STIFTUNG DATENSCHUTZ

DATEN-PORTABILITÄT

POLICY PAPER

INHALT

Einleitung 2

Handlungsempfehlungen

- Zielrichtung der Norm 4
- Bestimmung des Anwendungsbereichs 4
- Umsetzungsstrategien 5

Resümee

- Herausforderungen 6
- Anwendungsbereich 7
- Kontrollrechte und Transparenz 8
- Rechte Dritter 9
- Governance-Struktur 10
- Datensouveränität 12

Workshop #01 – 11.09.2019
Ein Konzept für die Datenportabilität 13

Workshop #02 – 01.10.2019
Datenportabilität in der Praxis 17

Workshop #03 – 01.11.2019
Praktische Herausforderungen und Lösungen bei der Implementierung von Datenportabilität 25

Autorin: Prof. Dr. Anne Riechert, Stiftung Datenschutz/Frankfurt University of Applied Sciences

EINLEITUNG

Die Stiftung Datenschutz hat im Herbst 2019 unter Mitwirkung von Akteuren aus Politik, Aufsichtsbehörden, Wirtschaft, Wissenschaft und Gesellschaft das Thema „Datenportabilität" in drei Workshops diskutiert. Angeregt wurden diese Diskussionsrunden u.a. von Facebook. Das Unternehmen engagiert sich für einen Portabilitätsstandard im Data Transfer Project und die hat im Vorfeld der Workshops ein „White Paper" zu Fragen der Datenportabilität veröffentlicht. Die Stiftung griff aus diesem Anlass den Inhalt ihrer Projektarbeit aus 2017 wieder auf. Ziel war eine Bestandsaufnahme zu den Fragen: (Wie) ist das Recht auf Datenportabilität mittlerweile in der Praxis angekommen? Welche Chancen und Risiken des noch jungen Betroffenenrechts aus der DSGVO zeigen sich aktuell?

Die einzelnen Diskussionen wurden von der Stiftung Datenschutz in anonymisierter Form zusammengefasst und ausgewertet und die jeweiligen Schlussfolgerungen in einem übergreifenden Resümee verknüpft (s. hierzu die folgenden Kapitel). Darauf basierend wurden Handlungsempfehlungen erstellt.

In der Praxis gibt es weitgehend noch keine Erfahrungswerte zum Umgang mit dem Recht auf Datenübertragbarkeit. Insgesamt besteht jedoch ein großer Bedarf an einer umfassenden Analyse dahingehend, wie sich das bestehende Portabilitätsrecht sowohl auf den Markt als auch auf die Gesellschaft auswirkt und welchen technischen Herausforderungen begegnet werden muss. So befassen sich aktuell verschiedene Initiativen mit diesem Thema, wie etwa das „Data Transfer Project", die „Data Portability Cooperation" unterschiedlicher Telekommunikationsanbieter oder die Idee einer „New Governance" mit dem Fokus auf einen branchen- und sektorübergreifenden Datentransfer.[1] Aus datenschutzrechtlicher Sicht muss bei sämtlichen Aktivitäten die Stärkung des Kontrollrechts der Betroffenen gemäß Erwägungsgrund 68 im Mittelpunkt stehen, so dass neue Geschäftsmodelle dieses Kontrollrecht – etwa unter Berufung auf eine serviceorientierte Auslegung – auf keinen Fall aushebeln dürfen. Dieses Papier zeigt daher auch Herausforderungen auf, auf die weder die DSGVO noch die bisherigen Leitlinien zum Recht auf Datenübertragbarkeit bislang eine eindeutige Antwort geben können. Zwar hat die von der Bundesregierung eingesetzte Datenethikkommission durch ihre Empfehlung, von einer Erweiterung der Datenportabilität vorerst abzusehen und zunächst eine entsprechende Evaluierung durchzuführen, eine entsprechende Zielrichtung vorgegeben.[2] Dennoch muss der Blick auf eine mögliche gesamteuropäische Auslegung und entsprechende Umsetzung ausgerichtet sein. In den einzelnen Workshops wurde diesbezüglich die Erwartungshaltung geäußert wurde, dass in den kommenden Jahren keine Änderung von Artikel 20 DSGVO erfolgen wird. Daher bedarf es in der Praxis umso dringender einer klaren Richtschnur für die Auslegung des Verordnungstextes.

Hervorzuheben ist, dass die Studie der Stiftung Datenschutz „Praktische Implikationen der Datenportabilität in der Praxis" aus dem Jahre 2017 sowie die daraus resultierenden Handlungsempfehlungen nach wie vor von großer Aktualität sind.[3] In diesem Sinne hat auch die Datenethikkommission in ihrem am 23.10.2019 veröffentlichten Gutachten auf die Notwendigkeit von branchenbezogenen Verhaltensregeln und Standards verwiesen.[4] Im Rahmen der drei Workshop-Diskussionen konnten nun weitere wichtige Fragestellungen erarbeitet werden, die die Stiftung Datenschutz mit Blick auf rechtliche, technische und gesellschaftliche Auswirkungen analysiert hat. Dabei sind ebenso eigene Überlegungen der Stiftung Datenschutz sowohl in die Auswertung als auch in die Handlungsempfehlungen eingeflossen.

1 In der Zusammenfassung und Auswertung des ersten und zweiten Workshop-Gesprächs werden diese Projekte näher erläutert.

2 Siehe Gutachten der Datenethikkommission, veröffentlicht am 23.10.2019, abrufbar unter https://sds-links.de/Datenethikkommission. Unter „Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten", S.21 empfiehlt sie von der Erweiterung des Portabilitätsrechts, etwa auf andere als bereitgestellte Daten oder auf Portierung in Echtzeit, vorerst abzusehen. Allerdings ist zu prüfen, inwieweit dies ebenso einer europaweiten Auslegung und Empfehlung entspricht.

3 Siehe die Studie der Stiftung Datenschutz „Praktische Umsetzung des Rechts auf Datenübertragbarkeit", abrufbar unter: https://sds-links.de/Studie2017.

4 Siehe Gutachten der Datenethikkommission, S. 136.

VORGEHENSWEISE

Im Mittelpunkt der Workshop-Reihe standen folgende Leitfragen:

- Was sind die Ziele der Datenübertragbarkeit?
- Was sind die Anforderungen und Grundprinzipien?
- Wie wird die Portabilität den Bedürfnissen der Menschen gerecht?
- Wann liegt ein Fall von Datenübertragbarkeit vor?
- Welche Daten sollten übertragbar sein?
- Wessen Daten sollten übertragbar sein?
- Was ist mit Daten umzugehen, die sich auf mehr als eine Person beziehen?
- Wie sollten Einzelpersonen und Controller Dritte auswählen? Sollten Dritte irgendwelche Regeln befolgen, und wenn ja, wie kann das sichergestellt werden? Wären solche Regeln mit den Zielen der Portabilität unter der DSGVO vereinbar? Was sollte Personen über die Ziele, zu denen sie Daten portieren könnten, mitgeteilt werden, wenn überhaupt?
- Wie kann sichergestellt werden, dass Datenübertragungen sicher, fair und reibungslos erfolgen?
- Wie kann die Industrie das Recht auf Datenübertragbarkeit verwirklichen und gleichzeitig den Schutz der Daten gewährleisten? Und wie kann das für andere Formen der Portabilität geschehen?
- Welche rechtlichen und technischen Fragen ergeben sich bei der Mobilität von Daten?
- Welche sind die richtigen Checks and Balances und wer ist im Falle von Vorfällen oder Verletzungen verantwortlich?

WIR BEDANKEN UNS FÜR DIE WERTVOLLEN BEITRÄGE ZUR DISKUSSION BEI:

Bock, Kirsten (Datenschutz-Expertin)

Brandt, Liz (Ctrl-Shift)

Chavez, Jessie (Google)

de Bièvre, Matthias (visionspol.eu)

Dion, Olivier (OneCube)

Dittmar, Thorsten (polypoly.eu)

Frank, Sabine (Google)

Jakobi, Timo (Universität der Künste Berlin)

Mache, Lutz (Google)

Madhani, Bijan (Facebook)

Molavi, Ramak (iRIGHTS law)

Quiel, Philipp (reuschlaw Rechtsanwälte)

Rens, Semjon (Facebook)

Schätzle, Daniel (Härting Rechtsanwälte)

Teubner, Timm (TU Berlin / Einstein Center for Digital Future)

van den Boom, Jasper (Universität Tilburg)

van der Valk, Thomas (Facebook)

Willard, Brian (Google)

... und weiteren Mitwirkenden.

HANDLUNGSEMPFEHLUNGEN

ZIELRICHTUNG DER NORM

Das Recht auf Datenübertragbarkeit ist auf die **Stärkung der Kontrollrechte** der Betroffenen ausgerichtet. Eine Auslegung der Norm im Sinne einer eher **serviceorientierten Betrachtungsweise** bedarf vorab einer Untersuchung sowie einer darauf basierenden Abwägung, ob eine solche Interpretation den Kontrollrechten der Betroffenen zuwiderlaufen könnte. Hierbei sollten ethische Gesichtspunkte berücksichtigt werden.

Datenportabilität als Betroffenenrecht ermöglicht eine **DSGVO-konforme Verarbeitung** und bedarf einer **Geltendmachung durch den Betroffenen**. Datenportabilität kann keinen Transfer von Daten legitimieren, der ansonsten einer Rechtsgrundlage bzw. einer informierten Einwilligung des Betroffenen bedarf. Dies muss sowohl bei Begrifflichkeiten wie „Datenmobilität“ als auch bei neuen Geschäftsmodellen in der Praxis berücksichtigt werden.

Die Norm ermöglicht Betroffenen, einen kompletten Datensatz oder nur einen Teil davon zu jedem anderen Dienstleister ohne Angabe von Gründen zu übertragen oder übertragen zu lassen. Das Portabilitätsrecht umfasst keine automatischen Löschungsrechte und ist vom Auskunftsrecht abzugrenzen. Aufgrund der **Komplexität** des Rechts auf Datenübertragbarkeit sollten daher das Wissen und die Möglichkeiten und Grenzen des neuen Rechts bei den Verbraucherinnen und Verbrauchern durch **Informationskampagnen** gefördert werden.

Das **Recht ist der Technik und der Praxis voraus** und es empfiehlt sich eine **Untersuchung, inwieweit das Recht auf Datenübertragbarkeit zurzeit in der Praxis verlässlich umgesetzt** werden kann, insbesondere im Hinblick auf die in der DSGVO angedrohten Sanktionen

BESTIMMUNG DES ANWENDUNGSBEREICHS

Empfehlenswert ist eine Prüfung dahingehend, **welche Roh- und Metadaten übertragen werden müssen**, damit der Dienstanbieter das Recht auf Datenübertragbarkeit sowohl aus technischer und praktischer Sicht als auch im Interesse der Betroffenen umsetzen kann. Ergänzend könnten Nutzerumfragen durchgeführt werden, an welchen Daten ein **Transferinteresse** besteht.

Die Auslegung des Begriffs **„observed data“** sollte sich an der Stärkung der Kontrollrechte des Betroffenen ausrichten. Es empfiehlt sich eine Untersuchung, inwieweit ein umfassender Transfer von Nutzungsdaten und eine weit gefasste Definition von „bereitgestellten Daten“ das **Persönlichkeitsrecht der Betroffenen gefährden kann**, insbesondere aufgrund wirtschaftlicher (Eigen)Interessen der Dienstanbieter an der Nutzung dieser Daten.

Mit Blick auf neue Geschäftsmodelle sollten **eindeutige Kriterien entwickelt werden**, unter welchen rechtlichen Voraussetzungen ein „Antrag“ bzw. **„request“** des Betroffenen vorliegt. Die **Technik sollte weder das Recht vorgeben noch definieren**, sondern die Technik sollte sich vielmehr an den rechtlichen Vorgaben ausrichten.

Der **Europäische Datenschutzausschuss** könnte hinsichtlich des in seinen Leitlinien dargestellten Beispiels der Übertragung eines Kontaktverzeichnisses zu einem Webmaildienst klarstellend ausführen, in welchen konkreten Fällen die **Rechte von Dritten** bei einem Datentransfer verletzt werden können und inwieweit eine Verarbeitung aufgrund **berechtigter Interessen oder wissenschaftlicher Forschungszwecke** grundsätzlich möglich ist. Verhaltensregeln könnten dies zusätzlich unterstützen.

Empfehlenswert wäre eine Klarstellung, ob dem Betroffenen oder dem Provider vor einem Datentransfer (Prüf-)Pflichten obliegen könnten oder sollten. Im Rahmen der Prüfung ist zu berücksichtigen, dass der Dienstanbieter dem Grundsatz **„Datenschutz durch Technik“** unterliegt und der Betroffene regelmäßig Daten ausschließlich für persönliche und familiäre Tätigkeiten verarbeitet.

UMSETZUNGSSTRATEGIEN

Unternehmen müssen bei der Implementierung der Datenportabilitätsvorgaben ein ausgewogenes Maß finden, wenn es darum geht, die Nutzerinnen und Nutzer über die Umstände von Datentransfers zu informieren. Sie sollten ausreichende Transparenz schaffen, ohne die Nutzer mit Informationen zu überladen.

Der ordnungsgemäßen Authentifizierung der anfragenden Personen muss bei Portabilitätsanfragen große Aufmerksamkeit gewidmet werden, um Datenschutzverletzungen und unnötige Risiken für Persönlichkeitsrechte zu vermeiden. Die DSGVO verbietet es der datenverarbeitenden Stelle Datentransfers zu behindern. Dennoch sollten Mechanismen geprüft werden, um das Risiko zu verringern, dass personenbezogene Benutzerdaten an Dritte übertragen werden, die nicht vertrauenswürdig sind. Insgesamt können **Standards** unterstützen, das Vertrauen der Nutzer in die vorhandene Infrastruktur zu stärken. Standards sollten anhand konkreter Anwendungsfälle gebildet und stets fortgeschrieben werden, um die Chancen und Risiken klar aufzuzeigen. Um Datenportabilität in der Praxis anzukurbeln, könnte die Auswahl der Anwendungsfälle zunächst von den Unternehmen getroffen werden.

Die Entwicklung von und das Bekenntnis zu Standards schafft sowohl **Vertrauen** in das jeweilige Unternehmen und kann gleichermaßen als **Marketinginstrument** dienen. Durch entsprechende **Open-Source-Projekte** können auch kleinere Unternehmen das Recht auf Datenübertragbarkeit in der Praxis leichter umzusetzen.

Mit dem Recht auf Datenübertragbarkeit wird der Begriff der Datensouveränität verbunden. Daher empfiehlt sich eine eindeutige **Definition von Datensouveränität**, die gleichermaßen die Kontrollrechte des Betroffenen abbildet. Das **Recht auf informationelle Selbstbestimmung** könnte in diesem Sinne **auf europäischer Ebene weiterentwickelt** werden. **„Souverän“** sollte dabei in seinem **eigentlichen Wortsinn** ausgelegt werden, als **Kompetenz und das Wissen der betroffenen Person**, **autonome** und einem technischen System **überlegene Entscheidungen** in einer digitalen Welt zu treffen.

Hilfreich für die Operationalisierung der Datenportabilität können außerdem Lösungen aus dem PIMS-Bereich sein. Die sogenannten Personal Information Management Systems/Services könnten als Knotenpunkte zwischen den Unternehmen fungieren, zwischen denen die angeforderten Datensätze sicher übertragen werden sollen.

