale Anwendungen zu entwickeln, mit denen Nutzer ihre Daten an einen beliebigen Speicherort verschieben und zwischen verschiedenen Plattformen wechseln können. *Siehe* MIT-CSAIL, *What Does Solid Offer?*, Solid, https://solid.mit.edu/ (zuletzt aufgerufen am 22. Mai 2019). Die an der Data Mobility Infrastructure Sandbox beteiligten Unternehmen haben Anfang des Jahres begonnen, die von PIMS angebotenen Datenportabilitätsmöglichkeiten auszuwerten. *Siehe* Ctrl-Shift, *Data Mobility Infrastructure Sandbox* (Juni 2019), https://www.ctrl-shift.co.uk/wp-content/uploads/2019/06/DMIS_June_2019_Downloadable_Singles_Final4.pdf.

23. Drittparteien, die im Zuge einer von einem Nutzer angeforderten Übertragung von personenbezogenen Informationen gemäß des gängigen Portabilitätsvorgangs in den Besitz von solchen Daten kommen, unterliegen nicht automatisch denselben Kontrollen und Sicherheitsanforderungen wie solche Dritte, die personenbezogene Daten auf andere Weise erlangen. *Siehe* FTC-Entscheidung, In re Facebook, Inc., C-4365 (24. Juli 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

24. DSGVO Artikel 20 Absatz 1.

25. *Siehe* Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (9. Apr. 2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099. Kritiker bemängeln, das in der DSGVO begründete Recht auf Datenübertragbarkeit werde in den Leitlinien der Datenschutzgruppe zu stark eingeschränkt und fördere somit weder den Wettbewerb noch komme es den Nutzern zugute. *Siehe*

26. Viele US-Politiker, die sich am Entwurf von Datenschutzgesetzen beteiligen, haben darauf hingewiesen, dass kleinere Unternehmen von den neuen Vorschriften nicht überlastet werden dürfen. So enthalten viele Gesetzesentwürfe Ausnahmeklauseln für kleine Firmen. Ein Beispiel ist der US-amerikanische DASHBOARD Act. Er wurde von den Senatoren Mark Warner (Demokrat, Virginia) und Josh Hawley (Republikaner, Missouri) vorgelegt und findet nur für Unternehmen Anwendung, die (1) aus der Nutzung, Sammlung, Verarbeitung, dem Verkauf oder der Verbreitung von Nutzerdaten einen wesentlichen Umsatz verzeichnen; und (2) in den USA während eines Großteils des vorangegangenen Kalenderjahres mindestens 100.000.000 einmalige, monatlich aktive Nutzer vorweisen können. *Siehe* Pressemitteilung, *Warner & Hawley Introduce Bill to Force Social Media Companies to Disclose How They Are Monetizing User Data* (24. Juni 2019), https://www.warner.senate.gov/public/index.cfm/2019/6/warner-hawley-introduce-bill-to-force-social-media-companies-to-disclose-how-they-are-monetizing-user-data. Ein weiteres Beispiel nannte der Repräsentant Jan Schakowsky (Demokrat, Illinois), der bei einer Rede Folgendes sagte: „Wir dürfen nicht außer Acht lassen, welche negativen Folgen strikte Gesetze und Vorschriften für kleine und mittelständische Unternehmen haben können. Große, etablierte Unternehmen haben es einfacher, sich in einer komplexen und ressourcenintensiven Datenschutzlandschaft zurechtzufinden. Startups und kleine Firmen hingegen können es sich nicht leisten, Compliance-Kosten in Millionenhöhe zu stemmen."*Siehe Protecting Consumer Privacy in the Era of Big Data: Hearing Before the House Energy & Commerce Comm.*, 116th Cong. (26. Febr. 2019). Auch EU-Politiker haben bei den Datenschutzverpflichtungen für Unternehmen Ausnahmen für kleine und mittelständische Firmen vorgesehen, um einer unverhältnismäßigen Belastung vorzubeugen. *Siehe beispielsweise* Artikel 30 Absatz 5 der DSGVO, in der KMUs mit weniger als 250 Mitarbeitern von der Einhaltung bestimmter Datenspeicherpflichten befreit werden. Doch auch Anbieter werden in der DSGVO vor einer übermäßigen Belastung geschützt, indem ihnen das Recht vorbehalten bleibt, Anfragen „bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen" abzulehnen. *Siehe* DSGVO Artikel 12 Absatz 5 Buchstabe b.

27. *Siehe u. a.* Dr. Aysem Diker Vanberg, *The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience*, 21(7) J. Internet L. 1, 3 (2018) („[A]llowing one user to transfer a second user's information to another platform may violate the privacy rights of a second user."); Helena Ursic, *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control*, 15(1) SCRIPT-ed 42, 56 (2018), https://script-ed.org/wp-content/uploads/2018/08/ursic.pdf (Bezug auf diese zwei Textstellen: „‚additional difficulties in applying the right to data portability' when data contains ‚multiple persons' data which are … intertwined'"); Barbara Engels, *Data Portability Among Online Platforms*, 5 Internet Policy Rev. 2, 4–5 (2016), https://policyreview.info/articles/analysis/data-portability-among-online-platforms („Allowing one to transfer a second user's information may violate the privacy rights of second user.").

