STIFTUNG DATENSCHUTZ

Praktische Umsetzung des Rechts auf Datenübertragbarkeit

Rechtliche, technische und verbraucherbezogene Implikationen

Practical Implementation of the Right to Data Portability

Legal, Technical and Consumer-Related Implications

Studie

Januar 2018
3. Auflage

geringfügige Aktualisierungen im Anhang in den Abschnitten
g. ONECUBE, Dion, ab Seite 154 ff.
h. regiocom GmbH, Gutmann, ab Seite 170 ff.
i. Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF), Drepper, Schlünder, Buckow, ab Seite 178 ff.
j. TU Berlin Service-centric Networking, Göndör, ab Seite 198 ff.

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

Übersicht / Overview

Praktische Umsetzung des Rechts auf Datenübertragbarkeit

Rechtliche, technische und verbraucherbezogene Implikationen

Dr. Nikolai Horn, Prof. Dr. Anne Riechert,
Stiftung Datenschutz

Zusammenfassung

Mit der europäischen Reform des Datenschutzrechts wird ein Rechtsinstrument eingeführt, das neue Anforderungen an die Praxis beim Umgang mit personenbezogenen Daten stellt. Die EU-Datenschutzgrundverordnung gibt in ihrem Artikel 20 jeder natürlichen Person das „Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“.

Die Nutzer sind also zukünftig berechtigt, die sie betreffenden personenbezogenen Daten einer anderen Organisation zu übermitteln, ohne dabei von der ursprünglichen Organisation behindert zu werden. Mit diesem im Datenschutzrecht neuen Instrument sollen Monopole verhindert und Nutzer gleichsam aus großen Netzwerken „befreit“ werden. Der Reformgesetzgeber hofft, dass mit der Mitnahmemöglichkeit für „eigene“ Daten die Schwelle zum Wechsel des Anbieters digitaler Dienste sinken wird und die Verbraucher bessere Kontrollmöglichkeiten über ihre personenbezogenen Daten erhalten.

Wie dieser theoretisch plausible Mechanismus in der Praxis funktionieren kann, ist noch nicht konkretisiert. Wirtschaftsunternehmen und Aufsichtsbehörden haben bislang gleichermaßen keinerlei Erfahrung, da es weder eine Vorgängerregelung noch eine vorhandene richterliche Rechtsfortbildung gibt, wie etwa bei dem vom Europäischen Gerichtshof entwickelten und in der Verordnung aufgegriffenen „Recht auf Vergessenwerden“.

Aus diesem Grund untersucht die Stiftung Datenschutz in der vorliegenden Studie rechtliche, technische und verbraucherbezogene Implikationen des neuen Rechts und gibt Empfehlungen zur Nutzbarmachung des neuen Instruments. Zunächst wird der Regelungsgegenstand von Art. 20 DSGVO aufgezeigt und auf wesentliche Problemfelder bei der Umsetzung der Norm eingegangen. Sodann werden bestehende nationale und internationale Lösungsansätze zur Datenportabilität vorgestellt und die auf den Call for Papers[1] der Stiftung eingegangenen Beiträge sowie Empfehlungen externer Sachverständiger ausgewertet. Schließlich gibt die Studie Empfehlungen bezüglich der Zielsetzung der Norm, der Bestimmung des Anwendungsbereichs sowie hinsichtlich möglicher Umsetzungsstrategien und technischer Realisierung.

In Bezug auf die Zielrichtung der Norm wird dargelegt, dass das Recht auf Datenportabilität den Nutzern grundsätzlich bessere Kontrollmöglichkeiten über personenbezogene Daten verschaffen kann. Eine zu weite Auslegung der Norm könnte unter Umständen jedoch Datenschutzrisiken vergrößern und zugleich unverhältnismäßig großen Aufwand beim Kategorisieren und Herausziehen von Datensätzen bei den datenverarbeitenden Stellen bereiten. Daher sollten bei der Interpretation des Art. 20 DSGVO nur solche Daten erfasst werden, deren Übertragbarkeit tatsächlich zur Förderung der informationellen Selbstbestimmung beiträgt. Der Aufwand für die Normumsetzung muss verhältnismäßig sein, auch im Hinblick auf den tatsächlichen Nutzen für die Verbraucher.