RESÜMEE

HERAUSFORDERUNGEN

Die ursprüngliche Intention des Rechts auf Datenportabilität, den Wechsel zu datenschutzfreundlichen Netzwerken zu erleichtern, gerät zunehmend in den Hintergrund. Wenn derzeit über Datenportabilität diskutiert wird, steht oftmals der freie Datenfluss im Fokus, dem durch die vom Europäischen Datenschutzausschuss bestätigten Richtlinien der Artikel-29-Datenschutzgruppe aufgrund der nahezu grenzenlosen Übertragungsmöglichkeit von Daten über Branchen hinweg, der Weg geebnet wurde.[1] Der Umsetzung in der Praxis stehen allerdings einige Herausforderungen gegenüber. Gelingen kann eine umfassende Datenportabilität nur, wenn die Unternehmen die entsprechenden Voraussetzungen schaffen. Oftmals bestehen jedoch gerade gegenüber den großen Anbietern Vorbehalte im Hinblick auf eine Zusammenarbeit. Allerdings kann Portabilität keinen Erfolg haben, wenn jeder sein eigenes System entwickelt. Zu einer umfassenden, sektorübergreifenden Datenportabilität müssen daher einerseits Befürchtungen abgebaut und gemeinsame Standard entwickelt werden, damit neuer Nutzen und neue Dienste entstehen können. Andererseits bedarf dieses Thema gerade auch mit Blick auf besonders schützenswerte Daten, wie Versichertendaten, Gesundheitsdaten, etc., besonderer Sensibilität. Open-Source-Projekte und Kooperationen – wie die im Einleitungskapitel genannten- können dabei unterstützen und Unternehmen mit kleineren Marktanteilen und Start-Ups die Umsetzung der Datenportabilität grundsätzlich ermöglichen.

Aus technischer Sicht stehen Unternehmen zurzeit weiterhin vor der Herausforderung, gängige und gemeinsame Datenformate zu entwickeln. Dies betrifft unterschiedliche Anwendungsfälle, wie z.B. die Zusammenstellung von Playlists unterschiedlicher Dienste, kann sich aber ebenso auf den Transfer von Gesundheitsdaten beziehen. Darüber hinaus muss bei der Entwicklung neuer Services stets ein passendes Format gefunden werden, so dass die Herausforderung auch darin besteht, mit dem jeweiligen System Schritt zu halten.

Das Recht ist der Technik und der Praxis voraus und es empfiehlt sich – trotz und wegen der in den Workshops geäußerten Erwartungshaltung, dass keine Änderung der Gesetzeslage zu erwarten ist – eine Analyse, inwieweit das Recht auf Datenübertragbarkeit in realistischer Weise und mit den in der DSGVO angedrohten Sanktionen in der Praxis umgesetzt werden kann. Außerdem können Open-Source-Projekte dabei unterstützen, dass kleinere Unternehmen das Recht auf Datenübertragbarkeit realisieren können.

1 Die Leitlinien der Artikel-29-Datenschutzgruppe, angenommen am 13. Dezember 2016 zuletzt überarbeitet und angenommen am 5. April 2017, sind in unterschiedlichen Sprachen abrufbar unter: https://sds-links.de/Leitlinien. Der Europäische Datenschutzausschuss bestätigte die mit der Datenschutz-Grundverordnung zusammenhängenden Leitlinien der Artikel-29-Datenschutzgruppe bei seiner ersten Plenarsitzung am 25.05.2018, siehe unter https://sds-links.de/EDPB.

ANWENDUNGSBEREICH

In der Diskussion zum Thema „Datenportabilität“ wird regelmäßig auf weitere Begrifflichkeiten wie „Datenzugangsrechte“, „Datenteilung“ oder „Datenmobilität“ Bezug genommen. Diese Begriffe müssen vom Recht auf Datenportabilität abgegrenzt werden, insbesondere da hiervon oftmals regulatorische und/oder politische Fragestellungen umfasst sind. Vor allem bezüglich „Datenzugangsrechten“ wurde in der Diskussion auf spezifische, rechtliche Regelungen verwiesen und beispielhaft neue Geschäftsmodelle (etwa auf das private Finanzmanagement ausgerichtete Services) angeführt, für welche vorrangig die PSD2-Richtlinie gelten müsse. Andererseits werden die Begriffe der „Datenzugangsrechte“ und „Datenteilung“ ebenso im Zusammenhang mit anonymisierten Daten angeführt, so dass in diesem Falle die DSGVO nicht einschlägig wäre – unter der Voraussetzung, dass es im digitalen, vernetzten Zeitalter noch anonyme Daten gibt. Untersucht werden könnte jedoch, inwieweit eine Begriffsbildung wie „Datenmobilität“ im Sinne einer politischen oder gesellschaftlichen Betrachtungsweise relevant ist. Diskutiert wurde dies unter dem Aspekt, inwieweit andere technische Standards oder abweichende Anforderungen an Richtlinien, Policies, etc. erforderlich sein könnten. Aus rechtlicher Sicht muss die Bewertung allerdings ergeben, dass dem Begriff „Datenmobilität“ keine eigenständige rechtliche Relevanz zukommen kann. Allenfalls mit Blick auf neue Geschäftsmodelle und deren konkreter Ausgestaltung in der Praxis muss deutlich und klar abgrenzbar sein, dass Datenportabilität an die Voraussetzungen des Artikels 20 DSGVO geknüpft ist und dieses Recht ein Betroffenenrecht, aber kein Unternehmensrecht darstellt. Soll ein darüber hinausgehender Datenfluss erfolgen, handelt es sich bei der Übertragung von personenbezogenen Daten um eine Datenverarbeitung, die einer Rechtsgrundlage bedarf, beispielsweise in Form einer Einwilligung unter Berücksichtigung der Anforderungen des Artikel 4 Nr. 11 und Artikel 7 DSGVO.

Diskutiert wurde ebenso, ob der Begriff der „Datenmobilität“ bei Daten in Betracht kommen kann, die nicht von Artikel 20 DSGVO umfasst sind, etwa in Bezug auf Daten die vom Verantwortlichen aufgrund berechtigter Interessen erhoben wurden oder bei Daten, die keinen Personenbezug haben. In diesen Fällen wären die formalen Voraussetzungen des Artikels 20 DSGVO nicht erfüllt, so dass eine rechtliche Relevanz nur dann besteht, wenn eine entsprechende Erweiterung durch Leitlinien des Europäischen Datenschutzausschusses oder durch Änderung des gesetzlichen Wortlautes festgestellt wird. Möglicherweise muss jedoch der Herausforderung begegnet werden, dass in der Praxis durch neue Geschäftsmodelle entsprechende Fakten geschaffen werden.

Als wesentliche Voraussetzung ist ebenso hervorzuheben, dass Datenportabilität als Kontrollrecht des Betroffenen stets eines eindeutigen Antrags („request“) durch diesen bedarf. Die Grenzen zwischen „Anschubsen“ und „Auffordern“ können hier fließend sein. In diesem Zusammenhang könnte zwar die Frage aufgeworfen werden, welchen Einfluss die zugrundeliegende Technik darauf hat. Allerdings sollte die Technik nicht das Recht vorgeben, sondern umgekehrt die Frage gestellt werden, in welchen Fällen ein Antrag im Sinne eines „request“ des Nutzers vorliegt. Diese Frage kann sich etwa bei „One-Klick“- Lösungen stellen oder wenn generierte Daten fortlaufend über eine API-Schnittstelle übertragen werden. Hierfür müssen Richtlinien erarbeitet werden.

Datenportabilität ist ein Kontrollrecht des Betroffenen und dient dazu, eine DSGVO-konforme Verarbeitung umzusetzen. Insgesamt muss daher sichergestellt sein, dass kein Transfer von Daten stattfindet, der einer Rechtsgrundlage bedarf. Mit Blick auf mögliche Geschäftsmodelle sollten eindeutige Kriterien entwickelt werden, unter welchen Voraussetzungen ein „Antrag“ bzw. „request“ des Betroffenen vorliegt. Die Technik darf in diesem Zusammenhang nicht das Recht vorgeben.

KONTROLLRECHTE UND TRANSPARENZ

In der Praxis wird oftmals auf das Bedürfnis Bezug genommen, das Recht auf Datenübertragbarkeit „serviceorientiert“, anhand der Nutzerinteressen auszulegen. Wichtig ist es, den Erwägungsgrund 68 stets im Fokus zu haben: Datenportabilität soll die Kontrollrechte des Betroffenen stärken! Daher muss untersucht werden, welche Daten für den Nutzer von Interesse sind. So wurde in der Diskussion auch darauf hingewiesen, dass in der heutigen, schnelllebigen Zeit der Tweet aus der letzten Woche bereits uninteressant sein könnte. Auf der anderen Seite wurde argumentiert, dass auch eine gegenständliche Fotografie (z.B. Sonnenuntergang) mit einem persönlichen Kommentar vergleichbar sei, und dieser Transfer von der ursprünglichen Idee der Datenportabilität umfasst ist. Die Untersuchung des Nutzerinteresses könnte mit einer entsprechenden Umfrage einhergehen: An welchen Daten haben Nutzer ein Transferinteresse? Dabei spielt außerdem eine Rolle, ob der Begriff „observed data“, wie er in den Leitlinien der Artikel-29-Datenschutzgruppe definiert wurde, eine Einschränkung erfahren muss. Im Rahmen der jetzigen Auslegung könnten grundsätzlich auch auf Cookies basierende Daten erfasst sein (vor ihrer Auswertung bzw. Einordnung als „inferred data“), sofern der Nutzer für das Setzen der Cookies seine Einwilligung erteilt hat, oder andere Nutzungsdaten, z.B. Klicks, die der Nutzer erzeugt hat. In diesem Zusammenhang steht man außerdem nach wie vor der ungelösten Aufgabe gegenüber, wie die so genannte „law literacy“ oder „data literacy“ des Betroffenen sichergestellt werden kann. Dies kann sich zum einen etwa auf den Wert von Daten beziehen, den die Betroffenen regelmäßig nicht einschätzen können. Zum anderen ist das Verständnis und das Verstehen des Betroffenen über das „Wie“ der weiteren Datenverarbeitung wichtig. Es handelt sich damit gleichermaßen um die Sicherstellung der notwendigen Transparenz. Dem Betroffenen sollte darüber hinaus nicht nur bekannt sein, dass mit dem Transfer keine automatische Datenlöschung beim ursprünglichen Dienstanbieter verbunden ist, sondern ebenso ob und inwieweit der neue Dienstanbieter Daten aufgrund eigener, berechtigter Interessen verarbeiten darf.

Die Auslegung des Begriffs „observed data“ sollte sich an der Stärkung der Kontrollrechte des Betroffenen ausrichten. Es empfiehlt sich eine Untersuchung, inwieweit ein umfassender Transfer von Nutzungsdaten und eine weit gefasste Definition von „bereitgestellten Daten“ das Persönlichkeitsrecht der Betroffenen gefährden kann, insbesondere aufgrund wirtschaftlicher (Eigen)Interessen der Dienstanbieter an der Nutzung dieser Daten. Als Grundlage eines fairen und transparenten Verfahrens empfiehlt sich zudem eine Ausarbeitung von weiteren klaren Leitlinien und Verhaltensregeln mit Blick auf „berechtigte Interessen“, „wissenschaftliche Zwecke“ und „Weiterverarbeitung“, und zwar unter Berücksichtigung neuer Geschäftsmodelle der Datenportabilität und konkreter Anwendungsfälle in der Praxis. Darüber hinaus könnten klare und verbindliche Standards dazu beitragen, einen fairen Prozess zu gewährleisten.

Aufgrund der Komplexität des Rechts auf Datenübertragbarkeit ist ebenso wichtig, den Nutzer hinsichtlich der notwendigen „law literacy“ zu stärken. ggf. in Form von Informationskampagnen. Dies könnte seitens neutraler Einrichtungen oder der Aufsichtsbehörden erfolgen.

RECHTE DRITTER

Im Zusammenhang mit den Rechten Dritter stellt sich die Frage, inwieweit dem Provider, der die Daten überträgt, Prüfpflichten obliegen sollten – auch wenn die Leitlinien der Artikel-29-Datenschutzgruppe dem neuen Dienstleister die Verantwortung für die Datenverarbeitung zuweisen. Einerseits könnte der Grundsatz „Datenschutz durch Technik" eine solche Verpflichtung nahe legen, insbesondere da der Betroffene oftmals nicht in der Lage ist, die „Rechte Dritter" tatsächlich zu prüfen und außerdem bei Sozialen Netzwerken die Verarbeitung der Daten meist für ausschließlich persönliche und familiäre Zwecke erfolgt. Der Provider könnte beispielsweise Einwilligungsmechanismen implementieren. Dennoch wird die Auffassung vertreten, dass der Betroffene für die Überprüfung verantwortlich sein soll.[2] Allerdings soll der Provider den Datentransfer durch etwaige Prüfpflichten oder Warnhinweise nicht kontrollieren dürfen. Einer Klärung bedarf in diesem Zusammenhang, dass in den Leitlinien der Artikel-29-Datenschutzgruppe die Übertragung eines Kontaktverzeichnisses zu einem Webmaildienst als Portabilitätsbeispiel genannt ist.[3] Zwar wurde die Verarbeitung für eigene Zwecke, wie Marketingzwecke ausgeschlossen, aber angesichts der in den vorherigen Ausführungen bereits dargestellten Verarbeitungsmöglichkeiten aufgrund „berechtigter Interessen" oder zu „wissenschaftlichen Forschungszwecken" sind ergänzend weitere Leitlinien empfehlenswert. Dies könnte anhand von konkreten Anwendungsfällen erarbeitet werden und etwa auch in Form einer Negativ- oder Positivliste erfolgen. Anderenfalls müsste der klare Hinweis gegeben werden, dass jedwede Verarbeitung der Daten Dritter (etwa ohne dessen Einwilligung) durch den neuen Provider untersagt ist, so dass es sich beim Transfer der Daten lediglich um den Wechsel eines Speichermediums handeln würde.[4] In diesem Fall wäre aber dem neuen Provider ggf. die Berufung auf eine Verarbeitungsmöglichkeit untersagt, die dem ursprünglichen Provider erlaubt sein könnte.

Empfehlenswert wäre eine Klarstellung, unter welchen Voraussetzungen das Recht auf Datenübertragbarkeit nicht die Rechte Dritter verletzt und inwieweit dem Betroffenen oder dem Provider vor einem Datentransfer (Prüf-)Pflichten obliegen können. Zu beachten ist in diesem Zusammenhang, dass der Betroffene regelmäßig Dienste ausschließlich für persönliche oder familiäre Tätigkeiten nutzt,insoweit nicht den Pflichten der DSGVO unterliegt, und der Provider den Grundsatz „Privacy by Design" zu berücksichtigen hat.

2 Herbst in: Kühling/Buchner, DSGVO/BDSG, Artikel 20 DSGVO Rn. 17.
3 Leitlinien der Artikel-29-Datenschutzgruppe, S. 13. Siehe hierzu außerdem die Auswertung des zweiten Workshops.
4 Siehe hierzu die Auswertung des zweiten Workshops.

GOVERNANCE-STRUKTUR

Im Fokus der Diskussionsteilnehmer stand ebenso die grundsätzliche Frage, wie eine zukünftige Datenpolitik und eine damit verbundene Governance-Struktur ausgestaltet sein könnten. In diesem Zusammenhang wurden – über die formalen Anforderungen des Rechts auf Datenportabilität hinaus – unterschiedliche Modelle diskutiert, die in der Praxis einen transparenten und fairen Datenverarbeitungsprozess übergreifend sicherstellen könnten. Als mögliche Instrumente, die gleichermaßen der Stärkung der Kontrollrechte der Nutzer dienen können, wurden die Einführung von Standards, Zertifikaten, Datenschutzmanagementsystemen (PIMS) sowie die Etablierung einer neutralen Organisation erörtert, die nachfolgend näher erläutert werden Betont wurde in der Diskussionsrunde, dass die Sicherstellung von Neutralität wesentlich sei – ohne wirtschaftliche Interessen im Zusammenhang mit dem Betrieb des Systems. Insbesondere wurde auf die gesellschaftliche Relevanz neutraler Sozialer Netzwerke, neutraler E-Mail- und Chat-Lösungen hingewiesen.