28. *Siehe* Comments of New America's Open Technology Institute, *In re Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition*, (FTC, 20. Aug. 2018 um 16:00 Uhr), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0034-154926.pdf („[N]owhere is [the tension between the right to portability and friends' right of privacy] greater than when it comes to the portability of information about your contacts on social networks, or your ‚social graph'.").

29. *Siehe u. a.* Ira Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 Int'l Data Privacy L., 74–87 (2013), https://lsr.nellco.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1359&context=nyu_plltwp (in seinem Artikel befürwortet er das Prinzip eines eigentumbasierten Datenmodells zur Stärkung des Datenschutzes); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055 (2004), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1068&context=facpubs (in diesem Artikel wird ein eigentumbasiertes Datenmodell zur Stärkung des Datenschutzes vorgestellt); *siehe auch* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 Md. L. Rev. 335, 373 (2013) (Bezug auf diese Textstelle zum Recht auf Datenübertragbarkeit: „‚…appears more closely akin to the personal data ownership theory' than the right of access, and acknowledging debate around whether personal information is property").

30. *Siehe u. a.* Hayley Tsukayama, *Knowing the "Value" of Our Data Won't Fix Our Privacy Problems*, Electronic Frontier Foundation (15. Juli 2019), https://www.eff.org/deeplinks/2019/07/knowing-value-our-data-wont-fix-our-privacy-problems; Sarah Jeong, *Selling Your Private Information Is a Terrible Idea*, New York Times (5. Juli 2019), https://www.nytimes.com/2019/07/05/opinion/health-data-property-privacy.html.
31. *Siehe* Europäische Kommission, *Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, (10. Jan. 2017), https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy; *siehe auch* Cameron F. Kerry & John B. Morris, „Why data ownership is the wrong approach to protecting privacy", Brookings Institution (26. Juni 2019), https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.
32. Ähnliche Erwägungen gelten beim Thema Datenschutz im Fall von Datenübertragungen zwischen Unternehmen (die, wie oben bereits erwähnt, den Rahmen dieses Papers sprengen würden, jedoch für die Wettbewerbsförderung eine ebenso wichtige Rolle spielen wie das Recht auf Datenübertragbarkeit des Einzelnen). Darüber hinaus spielen bei solchen Übertragungen auch andere Faktoren eine Rolle, die starke Auswirkungen auf den Schutz der betroffenen Daten haben können.
33. *Siehe* Bennett Cyphers & Danny O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, Electronic Frontier Foundation (24. Juli 2018), https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine; Kevin Bankston, *How We Can 'Free' Our Facebook Friends*, New America Weekly (28. Juni 2018), https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends; *siehe auch* Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, E. L. Rev. 2017, 42(6), 793, 804-05 (2017) („[T]he inability to access [‚friends' data] could constitute a barrier to entry for potential competitors."). *Siehe auch* Ben Thompson, *The Bill Gates Line Follow-up, Twitter and the Bill Gates Line, Data Portability and Facebook*, Stratechery (29. Mai 2018), https://stratechery.com/2018/the-bill-gates-line-follow-up-twitter-and-the-bill-gates-line-data-portability-and-facebook/.
34. *Siehe u. a.* Comments of New America's Open Technology Institute, *In re Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition*, (FTC, 20. Aug. 2018 um 16:00 Uhr), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0034-154926.pdf („Most services will now let you download your own social media posts, but what about other people's comments to those posts, or your comments and tags on other people's posts and photos? … These are just some of the examples of the unresolved tension between my right to portability and my friends' right to privacy, and nowhere is that tension greater than when it comes to the portability of information about your contacts on social networks, or your ‚social graph'."); Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, 42(6) E. L. Rev. 793, 808 (2017) („A further potential cost and complication for data controllers will be ensuring data security, given the tension between data security and data access. The A29WP perhaps underestimates the extent of this challenge for data controllers stating simply that the GDPR right may also 'raise some security issues' while highlighting that the data controller will remain responsible for 'taking all the security measures needed to ensure that personal data is securely transmitted[.]'"); Dr. Aysem Diker Vanberg, The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience, 21 J. Internet L. 7 (2018) („The Article 29 Working Party arguably has not succeeded in offering more clarity as to what security standards are expected.").
35. *Siehe* Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 19:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
36. *Siehe* Personal Data Protection Commission von Singapur, *Discussion Paper on Data Portability*, (25. Febr. 2019 um 20:00 Uhr), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf.
37. *Siehe* Personal Data Protection Commission von Singapur, "Public Consultation on Review of the Personal Data Protection Act 2012 ? Proposed Data Portability and Data Innovation Provisions," (22. Mai 2019 um 17:00 Uhr).
38. Siehe Gennie Gebhart, Bennet Cyphers & Kurt Opsahl, *What We Mean When We Say "Data Portability"*, Electronic Frontier Foundation (13. Sept. 2018), https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability; Kevin Bankston, *How We Can 'Free' Our Facebook Friends*, New America Weekly (28. Juni 2018), https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends/.
39. Benachrichtigungsabnutzung ist ein Problem, das häufig im Kontext von Sicherheitsverletzungen diskutiert wird. *Siehe u. a.* Jeri Clausing, *'Security Fatigue' Complicates the Battle Against Data Breaches*, Internet Soc'y (21. Dez. 2016), https://www.internetsociety.org/blog/2016/12/security-fatigue-complicates-the-battle-against-data-breaches/; Christopher Mele, *Data Breaches Keep Happening. So Why Don't You Do Something?*, New York Times (1. Aug. 2018), https://www.nytimes.com/2018/08/01/technology/data-breaches.html.
40. *Siehe* Kevin Bankston, *How We Can 'Free' Our Facebook Friends*, New America Weekly (28. Juni 2018), https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends; Josh Constine, *Facebook Shouldn't Block You from Finding Friends on Competitors*, TechCrunch (13. Apr. 2018), https://techcrunch.com/2018/04/13/free-the-social-graph; Bennett Cyphers & Danny O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, Electronic Frontier Foundation (24. Juli 2018), https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine; *siehe auch* Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, 42(6) E. L. Rev. 793, 804-05 (2017) („[T]he inability to access ['friends' data] could constitute a barrier to entry for potential competitors."). *Siehe aber auch* Ben Thompson, *The Bill Gates Line Follow-up, Twitter and the Bill Gates Line, Data Portability and Facebook*, Stratechery (29. Mai 2018), https://stratechery.com/2018/the-bill-gates-line-follow-up-twitter-and-the-bill-gates-line-data-portability-and-facebook/.
41. *Siehe* Comments of New America's Open Technology Institute, *In re Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition*, (FTC, 20. Aug. 2018 zwischen 06:00 und 07:00 Uhr) https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0034-154926.pdf.
42. Comments of New America's Open Technology Institute, *In re Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition*, (FTC, 20. Aug. 2018 zwischen 06:00 und 07:00 Uhr) https://www.ftc.gov/