1 *https://stiftungdatenschutz.org/themen/projekt-datenportabilitaet.*

Zur Frage des rechtlichen Anwendungsbereichs regen wir an, dass die Aufsichtsbehörden eine über die Stellungnahme der Artikel-29-Datenschutzgruppe hinausgehende Präzisierung und Eingrenzung dahingehend vornehmen sollten, was unter „bereitgestellten Daten“ zu verstehen ist. Bei der Frage, ob sowohl Vertrags- als auch Nutzungsdaten vom Anwendungsbereich erfasst sind, sollte im Einzelfall und dienstbezogen entschieden werden, ob dadurch tatsächlich die Kontrollrechte der betroffenen Person verbessert werden. Von außerordentlicher Bedeutung ist ebenso die Sicherstellung von ausreichender Transparenz im Hinblick auf die Verarbeitung durch den früheren und neuen Verantwortlichen sowie die Abgrenzung zum Auskunftsrecht. Hinsichtlich des Datenformats und der geforderten Interoperabilität ist das Wettbewerbsrecht ergänzend zu berücksichtigen. Der Schutzzweck der Norm, nämlich den Anbieterwechsel zu erleichtern, muss zum Tragen kommen. Zur Schaffung von Orientierung muss schließlich bei der länderspezifischen Auslegung von Art. 20 DSGVO auf eine europäische Harmonisierung hingewirkt werden.

Bei der Analyse geeigneter Umsetzungsstrategien für das Recht auf Datenübertragbarkeit zeigen wir, dass vor allem durch Ansätze „regulierter Selbstregulierung“ ein Rahmen etabliert werden kann, in dem Aufsichtsbehörden, NGOs und Unternehmen Umsetzungsstrategien und Standards für die Datenportabilität entwickeln. Für eine effektive Ausgestaltung der Datenübertragbarkeit und Herstellung von Rechtskonformität ist außerdem eine frühzeitige Einbindung der voraussichtlich besonders betroffenen Unternehmen und Branchen in formelle Konsultationsprozesse der Aufsichtsbehörden empfehlenswert. Bei der praktischen Umsetzung der Datenportabilität kommen je nach Anwendungsbereich und Verarbeitungskontext sowohl branchenspezifische als auch universelle Lösungsansätze in Betracht. Bei sektorübergreifenden Ansätzen können Personal Information Management Systems (PIMS) eingesetzt werden. Falls sich nur eine sehr geringe Nachfrage nach Datenübertragungen gem. Art. 20 DSGVO zeigen sollte, könnte auf einzelfallbezogene, direkte Übertragung von Datensätzen zurückgegriffen werden.

Bei der Frage nach der technischen Gestaltung der Datenportabilität und den Anforderungen an ein geeignetes kompatibles, interoperables Format zeigen wir, dass es Mindestvoraussetzung ist, die Daten im einfachsten CSV-Format zu schreiben und eine einfache Beschreibung beizufügen, wie die Daten in der Datei angeordnet sind. Für komplexere Lösungen bieten sich XML oder JSON an. Diese beiden Standards erfüllen die Anforderungen der Maschinenlesbarkeit und der Interoperabilität. Sie enthalten die Daten sowie die beschreibenden Metadaten und haben aufgrund ihrer Struktur ausreichende Tiefe, um auch komplexe Datengerüste abbilden zu können. Die enthaltenen Informationen können außerdem mit Standardsoftware von dem Betroffenen selbst gelesen werden, was zugleich die Wahrnehmung der Informationsrechte der Nutzer unterstützt. In jedem Fall erscheint es notwendig, die zu übertragenden Daten zu verschlüsseln. Bei der technischen Umsetzung der Datenübertragbarkeit muss außerdem sichergestellt werden, dass verschiedene Lösungen durch offene Schnittstellen grundsätzlich interoperabel sind.

Inhaltsverzeichnis

A. Gegenstand der Regelung in Art. 20 DSGVO

I. Das Recht auf Datenübertragbarkeit

1. Ziel der Regelung

Ende Mai 2018 bekommen die EU-Bürger ein neues Rechtsinstrument – das Recht auf die Übertragung ihrer personenbezogenen Daten zwischen verschiedenen Dienstanbietern (Art. 20 DSGVO). Während das bisherige Datenschutzrecht für die verantwortlichen Stellen in dieser Hinsicht lediglich die Auskunftspflicht beinhaltete, soll die neue Regelung einer Person ermöglichen, „die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“ oder unmittelbar an einen anderen Verantwortlichen übertragen zu lassen. Die Idee hinter dieser Regelung ist, den Nutzern die freie Wahl zwischen konkurrierenden Internetdiensten zu ermöglichen, sodass sie in einem einmal gewählten Dienst nicht „eingeschlossen“ werden (sogenannter „Lock-in-Effekt“). Die Norm bezweckt, dass diejenigen personenbezogenen Daten, die einem Verantwortlichen im Rahmen eines Vertrages oder sonst mit Einwilligung des Nutzers zur Verfügung gestellt wurden, auf Wunsch des Nutzers ohne Kosten oder Behinderung ihm oder einer anderen Stelle übermittelt werden können. Dadurch sollen vor allem Asymmetrien aufgehoben werden, die Kunden daran hindern, den Anbieter zu wechseln. Die Kundenbindung durch proprietäre Verarbeitungsformate – wie beispielsweise im „Apple-Ökosystem“ – soll damit gelockert werden[2] und dadurch der Nutzerschaft im Sinne von „Datensouveränität“ mehr Wahlfreiheit bei der Entscheidung zwischen unterschiedlichen Dienstanbietern ermöglichen. Das Recht auf Datenportabilität soll eine Übertragung von personenbezogenen Daten ermöglichen, wie es beispielsweise bereits bei Postnachsendeauftrag, Portierung von Mobilfunknummern, Kontowechsel oder Übertragung des Schadenfreiheitsrabatts beim Wechsel einer Fahrzeugversicherung der Fall ist. So wären zukünftig Situationen vorstellbar, in denen ein Leasingnehmer eines Fahrzeuges die Übermittlung der Informationen zu seinem Fahrverhalten an einen anderen Leasinggeber verlangen könnte, um bessere Konditionen zu erzielen.[3]