Insgesamt wurde als Option die Umsetzung einer so genannten „New Governance“ vorgeschlagen. Der Fokus einer solchen Struktur liegt stets in einer (aus datenschutzrechtlicher Sicht vorteilhaften) dezentralen Datenhaltung beim Nutzer. Ein unabhängiges Kontrollgremium soll dabei unterschiedliche Akteure, wie z.B. Unternehmen, Organisationen, Institutionen koordinieren und auf den notwendigen Interessenausgleich achten. Ziel ist es, technologische Standards für die Portabilität und den Schutz personenbezogener Daten sowie „Good Practices“ anhand von konkreten Anwendungsfällen zu entwickeln. Es würde sich insoweit um eine Selbstregulierung handeln, die dadurch funktioniert, dass eine demokratische Struktur vorliegt und ein Leitungsorgan die Ausgewogenheit der unterschiedlichen Interessen überwacht. Die genannten Standards sollen Teil einer digitalen Infrastruktur sein und könnten parallel zu Zertifikaten, Leitlinien oder Verhaltensregeln in der Praxis etabliert werden. Leitlinien und Verhaltensregeln könnten beispielsweise die (abstrakte) Basis bilden, während die Standards einzelne konkrete Anwendungsbeispiele beschreiben.

Als weitere Möglichkeit wurde die Einrichtung einer neutralen Plattform diskutiert, die die Rechte des Nutzers wahrnimmt. Ein solches Repräsentativorgan könnte grundsätzlich eine entscheidende Rolle spielen, um die notwendige Neutralität sicherzustellen. Dies könnte auch im Zusammenhang mit der Monetarisierung von Daten interessant sein, etwa als Ausgestaltung eines Treuhandmodells. In diesem Zusammenhang wird in Literatur und Praxis immer wieder darauf verwiesen, dass der Einzelne aufgrund der komplexen Datenverarbeitungsprozesse nicht mehr in der Lage sei, eine selbstbestimmte Entscheidung zu treffen. Mit Blick auf die Monetarisierung von Daten geht es in diesem Kontext daher ebenso um faire Teilhabemöglichkeiten am Wertschöpfungsprozess von Daten, wie es bereits aus dem Urheberrecht bekannt ist.[5] Allerdings bedarf dies mit Blick auf das Persönlichkeitsrecht des Einzelnen einer umfassenden und eingehenden Untersuchung. Es handelt sich um ein äußerst sensibles Thema, da bislang unklar ist, ob es in der Praxis möglich ist, das Persönlichkeitsrecht des Einzelnen, insbesondere seine „informationelle Selbstbestimmung“ im Rahmen einer solchen Organisation tatsächlich wahrzunehmen und zu achten. Eine besondere Fragestellung ist, in wessen Verantwortung diese Plattform steht und wer diese strukturell überwacht.[6]

5 Nähere Ausführungen hierzu sind vor allem der Auswertung des dritten Workshops zu entnehmen.
6 Grundsätzlich hat auch die Datenethikkommission die nähere Erforschung von Treuhandmodellen empfohlen.

Weiterhin können PIMS-Systeme bzw. Datenschutzmanagementsysteme, die bereits im Jahre 2016 Gegenstand der Studie „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen" der Stiftung Datenschutz waren, zur Kontrolle und Sicherstellung eines transparenten Verfahrens beitragen.[7] Eine Herausforderungen ist dabei, je nach Ausgestaltung des Systems, allerdings die Umsetzung und Sicherstellung des Zweckbindungsgrundsatzes und außerdem die leichte bzw. nutzerfreundliche Handhabung und Bedienbarkeit des System.

Insgesamt spielte in der Diskussion über eine mögliche Governance-Struktur gleichermaßen die Frage des Speicherorts der Daten eine Rolle – ob eine Speicherung zentral oder dezentral erfolgen sollte. Allerdings wird insbesondere aus ökonomischer Sicht der Einwand erhoben, dass das vorrangige Ziel der Zugang zu den relevanten Daten sei und der Ort der Speicherung nicht relevant wäre.

Derzeit werden unterschiedliche Möglichkeiten diskutiert, wie eine Governance-Struktur zukünftig ausgestaltet sein könnte. Insgesamt schafft eine neutrale Struktur das notwendige Vertrauen sowie Transparenz und sichert die Unabhängigkeit von großen, marktbeherrschenden Unternehmen.

7 Studie der Stiftung Datenschutz "Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“, abrufbar unter: https://sds-links.de/PIMS.

DATENSOUVERÄNITÄT

Das Recht auf Datenportabilität wird mit dem Begriff „Datensouveränität“ in Verbindung gebracht. So kann ein Nutzer ohne Angabe von Gründen einen kompletten Datensatz oder Teile davon auf jedweden neuen Anbieter übertragen. Allerdings bleibt die Frage offen, ob „Datensouveränität“ mehr bedeutet als das Recht auf informationelle Selbstbestimmung. Im Fokus muss stets stehen, ob die mit Artikel 20 DSGVO verbundene Datensouveränität zum Vorteil des Betroffenen ist und der Stärkung seiner Kontrollrechte dient. Die Frage ist damit auch, ob Datenportabilität mehr Privatsphäre erlaubt oder ob es zum Gegenteil führt.

Insgesamt betrachtet kann der Begriff Datensouveränität hilfreich sein, um auf europäischer Ebene ein einheitliches Verständnis für ein modernes Datenschutzrecht zu erlangen und eine europaweite Definition zu entwickeln, da das Recht auf informationelle Selbstbestimmung vom Bundesverfassungsgericht geprägt wurde. Allerdings bedarf es einer Prüfung, was unter Datensouveränität zu verstehen ist und wie diese zugunsten der betroffenen Person umgesetzt werden kann. Es muss ein transparentes Verfahren sichergestellt sein – entsprechend der eigentlichen Bedeutung des Wortes „souverän“ und damit in diesem Kontext als Befähigung zur Ausübung des Rechts auf Datenübertragbarkeit verstanden werden. Wenn das Recht auf Datenübertragbarkeit daher ein Instrument ist, um Datensouveränität auszuüben, bedarf es in der Praxis der Bereitstellung der dazu erforderlichen Werkzeuge, und zwar im Sinne von einfachen, verständlichen und praktikablen Anwendungen. Nur dann wird das Recht dergestalt umgesetzt, dass ein Betroffener selbstständig, überlegen und unbeschränkt handeln kann. Dazu gehört ebenso die so genannte „law literacy“ und ein Verständnis über den möglichen Wert und Nutzen persönlicher Daten für andere bzw. (konkret formuliert) für Unternehmen mit eigenen Geschäftsinteressen.

Mit Datensouveränität darf vor allem nicht die Gefahr verbunden sein, dass andere Personen, Institutionen, etc. für den Nutzer nachteilige Entscheidungen treffen. Dies muss ebenso im Kontext der oben beschriebenen von Datenmanagementsystemen und Treuhandmodellen gesehen werden. Es bedarf hier stets einer kritischen Hinterfragung, wer diese Systeme bereitstellt und inwieweit Interessenkonflikte „des Systems“ bestehen können. In Literatur und Praxis wird auf eine „Informations- Asymmetrie“ verwiesen, die durch Unterwerfung unter Management- bzw. Assistenzsysteme entstehen können.

Die größte Herausforderung besteht daher zukünftig darin, dass Betroffene selbstbestimmte und auf dem eigenen Willen basierende Entscheidungen treffen, ohne dass sie etwa durch „Empfehlungen“ eines nicht neutral agierenden Systems dorthin geführt werden. Mit Blick auf die Datensouveränität sollte „souverän“ daher in seinem eigentlichen Wortsinn verstanden werden: Der Betroffene muss überlegt und überlegen handeln, nicht das System. Zu einem selbstbestimmten Datenschutz gehört daher ebenso das Aufbrechen von „Wissens-Asymmetrien“. Dies sollte notwendiger Bestandteil einer Definition von „Datensouveränität“ im digitalen Zeitalter sein. Eine digitale Ethik ist zukünftig mehr als notwendig.

STIFTUNG DATENSCHUTZ

WORKSHOP

#01 – 11.09.2019

ZUSAMMENFASSUNG UND ANALYSE

EIN KONZEPT FÜR DIE DATENPORTABILITÄT

EINLEITUNG

Dienste wie Facebook oder Google haben Nutzern das Recht auf Datenübertragbarkeit bereits in der Vergangenheit zur Verfügung gestellt, ohne dass eine entsprechende gesetzliche Verpflichtung bestand (z.B. Google Take out). Dennoch ist die Verankerung dieses Rechts in der DSGVO seitens des Europäischen Gesetzgebers visionär. Nach wie vor fehlt die Möglichkeit eines Datentransfers in anderen Industriezweigen vollständig. Manches Unternehmen scheint außerdem nicht unglücklich darüber zu sein, dass die Datenportabilität bislang nicht im Blickpunkt der Nutzer steht. Eine Herausforderung besteht daher darin, Unternehmen und Nutzer gleichermaßen von dem Potenzial der Datenportabilität – insbesondere auch sektorübergreifend – zu überzeugen. Die bisherige Zurückhaltung ist ebenso auf Vorbehalte gegenüber Giganten wie Facebook und Google zurückzuführen. Im Workshop wurde darauf verwiesen, dass gerade Unternehmen wie Banken und Versicherungen es bevorzugen würden, ihr eigenes System zur Datenportabilität zu entwickeln anstatt mit diesen Dienstleistern zusammenzuarbeiten. Zu einer umfassenden, sektorübergreifenden Datenportabilität müssen daher einerseits Befürchtungen abgebaut und gemeinsame Standard entwickelt werden, damit neuer Nutzen und neue Dienste entstehen können. Andererseits bedarf dieses Thema gerade auch mit Blick auf Versichertendaten, Gesundheitsdaten, etc. besonderer Sensibilität. Dieses Recht muss dementsprechend mit äußerster Sorgfalt und unter Beachtung eines grenzüberschreitenden Datentransfers entwickelt werden. Es geht also gleichermaßen um Vertrauen, gemeinsame Wertvorstellungen und letztendlich um ethische Maßstäbe – sowohl im Hinblick auf personenbezogene als auch nicht-personenbezogene Daten.

WAS SIND DIE ZIELE DER DATENÜBERTRAGBARKEIT?

Einigkeit besteht darüber, dass es sich beim Recht auf Datenübertragbarkeit um ein Persönlichkeitsrecht handelt. Das parallel existierende Auskunftsrecht ist hiervon abzugrenzen. Es ermöglicht dem Nutzer zwar, eine Kopie der über ihn gespeicherten Daten zum Zwecke der Transparenz und der Informiertheit zu verlangen, ggf. auch um weitere Rechte geltend zu machen oder rechtliche Schritte einzuleiten. Aber es gibt dem Einzelnen insgesamt weniger Möglichkeiten an die Hand. So beinhaltet Datenportabilität das Recht, einen kompletten Datensatz oder Teile davon zu einem beliebig anderen Anbieter aus einem beliebigen Grund zu übertragen. Dies muss in einem maschinenlesbaren Format erfolgen, so dass die Daten problemlos ausgelesen und bei einem weiteren Dienstleister automatisiert (weiter)verarbeitet werden können. Bei Datenportabilität geht es folglich um ein Mehr an Souveränität. Dabei ist so genannte „law literacy“ oder „data literacy“ der Betroffenen von enormer Bedeutung. Denn aus Sicht der Betroffenen existieren zwei parallele Rechte, die ggf. nicht immer leicht zu trennen sind. Datenportabilität betrifft außerdem ausschließlich Daten, die der Betroffene bereitgestellt hat und es sind damit – womit ggf. nicht alle Betroffenen rechnen – keine automatischen Löschungsrechte verbunden, die jedoch ohnehin ins Leere laufen würden, wenn beim ursprünglichen Provider noch eine Vertragslaufzeit besteht. Um eine Frustration beim Nutzer zu vermeiden, ist daher das Verständnis und Verstehen wichtig, welche Möglichkeiten ihm das Recht bietet.

WIE KANN PORTABILITÄT DIE BEDÜRFNISSE ERFÜLLEN?

Welcher Lösungen bedarf es, damit Datenportabilität im Gesamten für Nutzer und Unternehmen interessant ist? Aus Nutzersicht kann es zukünftig ein Teil eines modernen Lebens sein, Daten auf allen von ihnen genutzten Plattformen zu teilen, wie etwa Musiklisten. Dennoch stellt der Import oder Export von Daten derzeit noch keinen Alltag dar. Zu bedenken ist, dass Nutzer teilweise außerdem kein Interesse daran haben, sämtliche Daten zu übertragen, sondern nur einen Teil der Daten. Nutzer scheinen jedoch immer noch in der Vorstellung zu leben, dass „Datenportabilität“ die Übertragung aller Daten bedeutet, etwa von einem Sozialen Netzwerk zu einem anderen. Wie kann also das Interesse an Datenportabilität erhöht werden, im Sinne eines Instruments zur Verwirklichung einer Datensouveränität? Muss Datenportabilität nur bequem sein oder müssen finanzielle Aspekte damit verbunden sein? Hierbei ist das Privacy Paradox zu berücksichtigen: Einfache und praktische Instrumente erleichtern zwar den Transfer, allerdings kann ein sorglos implementierter Download-Button auch eine Missbrauchsgefahr beinhalten. Daher müssen sich auf der anderen Seite Unternehmen damit auseinandersetzen, wie in bereits vorhandenen Mechanismen Datenschutz und Datenschutzrichtlinien eingepflegt werden können.

In diesem Zusammenhang stellt die Datenspeicherung eine weitere Herausforderung dar und die damit verbundene Frage, ob es zielführend ist, Daten zentral zu speichern. In diesem Zusammenhang erfolgt oftmals der Verweis, dass man -wie auch in anderen Ländern- einen großen Datentopf schaffen könnte. Andererseits kommt ebenso die aus datenschutzrechtlicher Sicht vorzugswürdigere Variante einer dezentralen Speicherung (beim jeweiligen Nutzer) in Betracht. Insbesondere aus ökonomischer Sicht erfolgt hingegen der Einwand, dass die Frage des Ortes der Speicherung nicht relevant sei und viele Unternehmen nicht an einer Datenspeicherung interessiert sind, sondern dass vorrangige Ziel wäre, Zugang zu den relevanten Daten zu verschaffen.

Aktuell ist der richtige Zeitpunkt, um die grundlegenden Entscheidungen für die praktische Umsetzung zu treffen – wie Datenpolitik in der Zukunft gestaltet werden soll.

UNTER WELCHEN VORAUSSETZUNGEN HANDELT ES SICH BEI EINER DATENÜBERMITTLUNG UM DATENPORTABILITÄT?

Im Rahmen der Workshop – Diskussion wurden ebenso Apps besprochen, die auf Nutzerdaten und Daten Dritter zugreifen. Eine Parallele zur Datenportabilität wird insoweit aus technischer Sicht gezogen, da in beiden Fällen ein rechtswidriger Transfer von Daten stattfinden kann und daher fraglich ist, inwieweit einem Provider im Vorhinein Prüfpflichten obliegen, da er – andererseits – zur Erfüllung des Rechts auf Datenportabilität „ohne Behinderung" die Daten übertragen muss. Sowohl bei einer Aufforderung durch den Betroffenen als auch bei einer App könnte ohne Mitwirkung des Dritten (oder des Nutzers) ein Zugriff auf dessen Daten erfolgen. Allerdings wurde ebenso die Ansicht vertreten, dass es sich im Falle von Apps, die auf Daten zugreifen, nicht um Datenportabilität handelt.