system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0034-154926.pdf.

43. *Siehe u. a.* Information Commissioner's Office, Monetary Penalty Notice (24. Okt. 2018), https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf; Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2019-002 (25. Apr. 2019), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/.
44. Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 19:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
45. Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 19:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
46. *Siehe* Personal Data Protection Commission von Singapur, „Discussion Paper on Data Portability", (25. Febr. 2019 um 20:00 Uhr), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf.; Gus Rossi & Charlotte Slaiman, *Interoperability = Privacy + Competition*, Public Knowledge (26. Apr. 2019), https://www.publicknowledge.org/news-blog/blogs/interoperability-privacy-competition („[B]ecause they are dealing with personal data, third parties that want to interoperate would be required to follow a clear and transparent open model for user privacy, including potential requirements for pre-approval or certification by an independent entity.").
47. *Siehe u. a.* DSGVO Artikel 42 und 43
48. Die Personal Data Protection Commission von Singapur hat erst kürzlich vorgeschlagen, dass sie dazu berechtigt werden sollte, verbindliche Verhaltenskodizes für bestimmte Bereiche auszuarbeiten, die den Schutz der Verbraucher, Zusicherungen von Gegenparteien, Interoperabilität und den Schutz von Daten betreffen. *Siehe* Personal Data Protection Commission von Singapur, „Public Consultation on Review of the Personal Data Protection Act 2012 ? Proposed Data Portability and Data Innovation Provisions," (22. Mai 2019 um 17:00 Uhr) (in diesen Verhaltenskodizes würden die Mindestanforderungen an Interoperabilität und Sicherheit sowie die Verifizierungskriterien für die die Daten empfangende Partei und Informationen genannt, die die Verbraucher benötigen, um ihr Recht auf Datenübertragbarkeit auszuüben).
49. *Siehe* Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 zwischen 06:00 und 07:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.
50. *Siehe* Personal Data Protection Commission von Singapur, *Discussion Paper on Data Portability*, (25. Febr. 2019 um 20:00 Uhr), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf.
51. *Siehe* Personal Data Protection Commission von Singapur, „Public Consultation on Review of the Personal Data Protection Act 2012 ? Proposed Data Portability and Data Innovation Provisions", (22. Mai 2019 um 14:00 Uhr).
52. Artikel-29-Datenschutzgruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit" (5. Apr. 2017 um 11:00 Uhr), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.