2. Inhalt der Regelung

Durch das Recht auf Datenübertragbarkeit sollen die Nutzer berechtigt werden, ihre persönlichen Daten, die sie einer Institution zur Verfügung gestellt haben, einer anderen Organisation zu übermitteln, ohne dabei von dem ursprünglichen Datennehmer behindert zu werden.

Die wesentlichen Voraussetzungen für das Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO sind im Einzelnen folgende:

- Es muss sich um personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO handeln, das Recht ist auf natürliche Personen beschränkt.

- Grundlage der Datenverarbeitung ist eine Einwilligung des Nutzers oder ein Vertrag mit diesem (Art. 20 Abs. 1a DSGVO).

2 *Sperlich, T., Das Recht auf Datenübertragbarkeit, DuD 6/2017, S. 377.*

3 *Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, S. 73.*

- Der Nutzer hat die betreffenden Daten dem Verantwortlichen „bereitgestellt“, also diejenigen Daten, über die die Person Kontrolle hat und auf die sie selbst zurückgreift: Daten, welche vom Datennehmer durch Verarbeitungsprozesse automatisch generiert wurden, bleiben von der Regelung unberührt.

- Die Verarbeitung erfolgt mithilfe automatisierter Verfahren (Art. 20 Abs. 1b DSGVO).

Was die **technische Realisierbarkeit** anbetrifft, so wird durch die Regelung hervorgehoben, dass die Weitergabe der Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“ (Art. 20 Abs. 1 DSGVO) erfolgen muss, wobei „die Verantwortlichen dazu aufgefordert werden [sollten], interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen“ (Erwägungsgrund 68). Die betroffene Person darf außerdem verlangen, dass die Übermittlung direkt von einem Verantwortlichen zu dem anderen erfolgt, „soweit dies technisch machbar“ ist (Art. 20 Abs. 2 DSGVO).

Das Recht auf Datenübertragung soll außerdem das **Recht auf Löschung** von personenbezogenen Daten nach Art. 17 DSGVO nicht berühren (Art. 20 Abs. 3 S.1 DSGVO; Erwägungsgrund 68). Das Recht auf Datenübertragung ist daher kein unmittelbares Recht auf Löschung und löst damit auch keine eigenständige Pflicht zur Löschung aus. Im Grunde entsteht also damit das Recht auf den Erhalt einer „Kopie“[4] der zur Verfügung gestellten personenbezogenen Daten. Die Anforderung der Datenübertragung durch den Nutzer stellt auch keine konkludente Kündigung dar.[5]

In Art. 20 Abs. 3 S. 2 DSGVO wird außerdem klargestellt, dass das Recht auf Datenübertragbarkeit nicht für die Verarbeitung gilt, „die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“. Werden die personenbezogenen Daten also in **Erfüllung öffentlicher Aufgaben** verarbeitet (darunter auch für Archiv-, Statistik- oder Forschungszwecke), kann dieses Recht nicht gegen Verantwortliche ausgeübt werden.[6] Vom Recht auf Datenübertragbarkeit sind außerdem personenbezogene **Daten Dritter** nicht erfasst (Art. 20 Abs. 4 DSGVO), da sie die informationelle Selbstbestimmung anderer Personen betreffen.

Gemäß Art. 13 Abs. 2b bzw. Art. 14 Abs. 2c DSGVO muss der Verantwortliche über das Recht auf Datenübertragbarkeit informieren. Art. 13 Abs. 2b DSGVO verlangt die Information zum Zeitpunkt der Datenerhebung.