Ergänzend soll in diesem Zusammenhang auf folgendes hingewiesen werden: Geht die Aufforderung zum Transfer der Daten vom jeweiligen Nutzer aus, ist fraglich, inwieweit der Provider ebenso Anfragen ablehnen darf oder sogar muss. Bei der Übertragung von Daten Dritter bedarf es einer Rechtsgrundlage, die gleichermaßen auf Artikel 6 Absatz 1f DSGVO beruhen kann. Die Frage ist allerdings, ob der Provider oder der Nutzer die Interessenabwägung durchführen muss? Den Nutzer treffen grundsätzlich im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten keine Pflichten der DSGVO (Artikel 2 Absatz 2 DSGVO). Im Rahmen der Datenportabilität wird dennoch vertreten, dass dem Provider keine Prüfpflichten obliegen, sondern vielmehr der Nutzer entscheiden muss, welche Daten übertragen werden.[1] Allerdings könnte es auch unter dem Gesichtspunkt „Privacy by design", zu kurz gegriffen sein, wenn dem Provider, der die Technik vollumfänglich bereitstellt, keinerlei Verantwortung obliegen soll. Auch für diese Fälle müssen verbindliche Standards entwickelt werden. Insgesamt stellt dies eine Frage der Rollenverteilung und eine Frage der Regulierung dar.

WAS SIND DIE ANFORDERUNGEN UND GRUNDPRINZIPIEN?

Grundprinzip einer Datenportabilität ist eine umfassende Sichtweise, die alle möglichen Perspektiven (Verbraucher, Technologie, Recht) in die Risiko- aber auch Chancenbewertung mit einbezieht. Zu diesem Zweck können unterschiedliche Mechanismen geschaffen werden. Eine Frage ist, ob es eine Notwendigkeit gibt, den weiteren Begriff der „Datenmobilität" zu verwenden und wie dieser vom Begriff der „Datenportabilität" abzugrenzen ist – ob es sich um zwei unterschiedliche Bereiche handelt. Dies wird insbesondere aus technischer Sicht und unter dem Gesichtspunkt bejaht, dass verschiedene Strategien/Policies benötigt werden.

Es gibt in diesem Bereich bereits zwei Konzepte, die Datenportabilität und Datenmobilität im Fokus haben. Eine Idee kommt aus Großbritannien und wurde von dem Unternehmen Ctrl-Shift entwickelt.[2] Im Fokus steht hier die Datenmobilität in unterschiedlichen Lebensbereichen, wie Gesundheitsmanagement, privates Haushaltsmanagement, privates Finanzmanagement, etc. Ein weiteres Projekt ist insoweit abstrakter definiert, da ein Gesamtkonzept für eine so genannte „New Governance" neu entwickelt werden soll.[3]

CTRL-SHIFT

Im Rahmen dieses Projekt ist geplant, eine Infrastruktur zu entwickeln, die den Einzelnen dabei unterstützt, seine privaten Lebensbereiche zu verwalten. Dazu muss ebenso die Interoperabilität sichergestellt sein. Möglich wäre hier etwa eine so genannte „Sandbox", in welcher der Nutzer von unterschiedlichen Services seine Daten importiert und zu einem anderen Service exportiert. Grundvoraussetzung des Erfolges für dieses Projekt ist vor allem die Sicherstellung der Benutzerfreundlichkeit und nicht nur allein die technologische Umsetzung. Die Herausforderung ist, dies für unterschiedliche Stakeholder und unterschiedliche Personen umzusetzen. Dabei muss ebenso die Frage der Datenspeicherung beachtet werden. Eine Überlegung ist, die Daten zu verlinken, ohne diese an einem zentralen Ort zu speichern.

1 Herbst in: Kühling/Buchner, DSGVO/BDSG, Artikel 20 DSGVO Rn. 17.
2 https://www.ctrl-shift.co.uk/.
3 https://www.privacytech.fr/livre-blanc/.

NEW GOVERNANCE

Dieses Projekt hat die Erarbeitung von Datenverbreitungs- und Schutzstandards im Fokus, um den Herausforderungen in der digitalen Welt besser begegnen zu können.[4]

Für die Umsetzung dieses Projekts sind vor allem Standards und Tools erforderlich. Basis dafür bildet eine demokratische Struktur, welche die Prozesse definiert und Standards unterstützt, aber auch Personen dabei unterstützt, die beste Lösung zu finden. Dazu wird ein unabhängiges Kontrollgremium gebildet, welches die unterschiedlichen Akteure koordiniert. Es sollen technologische Standards für die Portabilität und den Schutz personenbezogener Daten sowie „Good Practices" im Einklang mit den Grundsätzen der DSGVO entwickelt werden. Durch die geplante Prüfung in realen Anwendungsanfällen durch Experten sollen diese direkt von Marktteilnehmern angewendet werden können.

FAZIT

Die ursprüngliche Intention der Datenportabilität, den Wechsel zu datenschutzfreundlichen Netzwerken zu erleichtern, gerät zunehmend in den Hintergrund. Wenn derzeit über Datenportabilität diskutiert wird, steht oftmals der freie Datenfluss im Fokus, dem durch die Richtlinien der Artikel-29-Datenschutzgruppe aufgrund der nahezu grenzenlosen Übertragungsmöglichkeit von Daten über Branchen hinweg, der Weg geebnet wurde. Ein neuer Begriff, der sich herausgebildet hat, ist die Datenmobilität. Diesbezüglich muss noch erarbeitet werden, inwieweit dies andere technische Standards oder abweichende Anforderungen an Policies erfordert. Mit der Transfermöglichkeit von Daten wird ein neuer Wert und Nutzen für die Betroffenen geschaffen. Aber dieser neue Wert benötigt Regulierung. Die Forderung, die sich daher notwendigerweise anschließt, besteht aus datenschutzrechtlicher Sicht darin, Standards zu implementieren, die nach wie vor das Persönlichkeitsrecht der Nutzer in den Mittelpunkt rücken. Hier spielen ebenso ethische Gesichtspunkte eine große Rolle. Es wird in Zukunft mehr und mehr entscheidend sein, dass sich Unternehmen an ethischen Gesichtspunkten orientieren und ihre Unternehmenskultur in diesem Sinne transparent ausrichten. Andererseits müssen die Nutzer die entsprechende Bildung und das Wissen haben, über die Verarbeitung „ihrer" Daten zu entscheiden. Dazu gehört ebenso eine Vorstellung über den damit verbundenen Wert. Insgesamt sind „Law literacy" oder „Data literacy" sind in diesem Kontext die entsprechenden Stichworte, ebenso wie die Vision einer „New Governance", die aufgrund demokratischer, unabhängiger Strukturen Wegbereiter für eine faire und transparente Datenverarbeitung sein kann. Eine digitale Ethik – hier liegt ein langer Weg vor uns.

4 Im April 2019 wurde unter der Leitung von Olivier Dion ein White Paper koordiniert – eine „Neue Governance" für Daten im XXI. Jahrhundert – für das französische Parlament mit 50 Organisationen (einschließlich MyData) aus 14 Ländern. Im Juni 2019 begann die Designphase für diese „New Governance". Siehe hierzu die Informationen unter https://mydata2019.org/presenter/olivier-dion/.

STIFTUNG DATENSCHUTZ

WORKSHOP

#02 – 01.10.2019
ZUSAMMENFASSUNG UND ANALYSE

DATENPORTABILITÄT IN DER PRAXIS

EINLEITUNG

Sowohl im ersten Workshop am 11.09.2019 als auch im Rahmen des zweiten Workshops am 01.10.2019 wurde von einzelnen Teilnehmern darauf hingewiesen, dass in den kommenden Jahren weder gesetzliche Änderungen des Artikel 20 DSGVO noch Änderungen der Leitlinien der Artikel-29-Datenschutzgruppe zum Recht auf Datenübertragbarkeit erwartet werden.[1] Dennoch besteht in der Praxis weiterhin Diskussionsbedarf, insbesondere mit Blick auf neue Geschäftsmodelle. Insgesamt wurden im Rahmen dieses zweiten Workshops die Herausforderungen erläutert, die bei der Entwicklung eines einheitlichen Formats für unterschiedliche Dienstleistungen auftreten können. Mit Blick auf die so genannten „observed data“ wurde zudem die Frage aufgeworfen, wie umfassend dieser Begriff ausgelegt werden sollte und ob eine weite Auslegung dem Persönlichkeitsschutz der Betroffenen zuwiderlaufen könnte. Diskutiert wurde darüber hinaus, ob vom Recht auf Datenübertragbarkeit ebenso weitere Datenumfasst sein könnten, die nicht auf den Rechtsgrundlagen der vertraglichen Erforderlichkeit oder der Einwilligung beruhen. Vor allem von Unternehmerseite wird auf den Bedarf aus Nutzersicht hingewiesen, das Recht auf Datenübertragbarkeit serviceorientiert auszulegen. Auch wenn die Datenethikkommission in ihrem Abschlussbericht die Empfehlung ausgesprochen hat, von einer Erweiterung des Rechts auf Datenportabilität zunächst abzusehen,[2] bedarf es in der Praxis zukünftig dennoch Richtlinien und Evaluierungen, die die Vor- und Nachteile einer Erweiterung abwägen – insbesondere aufgrund etwaiger Geschäftsmodelle in der Praxis. Insgesamt muss für die Beantwortung dieser Fragen stets der Fokus auf auf Erwägungsgrund 68 der DSGVO gerichtet werden: Die Kontrollrechte des Betroffenen sollen gestärkt werden!

1 Die Leitlinien der Artikel-29-Datenschutzgruppe, angenommen am 13. Dezember 2016 zuletzt überarbeitet und angenommen am 5. April 2017, sind in unterschiedlichen Sprachen abrufbar unter: https://sds-links.de/Leitlinien. Der Europäische Datenschutzausschuss bestätigte die mit der Datenschutz-Grundverordnung zusammenhängenden Leitlinien der Artikel-29-Datenschutzgruppe bei seiner ersten Plenarsitzung am 25.05.2018, siehe unter https://sds-links.de/EDPB.

2 Siehe Gutachten der Datenethikkommission, veröffentlicht am 23.10.2019, abrufbar unter https://sds-links.de/Datenethikkommission.

RECHTLICHE AUSGANGSSITUATION

BEREITGESTELLTE DATEN

Das Recht auf Datenübertragbarkeit gemäß Artikel 20 DSGVO ist trotz der ursprünglichen Absicht des Gesetzgebers, den Anbieterwechsel bzw. den Wechsel zu einem datenschutzfreundlichen Netzwerk zu erleichtern – ein Persönlichkeitsrecht. Es handelt sich um ein Betroffenenrecht. Die Leitlinien der Artikel-29-Datenschutzgruppe definieren einen breiten Anwendungsbereich. Danach gilt das Recht auf Datenübertragbarkeit grenzüberschreitend und branchenübergreifend. Es ist sowohl auf Daten anwendbar, die ein Nutzer aktiv für einen Dienst bereitstellt („Bestandsdaten") als auch für so genannte „observed data" („Nutzungsdaten"). Aufgrund dieser weiten Auslegung gab es bereits in der Vergangenheit seitens der Industrie die Forderung, den Begriff „bereitgestellte Daten" auf Daten zu beschränken, die vom Nutzer aktiv bereitgestellt wurden.[3]

DATENSOUVERÄNITÄT

Das Recht auf Datenportabilität wird ebenso mit dem Begriff „Datensouveränität" in Verbindung gebracht. So kann ein Nutzer ohne Angabe von Gründen einen kompletten Datensatz oder Teile davon auf jedweden neuen Anbieter übertragen. Allerdings bleibt die Frage offen, ob „Datensouveränität" mehr bedeutet als das Recht auf informationelle Selbstbestimmung. So scheint es, dass das Recht auf Datenübertragbarkeit einem Nutzer ermöglichen kann, mit seinen Daten zu handeln. Dies kommt vor allem in Betracht, wenn neue Geschäftsmodelle entwickelt werden, die dies unterstützen. Allerdings ist als problematisch hervorzuheben, dass der Wert der Daten nach wie vor unklar bleibt. Es wird hierbei auch vom „bewusst blinden Fleck" des Datenschutzrechts gesprochen.[4] Auch ist unklar, ob der Nutzer die Kompetenz für ein solches „Datengeschäft" hat, da ihm vor allem die Einschätzung schwerfallen wird, welche „beobachteten Daten" oder Nutzungsdaten, die er generiert hat, auch aus einem wirtschaftlichen Blickwinkel heraus als wertvoll betrachtet werden können. In diesem Zusammenhang scheint es nicht eindeutig zu sein, ob es in allen Fällen für den Persönlichkeitsschutz des Betroffenen hilfreich ist, die persönlichen Daten in einem maschinenlesbaren Format zu erhalten, z.B. auch auf Cookies basierende Daten, für die er seine Einwilligung gegeben hat oder eine Link- oder Klickliste, da dies ebenso zu einem „Ausverkauf" von Daten führen kann. Darüber hinaus sollen – gemäß der Ausführungen der Artikel-29-Datenschutzgruppe – die für die Datenverarbeitung Verantwortlichen für den Transfer personenbezogene Daten zusammen mit nützlichen Metadaten auf dem bestmöglichen Niveau der Granularität bereitstellen" sollen.[5] Einige Kritiker sprechen hierbei von einer „alarmierenden" Praxis, einen ganzen Datensatz zu übertragen und im Anschluss zu prüfen, ob die gesamten Daten tatsächlich benötigt werden. So können also eine Menge Daten betroffen sein, für die der Begriff „Datensouveränität" bestimmt werden muss.

RECHTE DRITTER

In Bezug auf die Rechte Dritter hat die Artikel-29-Datenschutzgruppe in ihren Leitlinien als Fallbeispiel einer Datenportabilität den Sachverhalt dargestellt, dass ein Nutzer ein Verzeichnis der Kontakte, Freunde und Familie an einen anderen Anbieter überträgt (Webmaildienst). Als Voraussetzung dieses Beispiels wird jedoch nicht das Erfordernis einer Einwilligung des Dritten genannt. Die Artikel-29-Datenschutzgruppe stellt lediglich klar, dass der neue Anbieter das Verzeichnis nicht für Marketingzwecke verwenden dürfe.[6] An diese Ausführungen schließt sich nun die Frage an, ob sich ein Verantwortlicher dennoch auf berechtigte Interessen gemäß Artikel 6 Absatz 1 f DSGVO oder aber wissenschaftliche Zwecke gemäß Artikel 89 DSGVO stützen könnte oder ob jedwede Verarbeitung untersagt ist. Wäre jedwede Verarbeitung untersagt, würde es sich lediglich um den Wechsel des Speichermediums handeln – wobei jedoch mehr als fraglich ist, ob dies in der Praxis realistisch ist. Auf der anderen Seite ist zu berücksichtigen, dass gemäß Artikel 6 Absatz 1f DSGVO und Artikel 89 DSGVO eine Interessenabwägung stattfinden muss und somit grundsätzlich denkbar wäre, dass

3 Siehe etwa Stellungnahme der Bitkom vom 14.03.2017, abrufbar unter https://sds-links.de/Bitkom. Auf S. 7/8 wird ausgeführt, dass es ausreichend sein sollte, nur die Daten zu berücksichtigen, die der Betroffene kontrolliert und über die er selbst verfügt (z.B. Bilder, E-Mails während der Laufzeit des Vertrages). Dies schließe Nutzungsdaten aus. Insbesondere sollten gemäß Auffassung von Bitkom keine Daten unter das Recht fallen, die bei Nutzung des Dienstes automatisch generiert werden (z.B. Logfiles, Verkehrsdaten).

4 V. Lewinski, Wert von personenbezogenen Daten, in: Stiftung Datenschutz – DatenDebatten III, S. 215.

5 Leitlinien der Artikel-29-Datenschutzgruppe, S. 21.

6 Leitlinien der Artikel-29-Datenschutzgruppe, S. 13.

keine Einwände gegen die Verarbeitung bestehen.[7] Hierzu wäre es vorab erforderlich, entsprechende Kriterien zu entwickeln. So hat die Datenschutzkonferenz eine Liste von Verarbeitungstätigkeiten erstellt, für welche eine Datenschutz-Folgenabschätzung durchzuführen ist. Auch wenn eine solche Liste bezüglich „berechtigter Interessen" keine Vorgabe der DSGVO ist, stellt dies keinen Hinderungsgrund dar, eine solche zu erstellen. Man könnte etwa eine beispielhafte Liste (Negativ- oder Positivliste) gleichermaßen im Rahmen von Verhaltensregeln erarbeiten. Allerdings wäre dies in dem Falle obsolet, wenn von vorneherein jede Übertragung von Daten Dritter zu einem Anbieter ohne entsprechende Einwilligung des Dritten untersagt wäre. Bei diesem Ergebnis wäre jedoch das Beispiel der Artikel-29-Datenschutzgruppe nicht konsistent.

Daher muss insgesamt die Frage beantwortet werden, ob jedwede Verarbeitung durch den neuen Dienstleister ohne Einwilligung des Dritten ausgeschlossen ist (und wie dies in der Praxis sichergestellt werden kann)[8] oder ob eine Verarbeitung – etwa aufgrund berechtigter Interessen – grundsätzlich in Betracht kommen könnte. Darüber hinaus wäre zu klären, ob es weitere persönliche Daten gibt, die außerdem übertragen werden dürften. In diesem Falle müssten die Leitlinien überarbeitet, wobei es ebenso notwendig sein könnte, Verhaltensregeln gemäß Artikel 40 DSGVO zu erarbeiten, die auch „berechtigte Interessen", „Weiterverarbeitung" und „wissenschaftliche Zwecke" betreffen.

In diesem Zusammenhang ist besonders zu beachten, dass diese Frage vom Grundsatz nicht anders beantwortet kann als eine (erlaubte) Datenspeicherung beim ursprünglichen Provider. Regelmäßig speichert der Nutzer zu persönlichen oder familiären Zwecken Daten, wie Fotos, etc., bei einem Dienstleister. Sofern eine solche Speicherung ohne Einwilligung des betroffenen Dritten möglich ist, muss diese Bewertung auch für den neuen Provider gelten. Unterschiede können sich nur dann ergeben, wenn klar ist, dass der neue Provider den vorgegebenen Level der DSGVO nicht einhält.

PROJEKTE IN DER PRAXIS[9]

DATA TRANSFER PROJECT

Im Jahre 2018 wurde das „Daten Transfer Project" ins Leben gerufen, um die Datenportabilität für Nutzer und Dienstleister zu verbessern.[10] In diesem Projekt arbeiten unterschiedliche Unternehmen (wie z.B. Facebook und Google) zusammen. Ziel des Projekts ist es, eine Open-Source-Plattform für die Datenportabilität zu schaffen: Jeder Nutzer soll jederzeit im Internet Daten zwischen Online-Dienstleistern austauschen können. Technisch umgesetzt wird dies mit Hilfe von dienstspezifischen Adaptern. Hierdurch können die vorhandenen APIs für den Zugriff auf Daten verwendet werden, aber dennoch Daten in ein gemeinsames Format und anschließend wieder in die API des neuen Dienstes übertragen werden. Das praktische Ergebnis für die Nutzer ist, dass Daten direkt von und zu jedem Anbieter übertragen werden können, der an diesem Projekt teilnimmt. Anhand eines hypothetischen Beispiels wird im White Paper zum Data Transfer Projekt gezeigt, wie ein Nutzer seine Fotos von Google nach Microsoft OneDrive verschieben kann.[11] Dazu ist die Einbindung der Dateiübertragungsschnittstelle von Google erforderlich, wobei der Nutzer das Ziel auswählen und die Übertragung genehmigen muss. Die ausgewählten Dateien werden automatisch kopiert und an das Ziel weitergeleitet.[12]

TELEKOMMUNIKATIONSSEKTOR

In der Telekommunikationsbranche wurde im Jahre 2017 ebenfalls eine Initiative zur Datenportabilität von unterschiedlichen Anbietern gestartet: Data Portability Cooperation.[13] Es handelt sich um eine Arbeitsgruppe, die von der GSMA moderiert und von europäischen Telekommunikationsunternehmen wie der Deutschen Telekom, Orange

7 Gemäß Artikel 89 GDPR werden angemessene Garantien für die Rechte und Freiheiten der betroffenen Person gefordert.
8 Siehe die Studie der Stiftung Datenschutz „Praktische Umsetzung des Rechts auf Datenübertragbarkeit", S. 250, abrufbar unter: https://sds-links.de/Studie2017.
9 Die Projekte „New Governance" oder CTRL-Shift wurden bereits im Rahmen der ersten Workshop-Diskussion am 11.09.2019 dargestellt. Siehe für weitere Nachweise dort.
10 Siehe zum Data Transfer Project unter https://datatransferproject.dev.
11 Siehe hierzu unter https://datatransferproject.dev/dtp-overview.pdf.
12 Siehe hierzu unter https://datatransferproject.dev/dtp-overview.pdf.
13 Siehe hierzu unter https://sds-links.de/Telekom.

und Telefónica gesteuert wird.[14] Geplant ist, einen gemeinsamen Code of Conduct zu entwickeln. Der Fokus liegt hierbei auf Transparenz und Kontrolle für die Nutzer. Es sollen Tools und Services entwickelt werden, die den Nutzern einen Überblick über die Verwendung ihrer Daten geben und damit die Privatsphäre der Nutzer sicherstellen. Dazu gehören ebenso gemeinsame Datenformate.

HERAUSFORDERUNGEN IN DER TECHNISCHEN UMSETZUNG

FORMATE

Im Rahmen des „Data Transfer Projekts" wird derzeit für Fotos ein erster Anwendungsfall durchgeführt. Hierbei hat sich herausgestellt, dass aufgrund der unterschiedlichen Ausrichtung der Dienstleistungen der Export im Einzelfall mit Schwierigkeiten verbunden sein kann. Zwar können aufgrund der Open-Source-Initiative und des Einsatzes eines entsprechenden Adapters die Formate unterschiedlicher Dienstleister miteinander abgeglichen und Daten transferiert werden. So kann der neue Anbieter beispielsweise den Standort erkennen, welches Telefon und welche Kamera benutzt und welche Daten aufgenommen wurden. Probleme kann es jedoch geben, wenn die Dienste unterschiedliche Services beinhalten, z.B. wenn ein Anbieter ein so genanntes „Social Tagging" bei den Fotografien vornimmt.[15] Probleme beim Datentransfer können ebenso bei anderen Daten als Fotos auftreten, etwa bei Musiklisten oder Videos. An diesen Herausforderungen arbeitet das „Data Transfer Project" derzeit und ist unter anderem mit der Frage konfrontiert, wie etwa die Playlists von unterschiedlichen Diensten zusammengestellt werden können, z.B. der Lieblingssong oder welcher Song mit der Familie geteilt wurde, da es hierfür bislang kein Format gibt. Ebenso kann die Entwicklung neuer Services problematisch sein, da in diesem Falle wiederum ein passendes Format gefunden werden müsste. Herausforderung ist also, mit dem jeweiligen System Schritt zu halten. In der Workshop-Diskussion wurde ebenso darauf verwiesen, dass es kein gängiges Format für Gesundheitsdaten gibt und die Übertragung teilweise per pdf oder CSP erfolgen müsse, so dass die Nutzung von existierenden APIs das Verfahren vereinfachen könnte.

Folglich bleibt insgesamt abzuwarten, bei welchen Services ein gängiges und gemeinsames Datenformat entwickelt werden kann.

In Bezug auf Unternehmen mit kleineren Marktanteilen und kleinen Start-Ups wurde im Übrigen die Wichtigkeit von Open-Source-Projekten bei der Erarbeitung von Standards hervorgehoben, um gerade diesen Unternehmen die Datenportabilität überhaupt zu ermöglichen, zu erleichtern und die Basis für neue Produktentwicklungen zu schaffen, z.B. den Transfer von Standortdaten für (Reise)Empfehlungen oder Fitnessdaten für Versicherungsunternehmen.

INFRASTRUKTUR

Vor allem mit Blick auf die Nutzer ist die Infrastruktur von großer Bedeutung. So werden technische Lösungen erarbeitet, im Rahmen derer der Nutzer der Nutzung durch die exportierende Partei sowie der Nutzung der API durch die importierende Partei zustimmen muss, so dass man unterschiedliche Ebenen von Zustimmung und Autorisierung hat.

Weitere Projekten, wie Ctrl-Shift,[16] fokussieren sich auf Managementsysteme, die für den Nutzer handeln bzw. anstelle des Nutzers der Verwendung der Daten zustimmen sollen. Hiervon kann ebenso die Prüfung der zugrundeliegenden allgemeinen Geschäftsbedingungen mitumfasst sein. Bei diesen Vorschlägen muss natürlich stets der Zweckbindungsgrundsatz beachtet und die Frage beantwortet werden, inwieweit diese Systeme für den Nutzer verständlich und transparent sind. Auf diese Problematik wurde bereits im Rahmen der Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen" vertieft

14 Die GSMA vertritt die Interessen der Mobilfunkbetreiber weltweit. Zu ihr gehören u.a. Hersteller von Mobiltelefonen und Geräten, Softwareunternehmen, Geräteanbieter und Internetunternehmen (siehe https://sds-links.de/Telekom).

15 Betont werden soll an dieser Stelle, dass es sich an dieser Stelle ausschließlich um die technische Darstellung handelt – unabhängig von der Frage der datenschutzrechtlichen Zulässigkeit.

16 Siehe die Auswertung der ersten Workshop-Diskussion vom 11.09.2019. Siehe außerdem die Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen", in der unterschiedliche Datenschutzmanagement untersucht und dargestellt werden, abrufbar unter: https://sds-links.de/PIMS.

eingegangen.[17] Daher muss stets kritisch geprüft werden, inwieweit ein solches System die Anforderungen der DSGVO tatsächlich erfüllen kann. Dennoch ist in diesem Zusammenhang darauf hinzuweisen, dass ebenso die Datenethikkommission nicht nur auf die denkbare Möglichkeit von Treuhandsystemen sondern ebenso auf den Einsatz von Datenschutzmanagementsystemen in der Praxis hingewiesen hat, die zukünftig untersucht werden sollten.[18]

HERAUSFORDERUNGEN IN DER RECHTLICHEN UMSETZUNG

WELCHE DATEN SOLLTEN ÜBERTRAGEN WERDEN?

Fraglich ist, ob auch weitere Daten, die formal nicht von Artikel 20 DSGVO erfasst sind, vom Recht auf Datenübertragbarkeit erfasst sein sollten. Hier könnten sowohl anonyme Daten darunter fallen als auch Daten, die auf anderen Rechtsgrundlagen als den in Artikel 20 DSGVO genannten basieren, z.B. vom Dienstanbieter aufgrund berechtigter Interessen erhoben wurden. Allerdings würde es sich hierbei lediglich um einen freiwilligen Service handeln, den Unternehmen ihren Nutzern anbieten, da derzeit weder die Leitlinien der Artikel-29-Datenschutzgruppe noch das Gesetz eine solche Auslegung unterstützen. In diesem Sinne empfiehlt ebenso die Datenethikkommission in ihrem Abschlussbericht,[19] dass von einer vorschnellen Erweiterung des Portabilitätsrechts, etwa auf andere als bereitgestellte Daten, vorerst abgesehen werden sollte. Dennoch ist eine andere Auslegung zukünftig denkbar. In diesem Falle kann Datenportabilität dazu genutzt werden, den Servicegedanken (mit Blick auf den Nutzer) verstärkt in den Vordergrund zu rücken. Der Datenschutz darf dabei jedoch nicht auf der Strecke bleiben, damit nicht der bereits eingangs genannte „Ausverkauf von Daten" die Folge ist. Im Fokus muss stets stehen, ob die mit Artikel 20 DSGVO verbundene Datensouveränität zum Vorteil des jeweiligen Nutzers ist und der Stärkung seiner Kontrollrechte dient.

In diesem Zusammenhang ist ergänzend auf die Problematik hinzuweisen, dass Datenportabilität nicht mit einer (automatischen) Datenlöschung verbunden ist. So kann es für manche Nutzer unbefriedigend sein, die Daten zu kopieren, da sie ausschließlich einen neuen Dienst nutzen möchten. Es muss also untersucht werden, welche Erwartungen Nutzer haben und danach kann die technische Entwicklung ausgerichtet werden.

IN WELCHEN FÄLLEN HANDELT ES SICH UM DATENPORTABILITÄT?

Werden einfache „One-Klick-Möglichkeiten" von Daten zu einem Dienstleister angeboten, ist fraglich, inwieweit die notwendige Transparenz sichergestellt werden kann, z.B. bei einer Übertragung von Standortdaten an einen anderen Anbieter (im Moment, in dem sie generiert werden) für Empfehlungen.[20] In diesem Zusammenhang ist darauf zu verweisen, dass die Datenethikkommission in ihrem Abschlussbericht empfohlen hat, vorerst von einer Portierung in Echtzeit abzusehen.[21] Insgesamt ist zu betonen, dass Datenportabilität keine Rechtsgrundlage, sondern ein Recht der betroffenen Person darstellt, das von dieser ausgeübt werden muss. Gemäß Artikel 12 DSGVO heißt es in der englischen Fassung „request" und wird in der deutschen Fassung mit „Antrag" übersetzt. Dies bedeutet meint aber nichts anderes, als dass Dienstleister diesem Recht nach Aufforderung durch den Betroffenen innerhalb einer gewissen Zeit nachkommen muss. Es ist wichtig sicherzustellen, dass keine Datenübermittlung ohne willentliche und informierte Entscheidung des Betroffenen stattfindet, die ansonsten einer Rechtsgrundlage bedarf. Bei einem Datentransfer zu einem anderen Dienstleister kann sich daher ebenso die Frage stellen, inwieweit eine Einwilligung gemäß Artikel 7 DSGVO die notwendige rechtliche Basis darstellt. Die Rechtmäßigkeit einer Einwilligung muss vom Verantwortlichen stets nachgewiesen werden und das Ersuchen um Einwilligung unterliegt strengeren Formvorschriften. Die Rechte der Betroffenen

17 Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen", abrufbar unter: https://sds-links.de/PIMS.

18 Siehe Gutachten der Datenethikkommission, veröffentlicht am 23.10.2019, abrufbar unter https://sds-links.de/Datenethikkommission, S. 136.

19 Siehe Gutachten der Datenethikkommission. Unter „Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten", S.21 empfiehlt sie von der Erweiterung des Portabilitätsrechts, etwa auf andere als bereitgestellte Daten oder auf Portierung in Echtzeit, vorerst abzusehen (https://sds-links.de/Datenethikkommission).

20 Die Datenethikkommission nimmt hier auf die Begriffe des „Echtzeit-Streaming von Datenflüssen" sowie dynamische Echtzeit-Portabilität Bezug, siehe S. 137.

21 Siehe Gutachten der Datenethikkommission, S.21.

gemäß Artikel 12 ff. DSGVO knüpfen im Übrigen immer an eine bereits erfolgte (rechtmäßige) Datenerhebung an und ein Dienstleister kann sich nicht auf Artikel 20 DSGVO berufen; er benötigt stets den Antrag bzw. die Geltendmachung des Rechts durch den Betroffenen. Hierbei spielt ebenso die Authentifizierung eine wichtige Rolle. Es muss ein Identifizierungsprozess gestartet werden, und zwar sowohl mit Blick auf den Nutzer als auch mit Blick auf den neuen Provider. Die Frage muss dabei auch sein, inwieweit in Übereinstimmung mit Artikel 6 DSGVO gehandelt wird. In Bezug auf Apps, die Daten zu anderen Dienstleistern weiterleiten, wird auf die Auswertung der ersten Workshop-Diskussion verwiesen.[22] Daran anknüpfend wurde im Rahmen der zweiten Diskussionsrunde erläutert, dass transparente Mechanismen entwickelt werden müssen, damit der Nutzer sicherstellen und entscheiden kann, mit wem er seine Daten teilt. Allerdings wurde in diesem Zusammenhang auf bereits existierende API Mechanismen verwiesen.

Ergänzend könnte die Prüfung erfolgen, ob die Verwendung von API-Mechanismen Einfluss auf die rechtliche Einordnung eines Transfers als Datenportabilität im Sinne von Artikel 20 DSGVO nehmen kann bzw. eine solche ausschließen kann. Zu beachten ist jedoch, dass die Technik nicht das Recht bestimmen sollte, sondern allenfalls die äußeren Umstände Anhaltspunkte für die rechtliche Einordnung geben können. Der Ausgangspunkt der Frage, ob es sich im Einzelfall um die Ausübung des Rechts auf Datenübertragbarkeit handelt, muss daher darauf fokussiert sein, ob es sich um einen (willentlichen) Antrag („request“) des Nutzers handelt bzw. wie ein solcher zu definieren ist. Die zugrundeliegende Technik sollte dafür unerheblich sein.

GEFAHREN BEI DER ERWEITERUNG DES DATENPORTABILITÄTSRECHTS

Grundsätzlich umfassen Betroffenenrechte (gemäß der Artikel 12 – 23 DSGVO) Anforderungen für eine DSGVO-konforme Datenverarbeitung, stellen aber nicht die Rechtsgrundlage für die Verarbeitung von Daten dar. Sie beinhalten auch Maßnahmen, die ein Dienstanbieter umsetzen muss, um den Pflichten nach Artikel 24 DSGVO nachzukommen. Mit Blick auf das Recht auf Datenübertragbarkeit darf daher durch eine serviceorientierte Sichtweise bzw. eine Erweiterung des Begriffs der „bereitgestellten Daten“ die Intention des Artikel 20 DSGVO, die Kontrollrechte des Betroffenen zu stärken, nicht ins Gegenteil verkehrt und eine Basis für Unternehmen geschaffen werden, Daten auf einfachem Weg zu übertragen und zu nutzen. Zu betonen ist wiederum, dass sich ein Unternehmen nicht auf Artikel 20 DSGVO berufen kann, sondern der Nutzer dieses (bewusst) geltend machen muss.

Intention der Datenportabilität war ursprünglich, Daten von einem Sozialen Netzwerk zu einem ggf. datenschutzfreundlicheren Netzwerk zu übertragen. Ausgeschlossen ist derzeit aber ebensowenig, dass branchenübergreifend „One-Klick-Lösungen“ in beide Richtungen angeboten werden: Zum einen ist vorstellbar, dass der ursprüngliche Dienstleister einen Button „Datentransfer“ implementiert (ggf. sogar damit ein Transfer zu Partnerunternehmen veranlasst wird). Zum anderen könnte der neue Dienstleister einen Button „Bring my Data in“ anbieten. Die Frage ist nicht nur, ob damit eine Verarbeitung stattfindet, die ansonsten einer Rechtsgrundlage bedarf, sondern auch, ob damit die Pflichten nach Artikel 30 DSGVO oder Artikel 35 DSGVO ausgehebelt werden könnten. So ist im Rahmen von Artikel 30 DSGVO für jede einzelne Verarbeitungstätigkeit eine Beschreibung nach Maßgabe des Art. 30 DSGVO anzufertigen, wobei als Verarbeitungstätigkeit im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden wird. Dabei soll ein strenger Maßstab angelegt werden, so dass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt.[23] Diese Vorgabe müsste etwa bei der Rechtsgrundlage der Einwilligung erfüllt werden unter Beachtung der Informationspflichten und des Widerrufsrechts. Findet nun eine Datenübertragung statt, z.B. zu einem Dienstleister, der aufgrund der übermittelten Datenbasis dem Nutzer Empfehlungen bereitstellt, ist damit eine Zweckänderung des ursprünglichen Dienstes verbunden. Zieht sich der Dienstleister aber auf den Standpunkt zurück, dass er „lediglich“ die Betroffenenrechte erfüllt, stellt sich die Frage, inwieweit dies tatsächlich noch der Stärkung der Betroffenenrechte entspricht. Der ursprüngliche Dienstleister wäre grundsätzlich vom Nachweis befreit, dass die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden

22 Siehe hierzu die Auswertung der ersten Workshop-Diskussion vom 11.09.2019.
23 Siehe zum Verzeichnis für Verarbeitungstätigkeiten die Ausführungen unter: https://sds-links.de/Verzeichnis

personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat bzw. zur Übermittlung von Daten zu einem anderen Dienstleister zu einem bestimmten Zweck. Der ursprüngliche Provider müsste auch nicht über das Widerrufsrechts informieren. Zwar muss der neue Dienstleister die Rechtmäßigkeit der (anschließenden) Datenverarbeitung nachweisen können. Aber diese muss nicht notwendigerweise auf Vertrag oder Einwilligung beruhen, sondern könnte grundsätzlich ebenso aufgrund berechtigter Interessen erfolgen.

Daher muss entschieden werden, in welchen Fallkonstellationen eine Datenverarbeitung vorliegt, für die eine Rechtsgrundlage (etwa eine Einwilligung) benötigt wird, und in welchen Fällen es sich um Datenportabilität handelt, so dass die Stärkung der Kontrollrechte des Betroffenen im Fokus ist.

FALLGESTALTUNGEN

TRANSFER EINER MUSIKLISTE

Dies kann man als einen typischen Fall von Datenportabilität einstufen, der ebenso in den Leitlinien der Artikel-29-Datenschutzgruppe beispielhaft aufgeführt ist.[24]

TRANSFER VON FOTOS

Beim Transfer von Fotos müssen zunächst die Rechte geklärt werden. Im Rahmen dieser Workshop- Diskussion wurde darauf verwiesen, dass es sich auch im Falle einer gegenständlichen Fotografie (z.B. Sonnenuntergang) um die ursprüngliche Idee der Datenportabilität handelt, nämlich als Nutzer seine Historie zu einem anderen Provider mitnehmen zu können. Ein Nutzer solle eine solche Fotografie ebenso übertragen dürfen wie einen persönlichen Kommentar. Nicht einheitlich diskutiert wurde allerdings, ob es sich um ein personenbezogenes Datum handelt, was für Artikel 20 DSGVO Voraussetzung wäre. Für diese Sichtweise könnte sprechen, dass der Betroffene die Fotografie erstellt hat. Anderenfalls könnte ein solcher Transfer einen zusätzlichen Service darstellen. In diesem Zusammenhang wurde wieder auf den Begriff „Datenmobilität“ verwiesen, aber auch „Datenteilung“ als mögliche Option genannt. Rechtliche Grundlage wäre hierfür die Einwilligung (im Sinne der DSGVO, sofern es sich um ein personenbezogenes oder personenbeziehbares Datum handelt).

In Bezug auf Fotografien muss ebenso bedacht werden, dass auf diesen weitere Personen abgebildet sein können. Soll die Verletzung von Rechten Dritter ausgeschlossen werden, müsste es sich beim Transfer um den Wechsel ausschließlich des Speichermediums handeln. Allerdings zeigt die Praxis, dass regelmäßig eigene Analysen des Datenbestandes durchgeführt werden. Die Frage ist daher, ob ein Verbot der Auswertung bzw. von Datenanalysen in der Praxis überhaupt sichergestellt werden kann.

Hier könnten entsprechende Guidelines unterstützen, die klar festlegen, was unter berechtigte Interessen oder wissenschaftliche Zwecke oder Weiterverarbeitung fällt. Es wäre ein vergleichbarer Sachverhalt, als wenn die Daten beim ursprünglichen Provider gespeichert wären. Auch dieser darf die Rechte des Betroffenen und des Dritten nicht verletzen. Anderenfalls drohen Sanktionen. Dreh- und Angelpunkt ist, dass stets die DSGVO im Blickpunkt stehen und ihr Datenschutzlevel eingehalten werden muss.

DER TRANSFER VON FINANZINFORMATIONEN

In der Praxis werden Services angeboten, die den Nutzern ermöglichen, sämtliche Zahlungsinformationen bzw. die Transaktionshistorie aus ihren Bankgeschäften in eine einzige Schnittstelle zu integrieren (Sparkonto, Aktienkonto, etc.). Hierbei wird eine bestehende API verwendet (PSD2).

Zur Bewertung dessen, ob es sich um Datenportabilität handelt, ist die Richtlinie PSD2 zu berücksichtigen. Ihre Anforderungen müssen erfüllt sein. Aus datenschutzrechtlicher Sicht beinhaltet PSD2 die Notwendigkeit, dass Drittanbieter eine Einwilligung benötigen. Das Vorliegen einer Einwilligung wird durch die Zugangsdaten symbolisiert, die der Nutzer vom Drittanbieter erhält. So können Drittanbieter Bezahlvorgänge direkt auslösen. Aus Verbrauchersicht gibt es nur Kontakt zwischen dem Drittanbieter und dem Kunden und es gibt keine Verbindung zwischen dem Kunden und der Bank. Es ist ein anderer Ansatz, der sich von der Daten-

24 Siehe Leitlinien der Artikel-29-Datenschutzgruppe, S. 5, 9.

übertragbarkeit unterscheidet. Diskutiert wurde, dass es sich aufgrund der spezifischen Vorgaben der PSD2-Richtlinie aus rechtlicher Sicht um Datenzugang handeln soll, auch wenn es aus technischer Sicht der Datenportabilität entsprechend umgesetzt ist.

FAZIT

In der Praxis ist beim Recht auf Datenübertragbarkeit sicherzustellen, dass dieses als Betroffenenrecht und nicht als Unternehmensrecht gehandhabt wird. Datenportabilität dient dazu, eine DSGVO-konforme Verarbeitung sicherzustellen und es darf nicht eine eigene Rechtsgrundlage für neue Services geschaffen werden. In der Praxis besteht gleichwohl die Vorstellung, das Recht auf Datenübertragung zunehmend als Service für die Nutzer zu betrachten und umso wichtiger ist es, dass der Persönlichkeitsschutz des Betroffenen nicht aus dem Blick gerät. So wird oftmals die Übertragungsmöglichkeit von Daten angestrebt, die nicht unter den Begriff der „bereitgestellten Daten" fallen, der in Artikel 20 DSGVO und den Leitlinien der Artikel-29- Datenschutzgruppe definiert ist. Hierbei taucht ebenso die Fragestellung auf, inwieweit Gegenstandsfotografie (z.B. Sonnenuntergang) von dem gesetzlichen Recht auf Datenübertragbarkeit umfasst ist, ob es überhaupt als personenbezogenes Datum zu bewerten ist. Zu berücksichtigen ist in diesem Zusammenhang, dass es noch keine Erfahrungswerte in der Praxis gibt, welche Datenübertragung zur Stärkung der Kontrollrechte beiträgt. In diesem Sinne wurde ebenso von der Datenethikkommission empfohlen, von der Erweiterung des Begriffs der „bereitgestellten Daten" vorerst abzusehen. Eine zukünftige Ausweitung ist jedoch nicht ausgeschlossen, sogar eine Erweiterung durch Schaffung von Fakten in der Praxis scheint nicht ausgeschlossen zu sein. Aus diesem Grunde bedarf es Leitlinien und verhaltensökonomische Studien, die ethische Bewertungsmaßstäbe beinhalten, um den eigentlichen Kern des Rechts auf Datenübertragbarkeit sicherzustellen: Die Stärkung der Kontrollrechte des Einzelnen. Zu berücksichtigen ist in diesem Zusammenhang, dass auch der Begriff der „bereitgestellten Daten" bzw. der Begriff „observed data" nach wie vor bezüglich seines Spielraums einer Definition bedarf. Gerade mit Blick auf mögliche zukünftige Geschäftsmodelle ist nicht auszuschließen, dass ein Konkurrenzunternehmen am Erhalt von Nutzungsdaten, Standortdaten, etc. in einem maschinenlesbaren Format „mit einem Klick" mehr Interesse haben könnte als der Nutzer. Hierzu gehört ebenso eine Definition dahingehend, was unter „Anfrage bzw. Antrag durch den Nutzer" („request") zu verstehen ist. Der Nutzer muss dieses Recht geltend machen bzw. aktiv einfordern. In der Praxis kann die Grenze zwischen „Anschubsen" und „Auffordern" durch ein Unternehmen (mit ggf. eigenen Geschäftsinteressen) jedoch verschwimmen. Daher bedarf es auch hier einer Auslegung und einer Leitlinie, welche Mindestvoraussetzungen vorliegen müssen. Hinsichtlich medizinischer Daten besteht im Übrigen die Forderung, von „One-Klick-Lösungen" grundsätzlich abzusehen.

Die Frage ist, ob Datenportabilität mehr Privatsphäre erlaubt oder ob es zum Gegenteil führt. Insgesamt betrachtet kann in diesem Zusammenhang der Begriff Datensouveränität hilfreich sein, um auf europäischer Ebene ein einheitliches Verständnis für ein modernes Datenschutzrecht zu erlangen und eine europaweite Definition zu entwickeln, da das Recht auf informationelle Selbstbestimmung vom Bundesverfassungsgericht geprägt wurde. Allerdings bedarf es einer Prüfung, was unter Datensouveränität zu verstehen ist und wie diese zugunsten der betroffenen Person umgesetzt werden kann. Es muss ein transparentes Verfahren sichergestellt sein – entsprechend der eigentlichen Bedeutung des Wortes „souverän" als Befähigung zur Ausübung seines Rechts auf Datenübertragbarkeit. Wenn das Recht auf Datenübertragbarkeit daher ein Instrument ist, um Datensouveränität auszuüben, bedarf es in der Praxis der Bereitstellung der dazu erforderlichen Werkzeuge, und zwar im Sinne von einfachen, verständlichen und praktikablen Anwendungen. Nur dann wird das Recht dergestalt umgesetzt, dass ein Betroffener selbständig, überlegen und unbeschränkt handeln kann. Dazu gehört ebenso „law literacy" und ein Verständnis über den möglichen Wert und Nutzen persönlicher Daten für andere, sprich für Unternehmen mit eigenen Geschäftsinteressen.

Mit Datensouveränität darf nicht die Gefahr verbunden sein, dass andere Personen, Institutionen, etc. für den Nutzer nachteilige Entscheidungen treffen. Dies muss ebenso im Kontext von Datenmanagementsystemen und Treuhandmodellen gesehen werden. Die Aufforderung bzw. der Antrag zur Datenübertragung muss stets vom Nutzer als dessen „request" ausgehen.

STIFTUNG DATENSCHUTZ

WORKSHOP

#03 – 01.11.2019
ZUSAMMENFASSUNG UND ANALYSE

PRAKTISCHE HERAUSFORDERUNGEN UND LÖSUNGEN BEI DER IMPLEMENTIERUNG VON DATENPORTABILITÄT

EINLEITUNG

Im Fokus des dritten Workshops stand die Frage, welche Anforderungen erfüllt sein müssen, damit Nutzer befähigt werden, mehr Kontrolle über ihre Daten ausüben zu können. Dazu gehören ebenso angemessene Schutzmaßnahmen, um die Rechte Dritter sicherzustellen, wenn Daten direkt zu einem anderen Provider übertragen werden. Darüber hinaus diskutierten die Teilnehmer über die grundsätzlichen Anforderungen einer zukünftigen Struktur und Governance, die einen fairen und transparenten Datenverarbeitungsprozess in einer umfassenden Weise sicherstellen könnten.

Insgesamt können neu auftauchende Geschäftsmodelle problematisch sein, die den Datentransfer mit finanziellen Anreizen verbinden. Die Stiftung Datenschutz hat bereits im Jahre 2016 in ihrer Studie „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“ auf dieses Risiko hingewiesen.[1] So wird beispielsweise derzeit ein Dienst angeboten, der im Namen seiner Kunden (Abonnenten) deren Recht auf Datenübertragbarkeit ausübt. Der Dienstanbieter fokussiert sich vor allem auf die Übertragung von Daten aus Treueprogrammen und verspricht seinen Kunden entsprechende Vorteile.[2] Alles in allem geht es daher nicht nur um die Frage der Kontrolle, sondern gleichermaßen um die Frage, wie das notwendige Verständnis und die Entscheidungskompetenz beim Nutzer sichergestellt werden kann, insbesondere auch mit Blick auf den Wert der Daten. So wurden etwa „Preisschilder“ für Daten als hilfreich im Rahmen dieser Workshop- Diskussion hervorgehoben. Außerdem wurde auf die Möglichkeit Bezug genommen, dass die Wahrnehmung der Nutzerrechte ebenso durch eine neutrale Organisation ausgeübt werden könnte.

1 Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“, abrufbar unter: https://sds-links.de/PIMS.

2 https://sds-links.de/IAPP: „Kurz gesagt, um die Dienste der Plattform zu fördern, einschließlich der Ausübung des Rechts auf Portabilität im Namen der betroffenen Personen, verspricht Weople seinen Abonnenten Vorteile, die proportional zur Menge und Qualität der personenbezogenen Daten sind, die der Plattform übertragen und über verschiedene Quellen gesammelt werden (im Wesentlichen die Treueprogramme, bei denen die betroffenen Personen ein Abonnement haben), die die Plattform zur Schaffung von kommerziellem Wert nutzt.“

KONTROLLE

Im Rahmen der Diskussion wurde hervorgehoben, dass in der Vergangenheit bereits viel getan wurde, um die Aufmerksamkeit der Nutzer auf Datenschutzprobleme zu lenken. Besonders wichtig ist neben der transparenten Ausgestaltung von Dienstleistung und der damit verbundenen transparenten Darstellung der Datenverarbeitung jedoch gleichermaßen die Bereitstellung von Alternativen: Die Betroffenen müssen eine Wahl zwischen unterschiedlichen Dienstleistungen haben. Die Schaffung von Transparenz, etwa mittels Icons, oder die Bereitstellung von datenschutzfreundlicher Technik können daher allein keine Lösungen darstellen. Für wirkliche Autonomie oder Souveränität ist eine Entscheidungsmöglichkeit zwischen unterschiedlichen Dienstanbietern, aber gleichermaßen Entscheidungsfähigkeit erforderlich. Eine besondere Herausforderung kann dabei die Fülle von Informationen darstellen. So besteht die Gefahr, dass die Aufmerksamkeit des Nutzers sinkt, je mehr Informationen bereitgestellt werden. Hier spielt wieder die bereits in den ersten beiden Workshop- Gesprächen diskutierte so genannte „Law literacy“ oder „Data literacy“ eine bedeutende Rolle. In diesem Zusammenhang wurde auf öffentliche Kampagnen als mögliches Modell hingewiesen, die dazu dienen könnten, Nutzer über ihre Rechte zu informieren.

Als übergeordnetes Modell zur Schaffung von Transparenz und Kontrolle wurde die bereits im ersten Workshop- Gespräch diskutierte so genannte „New Governance“ als Option benannt. Zur Umsetzung dieses Models wurde als besonders wichtig hervorgehoben, dass zunächst die Unternehmen motiviert werden sollten, Anwendungsfälle zu bilden, die für sie von Vorteil sind. In der Praxis könnte dies am besten durch Unternehmen sichergestellt werden, die nicht im direkten Wettbewerb zueinander stehen. Gleichermaßen muss eine Orientierung an den Nutzerbedürfnissen erfolgen, um die Masse der Nutzer anzusprechen.

RECHTE DRITTER

In Bezug auf die Rechte Dritter wurde die Möglichkeit einer Einwilligung diskutiert. So könnte eine Nachricht an die betroffene Person gesendet und diese um Erlaubnis gefragt werden. Auf der einen Seite wurde erwartet, dass in einer Vielzahl der Fälle dieser Prozess sehr schnell von Statten gehen könnte – auch wenn mehrere Personen eingebunden sind (z.B. bei einem Foto, auf welchem mehrere Personen abgebildet sind). Auf der anderen Seite wurde der Einwand erhoben, dass es gerade im Rahmen von Sozialen Netzwerken für die Nutzer überfordernd und unpraktisch sein könnte, täglich mehrmals der Übertragung von Daten zustimmen zu müssen. Zu berücksichtigen ist in diesem Falle ebenso das Beispiel der Artikel-29-Datenschutzgruppe zur Übertragung von Kontaktdaten zu einem anderen Webmailanbieter.[3] Eine Einwilligung des Dritten wird von der Artikel-29-Datenschutzgruppe nicht als Voraussetzung der Übertragung genannt, lediglich ein Verbot der Nutzung für eigene Zwecke, wie Marketingzwecke. Allerdings ist damit die weitere Frage verbunden, wie dies in der Praxis sichergestellt werden kann und ob es andererseits eine erlaubte Nutzung, etwa aufgrund „berechtigter Interessen“ oder „wissenschaftlichen Forschungszwecken“ geben könnte.[4] Die Stiftung Datenschutz hat im Rahmen ihrer rechtlichen Auswertung des zweiten Workshop-Gesprächs auf die Möglichkeit von Guidelines oder Verhaltensregeln, ggf. auch in Form einer Positiv- oder Negativliste verwiesen. Auch wenn das Verfahren abgestimmter Verhaltensregeln gemäß Artikel 40 Absatz 7 bis Absatz 10 DSGVO längere Zeit in Anspruch nehmen kann, scheint es sich um einen lohnenswerten Weg zu handeln. So kann den unterschiedlichen Datenschutzlevels der Dienste begegnet werden und Unternehmern und Nutzern eine Entscheidungshilfe an die Hand gegeben werden. Nutzer werden regelmäßig nicht ohne weiteres bzw. ohne Hilfestellung die Entscheidung treffen können, ob sie mit der Verarbeitung ihrer Daten bei einem neuen Dienst einverstanden ist. Gerade mit Blick auf Fotografien sind die Stichworte „Tagging“ und „Tracking“ (etwa wenn aufgrund eines entsprechenden Algorithmus die Gesichter der Freunde „getrackt“ werden) zu nennen. Hierzu könnte eine Einwilligung

3 Leitlinien der Artikel-29-Datenschutzgruppe, S. 13. Die Leitlinien der Artikel-29-Datenschutzgruppe, angenommen am 13. Dezember 2016 zuletzt überarbeitet und angenommen am 5. April 2017, sind in unterschiedlichen Sprachen abrufbar unter: https://sds-links.de/Leitlinien. Der Europäische Datenschutzausschuss bestätigte die mit der Datenschutz-Grundverordnung zusammenhängenden Leitlinien der Artikel-29-Datenschutzgruppe bei seiner ersten Plenarsitzung am 25.05.2018, siehe unter https://sds-links.de/EDPB.

4 Siehe zu dieser Frage die rechtliche Auswertung des zweiten Workshop-Gesprächs.

erteilt werden, aber es ist ebenso möglich, von diesen Praktiken abzusehen. So kann die Erstellung der Verhaltensregeln die Etablierung eines Standards für konkrete Anwendungsbeispiele unterstützen. In der Regel dürfte damit auch verbunden sein, dass den Nutzern bekannt wird, welche Provider welche Praktiken weiterhin ausüben, da bzw. wenn diese sich nicht an Standards halten. Das Befolgen und das Bekenntnis zu abgestimmten Standards könnte gleichermaßen als Marketinginstrumente dienen, etwa durch eine prominente Hervorhebung auf den entsprechenden Unternehmenswebseiten.

Insgesamt ist es wichtig, die technischen Möglichkeiten im Blick zu behalten und im Rahmen eines fortwährenden Prozesses die unterschiedlichen Anwendungsfälle hinsichtlich ihrer Vereinbarkeit mit dem Persönlichkeitsrecht der Betroffenen (im Sinne von Nutzern und Dritten) zu untersuchen und die Standards fortzuschreiben. Dies hat ebenso unmittelbaren Einfluss auf ein transparentes Verfahren, wenn für Dienste – sowohl im Rahmen der ursprünglichen als auch im Rahmen der Verarbeitung nach einem Datentransfer – die ethisch vertretbaren und rechtlich zulässigen Möglichkeiten klar aufgezeigt werden.[5] Denn ebenso stellt sich beim ursprünglichen Provider mit Blick auf das Persönlichkeitsrecht des Dritten die Frage, ob ein Foto ohne dessen Einwilligung gespeichert werden darf – auch wenn die Speicherung für den Nutzer zu ausschließlich privaten oder familiären Zwecken erfolgt. In diesem Zusammenhang wird auf die rechtliche Auswertung der Stiftung Datenschutz des zweiten Workshop-Gesprächs verwiesen.

VERANTWORTLICHKEIT

In der Literatur wird die Auffassung vertreten, dass der Nutzer die Verantwortung für den Transfer der Daten trägt und dafür zu sorgen hat, dass keine Verletzung von Rechten Dritter stattfindet.[6] Dies könnte einerseits unter dem Aspekt „Privacy by Design“ zu kurz gegriffen sein. Andererseits ist zu berücksichtigen, dass Nutzer oftmals Daten für persönliche oder familiäre Zwecke verarbeiten. Daher wird der Nutzer bzw. der Betroffene im Sinne der DSGVO regelmäßig keine Verantwortung haben. Auch im Workshop wurde die Ansicht vertreten, dass es in der Verantwortung des ersten, die Daten übertragenden Providers liegen könnte, eine entsprechende Einwilligung einzuholen. Andererseits wurde die Verantwortung des ursprünglichen Providers auch insoweit kritisch gesehen, dass er diese „Macht“ nicht als Steuerungsinstrument bei einem potenziellen Wechsel einsetzen dürfe. Er sollte damit weder das „Ob“ eines Wechsels beeinflussen noch Warnung aussprechen dürfen („rote Flaggen“). Eine Prüfung sollte sogar verboten sein und er sollte die Daten ohne weiteres übertragen dürfen. In diesem Zusammenhang wurde außerdem die Möglichkeit vorgeschlagen, die Prüfung oder etwaige Warnungen durch eine Behörde vornehmen zu lassen.

Zurzeit gibt es keine entsprechende Verpflichtung zur Prüfung durch den Provider – weder im Sinne des Gesetzes noch gemäß der Leitlinien der Artikel-29-Datenschutzgruppe. Vielmehr soll gemäß den Leitlinien der Artikel-29-Datenschutzgruppe der empfangende Provider die rechtliche Verantwortung für die anschließende Verarbeitung der Daten tragen. In diesem Sinne wird darauf verwiesen, dass als Rechtsgrundlage für die Übermittlung und die anschließende Verarbeitung der Daten ebenso berechtigte Interessen gemäß Artikel 6 (1f) DSGVO in Betracht kommen können.[7] Aber insgesamt bedarf es auch hierzu (wie oben bereits geschildert) einer grundlegenden Entscheidung, klarer Vorgaben und ggf. Standards, um ein transparentes Verfahren sicherzustellen.

5 Siehe hierzu die Auswertung des zweiten Workshop- Gesprächs.
6 Herbst in: Kühling/Buchner, DSGVO/BDSG, Artikel 20 DSGVO Rn. 17.
7 Herbst in: Kühling/Buchner, DSGVO/BDSG, Artikel 20 DSGVO Rn. 18.

INTEGRITÄT EINER INFRASTRUKTUR BZW. EINES ÖKOSYSTEMS

Im Fokus der Diskussionsteilnehmer stand ebenso (wie in der Einleitung bereits dargestellt) die grundsätzliche Frage der Gestaltung einer zukünftigen Datenpolitik und einer damit verbundenen Governance-Struktur. In diesem Zusammenhang wurden – über die formalen Anforderungen an Datenportabilität hinaus – unterschiedliche Modelle diskutiert, die in der Praxis die notwendige Transparenz und Fairness insgesamt sicherstellen könnten. Hierbei wurde gleichermaßen auf mögliche Monetarisierungsinteressen hingewiesen, die im nachfolgenden Punkt nochmals separat behandelt werden.

Als Instrumente für ein transparentes, vertrauenswürdiges und faires Verfahren wurden im Rahmen dieses dritten Workshop-Gesprächs die Einführung von Standards sowie eine neutrale Organisation diskutiert (wie oben bereits dargestellt). Eine solche neutrale Organisation könnte auch zwischen dem Nutzer und dem jeweiligen Provider etabliert sein – etwa im Sinne einer Plattform, auf die bereits im Rahmen des zweiten Workshop-Gesprächs Bezug genommen wurde. Dies wäre eine dritte Person – im Sinne einer Vertrauensperson – die die Nutzer vertritt und deren Rechte wahrnimmt.[8] Die genannten Standards sollen Teil einer digitalen Infrastruktur sein. Betont wurde, dass dabei ebenso die Sicherstellung von Neutralität wesentlich sei – ohne wirtschaftliche Interessen im Zusammenhang mit dem Betrieb des Systems. Insbesondere wurde auf die gesellschaftliche Relevanz neutraler Sozialer Netzwerke, neutraler E-Mail- und Chat-Lösungen hingewiesen. Zurzeit gebe es zwar standardisierte Datenformate, aber andererseits fehlten noch viele weitere notwendige Standards, wie etwa technische, rechtliche Standards, Geschäftsmodellstandards, Designstandards, Branchennormen. Die Vision ist, diese Richtlinien unter einer einzigen Infrastruktur zu vereinigen. Dazu wäre ein gemeinschaftliches Interesse notwendig, da dies ansonsten von keinem Unternehmen und von keiner Institution allein umgesetzt werden könnte. Vorgeschlagen wurde ein Leitungsorgan, beispielsweise organisiert in Form einer öffentlichen Einrichtung oder einer gemeinnützigen Einrichtung, um alle Interessen auf demokratische Weise einzubeziehen und die Regeln und Standards festzulegen, so dass kein einzelnes Interesse die Oberhand gewinnt, sondern vielmehr alle Interessen vertreten sind: Private Unternehmen, Wissenschaftler, Institutionen, die eine öffentlich-private Partnerschaft eingehen. So könnten unterschiedliche Fallgestaltungen unter Einbindung aller Interessen abgestimmt und auf bereits vorhandenes Know-How zurückgegriffen werden.[9]

In Bezug auf die Standardisierung von Messengerdiensten wurde zum Vergleich auf das offene E-Mail-Protokoll Bezug genommen, das sich nicht nur in der Praxis als funktionsfähig bewährt habe, sondern ebenso neue Geschäftsmodelle und neue Funktionalitäten ermögliche. Bei Messengerdiensten handele sich dagegen um Silos. Dagegen wurde argumentiert, dass es technisch nicht schwierig sei, einen sicheren Kommunikationsmechanismus für Messenger zu etablieren, aber Unternehmen oftmals kein Interesse daran hätten, sondern in ihren Silos verweilen möchten. Außerdem wurde auf den möglichen Wettbewerbsnachteil kleinerer Unternehmen verwiesen, wenn sie mit einem größeren Messengerdienst interagieren. Weiterführende Hinweise zur Frage der Interoperabilität von Sozialen Netzwerken und Messengerdiensten sind im Annex zu finden, in dem unterschiedliche Stellungnahmen zusammengefasst sind.

Mit Blick auf die „Integrität von Diensten“ wurde ebenso die Möglichkeit von PIMS-Systemen diskutiert, die bereits im Jahre 2016 Gegenstand der Studie „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“ der Stiftung Datenschutz waren.[10] Allerdings kann – je nach Ziel und Ausgestaltung dieser Systeme – die Implementierung des datenschutzrechtlichen Zweckbindungsgrundsatzes eine große Herausforderung darstellen. Zudem benötigen diese Systeme ebenso entsprechende Standards, um Transparenz sowie eine faire Datenverarbeitung umzusetzen und damit Akzeptanz und Vertrauen beim Nutzer zu erzeugen. Vor allem muss der Nutzer in der Lage sein, dass System zu verstehen und einfach zu handha-

8 Siehe hierzu die bereits angesprochenen Treuhandmodelle, die auch unter dem Punkt „Monetarisierunginteressen“ nochmals aufgegriffen werden. Dies wurde bereits im zweiten Workshop-Gespräch thematisiert und ebenso die Datenethikkommission hat die nähere Erforschung dieser Modelle angeregt.

9 Dies umfasst die Idee einer „New Governance“, so dass insoweit auf die Auswertung des ersten Workshop-Gesprächs verwiesen wird.

10 Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“, abrufbar unter: https://sds-links.de/PIMS.

ben. Grundsätzlich orientiert sich die Umsetzung vieler PIMS-Systeme an einem Verfahren, wie es bereits vom altbekannten Protokoll P3P umfasst war:[11] P3P ist ein kostenloses Protokoll und ermöglicht die maschinenlesbare Beschreibung von Datenschutzerklärungen.

Zur Sicherstellung der Integrität können weiterhin „Zertifizierungen" beitragen. Diesbezüglich wurde im Rahmen der Diskussion betont, dass der Nutzer sich auf diese verlassen können muss. Außerdem müsse eine Prüfung und Vergabe von einer unabhängigen neutralen Organisation durchgeführt werden. Dies entspricht insoweit den Vorgaben des Artikel 42 DSGVO. Gemäß dem Kurzpapier Nr. 9 der Datenschutzkonferenz „Zertifizierung nach Artikel 42 DS-GVO" arbeiten die Aufsichtsbehörden des Bundes und der Länder an der Entwicklung abgestimmter, länderübergreifend geltender Kriterien, um einen „Wildwuchs" zahlreicher unterschiedlicher Zertifizierungsverfahren – so die Datenschutzkonferenz – gerade mit Blick auf ein einheitliches europäisches Datenschutzniveau im Interesse aller Beteiligten zu vermeiden.[12] Der Nutzer muss in diesem Zusammenhang ebenso einordnen können, ob ein gesamtes System zertifiziert wurde oder nur ein Teil davon. Wenn letzteres der Fall sein sollte, muss transparent sein, welche Auswirkung dies auf die Sicherheit der Daten des Betroffenen und auf dessen Persönlichkeitsrecht hat.

Insgesamt betrachtet stellt es eine wesentliche Anforderung dar, dass Betroffenen und Dritten klare, transparente und verbindlich geklärte Rechte in der Praxis zustehen. Standards und Zertifizierungen können dabei unterstützen. Dies könnte auch das sogenannte „Fatigue-Problem" lösen.

MONETARISIERUNGSINTERESSEN

Mit dem bereits in der Einleitung dargestellten Fall, dass ein Unternehmen im Namen seiner Abonnenten das Recht auf Datenübertragbarkeit ausübt, ist das Problem der Marktgängigkeit von personenbezogenen Daten verbunden. Außerdem besteht die Gefahr, dass das Unternehmen diese Daten kopiert und für eigene Zwecke nutzt – was den Nutzerinteressen entgegenläuft. In diesem Kontext wäre daher ebenso eine Befragung hilfreich, an welchen Daten tatsächlich ein Transferinteresse aus Nutzersicht besteht. So wurde in der Diskussion darauf hingewiesen, dass oftmals kein Interesse an der Übermittlung eines veralteten Datenbestandes besteht – dazu könne in der schnelllebigen Zeit etwa bereits der Tweet aus der letzten Woche gehören. Darüber ist es ebenso wichtig, Untersuchungen dahingehend durchzuführen, welche Rohdaten für einen Transfer aus Nutzer- und Unternehmenssicht interessant sind – unter Abwägung der Chancen und Risiken und ggf. unter neuer Definition des Begriffs „observed data", der sich an der Stärkung der Kontrollrechte des Betroffenen ausrichtet.[13]

Mit Blick auf die Monetarisierung von Daten ist weiterhin stets die Frage verbunden, ob ein Nutzer aufgrund der Komplexität des Verarbeitungsprozesses überhaupt in der Lage ist, eine souveräne Entscheidung zu treffen. Daher wird in Literatur und Praxis gleichermaßen die Etablierung einer neutralen, unabhängigen Organisation diskutiert, die diese Rechte für die Nutzer ausüben könnte. Im aktuellen Workshop-Gespräch wurde darauf verwiesen, dass nicht dieselbe Organisation gleichzeitig die Monetarisierung und die Rechte wahrnehmen darf.

In diesem Zusammenhang soll ergänzend seitens der Stiftung Datenschutz auf die folgenden Überlegungen verwiesen werden: In der digitalen Realität wird mit Daten gehandelt. Diese Realität wird aus rechtlicher Sicht untermauert, da die *Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und Dienstleistungen*[14] gilt (Artikel 3), wenn der Unternehmer dem Verbraucher digitale Inhalte oder digitale Dienst-

11 Die nachfolgende Beschreibung von P3P ist den bereits durchgeführten Studien und Gutachten der Stiftung Datenschutz zu entnehmen, und zwar S. 10 der Studie "Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen", abrufbar unter https://sds-links.de/Studie2016 und S. 6 „Rechtliche Aspekte (Riechert)" https://sds-links.de/Riechert zu entnehmen: "Die betroffenen Personen nehmen Voreinstellungen bezüglich der von ihnen präferierten Datennutzung vor und beantworten im Vorfeld eine standardisierte Liste von Multiple-Choice-Fragen zum gewünschten Umgang mit seinen personenbezogenen Daten. Erforderlich ist, dass sowohl Nutzer als auch Webseiten-Betreiber dieses Protokoll implementieren. sodass ein automatisierter Vergleich dahingehend erfolgen kann, ob die Datenschutzerklärung einer Webseite mit den Voreinstellungen des Nutzers zum Datenschutz übereinstimmt. So erscheint bei Abweichungen ein Warnhinweis (z. B. bei der Akzeptanz von Cookies). P3P wird jedoch vom Windows-Browser seit der Version Windows 10 nicht mehr unterstützt und Microsoft empfohlen hat, das Bereitstellen von P3P-Datenschutzrichtlinien auf den Webseiten zu vermeiden." Siehe außerdem https://sds-links.de/Microsoft, wo beschrieben ist, dass Microsoft P3P nicht mehr unterstützt.

12 Siehe Kurzpapier Nr. 9 der Datenschutzkonferenz, abrufbar unter https://sds-links.de/Zertifizierung.

13 Siehe hierzu die rechtliche Auswertung des zweiten Workshops.

14 Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, abrufbar unter https://sds-links.de/DigitaleInhalte.

leistungen bereitstellt oder deren Bereitstellung zusagt und der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt. „*Ziel ist es, auch Verbraucher, die keine Gegenleistung in Geld erbringen im Verhältnis zu Anbietern dieser Inhalte in eine, zahlenden Kunden vergleichbare, Position zu bringen.*“[15] Vielfach wird auch darauf hingewiesen, dass Verbraucher ein Interesse daran hätten, am Wertschöpfungsprozess ihrer Daten beteiligt zu werden.[16] Die wirtschaftliche Verwertung war aber bislang nicht vorgesehen. So wird auch vom „bewusst blinden Fleck“ des Datenschutzrechts gesprochen.[17] In der Praxis wird Daten also ein wirtschaftlicher Wert zugesprochen – auch wenn die Datenethikkommission dafür plädiert, von der Bezeichnung „Daten als Gegenleistung“ abzusehen.[18] Allerdings wird auch im Gutachten der Datenethikkommission ebenso ausgeführt, dass die DSGVO bereits heute in vielfacher Weise die wirtschaftliche Verwertung personenbezogener Daten erlaubt und neben die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) fünf weitere Rechtfertigungstatbestande treten, die teils explizit auf wirtschaftliche Interessen und Bedürfnisse zugeschnitten sind.[19] Daher drängt sich umso mehr die Frage einer notwendigen Teilhabe in den Vordergrund. So wird insgesamt in Literatur und Praxis diskutiert, den Einzelnen an der Wertschöpfung der von ihm generierten Daten teilhaben zu lassen. Teilhabe ist Bestandteil eines demokratischen und freiheitlichen Systems.[20] Dieser Grundgedanke der Wertschöpfung wird im Übrigen von der Datenethikkommission insoweit aufgegriffen, indem die Empfehlung ausgesprochen wird, in § 311 BGB die Sonderbeziehung zwischen einer Partei, welche zur Generierung von Daten in einem Wertschöpfungsprozess faktisch beitragen hat, und der Partei, welche die Daten faktisch kontrolliert, explizit anzuführen.[21] Andere Auffassungen verweisen darauf, dass es dem Einzelnen heute nicht mehr möglich ist, sein Selbstbestimmungsrecht „mangels Erfahrung und Komplexität der Datenverarbeitung“ auszuüben und daher Treuhandmodelle in Betracht kommen (entsprechend der Handhabung im Urheberrecht).[22] Abstrakter wird auf die Möglichkeit eines Repräsentativorgans verwiesen, das Bürgerrechte wahrnimmt.[23] Wichtig bei der Umsetzung solcher Vorschläge ist allerdings stets, die etwa in der Literatur geäußerten Bedenken zu berücksichtigen: „Wer überwacht die Wächter“?[24]

Insgesamt muss die Monetarisierung von Daten also auch unter dem Aspekt untersucht werden, in welcher Form ein Repräsentativorgan ausgestaltet sein muss, um die Rechte der Betroffenen ausüben zu können – mit Blick auf alle möglicherweise damit verbunden Gefahren für das Persönlichkeitsrecht des Betroffenen.

FAZIT

Insgesamt können Standards unterstützen, das Vertrauen der Nutzer in die vorhandene Infrastruktur zu stärken. Das Geschäftsmodell eines Unternehmens ist ansonsten zu komplex. Der Nutzer soll darauf vertrauen können, dass das Verfahren rechtskonform ausgestaltet ist und nicht seinen Interessen zuwiderläuft. Hier könnte ein paralleler Prozess angestoßen werden: Es könnten Verhaltensregeln erstellt werden, die mittels bestimmter Anwendungsfälle in der Praxis in eine konkrete Form überführt und stets fortgeschrieben werden. So können verbindliche Standards geschaffen werden. Ein Bekenntnis zu einem Standard seitens eines Unternehmens schafft zudem gleichermaßen Vertrauen in dieses Unternehmen und kann als Marketinginstrument dienen.

15 Siehe S. 1 in: Die Richtlinienvorschläge der Kommission zu Verträgen über digitalen Inhalt und Online-Warenhandel von Joachim Bokor, abrufbar unter: https://sds-links.de/Bokor

16 Specht, Stiftung Datenschutz – DatenDebatten III, S. 313 weist etwa in Bezug auf Verbraucher darauf hin, dass diese entsprechend ihres Beitrags am Wertschöpfungsprozess von Daten ein Interesse daran haben, beteiligt zu werden, also neben einem datenschutzrechtlichen Interesse auch ein Monetarisierungsinteresse besteht.

17 V. Lewinski, Wert von personenbezogenen Daten, in: Stiftung Datenschutz – DatenDebatten III, S. 215. V. Lewinski spricht vom „bewusst blinden Fleck“ des europäischen Datenschutzrechts und einem bewussten Nicht-Wahrnehmen der Marktgängigkeit von personenbezogenen Daten, die dazu führten, dass es an einer für Vertragsgerechtigkeit sorgenden Marktordnung fehle.

18 Siehe Gutachten der Datenethikkommission, S. 105. In diesem Zusammenhang stellt die Forderung der Datenethikkommission, Verbrauchern jeweils zumutbare Alternativen gegenüber der Freigabe von Daten zur kommerziellen Nutzung anzubieten (etwa entsprechend ausgestaltete Bezahlmodelle), ein außerordentlich wichtiges verbraucherschutzrechtliches Instrument dar.

19 Siehe Gutachten der Datenethikkommission, S. 141.

20 Fezer, Digitales Dateneigentum – ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft, in: Stiftung Datenschutz – DatenDebatten III, der die Teilhabe und Gestaltungsmöglichkeit im Rahmen des Dateneigentums diskutiert.

21 Gutachten der Datenethikkommission, S. 22, 147, 156.

22 Buchner, Eigentumsrechte an persönlichen Daten?, DGRI Jahrbuch 2011, Köln 2012, S. 51, 58.

23 Fezer, Digitales Dateneigentum – ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft, in: Stiftung Datenschutz – DatenDebatten III, S. 152: „Die repräsentative Wahrnehmung von Bürgerechten stellt ein ureigenes Prinzip der Organisation demokratischer Gesellschaftsordnungen dar.“

24 Diese Frage stellt Schneider, Regulierungsansätze in der Datenökonomie, S. 9 – abrufbar unter https://sds-links.de/Schneider.

Konkrete Anwendungsfälle können insbesondere die Chancen und Risiken einer Datenportabilität aufzeigen, was letztendlich dazu führt, dass Standards gebildet werden können. Dies beeinflusst ebenso die Transparenz einer Dienstleistung, wobei öffentliche Kampagnen dies unterstützen könnten. Auf diese Weise kann ein Lernprozess in der praktischen Durchführung dahingehend gestartet werden, wie eine Information bereitgestellt werden sollte und vor allem welche Informationen dem Nutzer besonders deutlich präsentiert werden sollten, damit dieser eine autonome und souveräne Entscheidung dahingehend treffen kann, die Möglichkeit der Datenportabilität zu nutzen oder auch nicht. Auf diese Weise können im Laufe der Zeit insgesamt mehr und mehr Standards entwickelt werden. Dies kann ein langer, aber lohnenswerter Prozess sein. Denn die technische Entwicklung ist nicht abzusehen und mittels konkreter Anwendungsfälle sowie unter Berücksichtigung von Diensten, die eine Vielzahl von Nutzern in Anspruch nehmen, kann auf die Probleme in der Praxis besonders gut reagiert werden. Repräsentativorgane können bei diesem Prozess eine entscheidende Rolle spielen, um die notwendige Neutralität sicherzustellen. Mit Blick auf die Monetarisierung von Daten geht es in diesem Kontext ebenso um faire Teilhabemöglichkeiten am Wertschöpfungsprozess von Daten.

Insgesamt bedarf es einer Aufgaben- und Machtverteilung, um eine neutrale Infrastruktur zu schaffen und Interessen mittels einer demokratischen Struktur einzubeziehen. Organisiert werden könnte dies in Form einer öffentlichen oder gemeinnützigen Einrichtung. Eine wichtige Voraussetzung für das Gelingen ist die Zusammenarbeit unterschiedlicher Unternehmen, Organisationen und Einrichtungen. So können gemeinsame, offene Standards entwickelt werden, um den Datentransfer für alle in der Praxis umzusetzen.

STIFTUNG
DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

gestiftet von der Bundesrepublik Deutschland
vertreten durch den Vorstand Frederick Richter