Wird das Recht auf Datenportabilität vom Betroffenen ausgeübt, hat dies keinen Einfluss auf etwaige Speicherfristen. Auch das Auskunftsrecht (Art. 15 DSGVO) bleibt hiervon unberührt. Es bezieht sich auf jedes personenbezogene Datum, ohne dass der Betroffene dieses im Sinne von Art. 20 DSGVO bereitstellen musste. Das Recht auf Datenübertragbarkeit und das Auskunftsrecht gem. Art. 15 DSGVO können einander so ergänzen.

Macht der Betroffene von seinem Widerrufsrecht aus Art. 7 Abs. 3 DSGVO oder von seinem Widerspruchsrecht aus Art. 21 DSGVO Gebrauch, kann er das Recht auf Datenübertragung so lange ausüben, wie der Verantwortliche die Daten verarbeitet und diese nicht gleichzeitig einem Löschungsanspruch unterliegen. Gemäß den Empfehlungen der Artikel-29-Datenschutzgruppe sollte der Betroffene vor Schließung eines Accounts daher auf das Recht auf Datenübertragbarkeit explizit hingewiesen werden.

4 Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, S. 74.

5 Vgl., Hennemann, Datenportabilität, PinG 01.17, S. 7.

6 Erwägungsgrund 68 DSGVO.

3. Erwartungen und Reaktionen [7]

Positive Erwartungen

Die Reaktionen auf die Einführung des Rechts auf Datenübertragbarkeit fallen unterschiedlich aus. Von den Befürwortern der neuen Regelung wird Art. 20 DSGVO als Katalysator eines Wettbewerbs um datenschutzfreundliche Technologien angesehen.[8] So wurde beispielsweise im Grünbuch „Digitale Plattformen" des Bundesministeriums für Wirtschaft und Energie (BMWi) das neue Recht positiv eingeschätzt, da durch die Erleichterung des Plattformwechsels „sowohl der Innovationswettbewerb als auch der Konditionswettbewerb gefördert werden",[9] (allerdings unter dem Vorbehalt der praxistauglichen Umsetzung[10]). Auch die Verbraucherzentrale Bundesverband begrüßte in einer Stellungnahme zum Grünbuch des BMWi die Einführung der Regelung ausdrücklich, da dadurch – eine effektive Umsetzung vorausgesetzt – ein wirksames Mittel geschaffen werde, um sowohl Datensouveränität in der digitalen Welt als auch den Wettbewerb zwischen Plattformen zu befördern.[11] In der Erstfassung der Guidelines der Artikel-29-Datenschutzgruppe vom 13. Dezember 2016 wurde betont, dass die Regelung auf die Förderung von neuen Geschäftsmodellen mit mehr Datenkontrolle ziele.[12] Auch im jüngst erschienenen Gutachten des Sachverständigenrats für Verbraucherfragen wird dem Recht auf Datenportabilität eine hohe Relevanz für die Ausübung digitaler Souveränität beigemessen. Das Gutachten fordert sogar, das Recht auf Datenportabilität als Kündigungsrecht zu betrachten.[13]

Nicht nur in Europa, auch in den USA wird das Thema Datenübertragbarkeit intensiv verfolgt. So wurde im Rahmen der öffentlichen Konsultation des White House Office of Science and Technology Policy (OSTP) von vielen Stakeholdern die Datenportabilität als ein wichtiges Instrument zur Steigerung des Wettbewerbs und Verbesserung der Kontrolle durch Nutzer benannt.[14]

Die positiven Erwartungen an die Auswirkungen der Datenportabilität werden schließlich auch von den Entwicklern von Personal Information Management Services (PIMS) betont: Die Datenübertragbarkeit und Wiederverwendung bestehender Datensätze ermöglichten den Ausbau und die Effizienzsteigerung von personalisierten Online-Diensten mit den gleichzeitig verbesserten Möglichkeiten zur Datenkontrolle durch die Nutzer.[15]

7 Auf einzelne Stellungnahmen sowie Stellungnahmen zu den Guidelines der Artikel-29-Datenschutzgruppe wird ausführlicher im Abschnitt B. eingegangen.

8 Albrecht, CR 2016, 88, 93.

9 Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, S. 73.

10 Weissbuch Digitale Plattformen. Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe, S. 76 f. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.pdf__blob=publicationFile&v=22

11 Grünbuch Digitale Plattformen, Stellungnahme des Verbraucherzentrale Bundesverbands v. 26. September 2016, S. 18.

12 Article 29 Data Protection Working Party, Guidelines on the right to data portability, 13 December 2016, S. 5.

13 Sachverständigenrat für Verbraucherfragen, Digitale Souveränität, Juni 2017, S. 26.

14 White House Office of Science and Technology Policy. Request for Information Regarding Data Portability. 10.01.2017. URL: https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/OSTP-Data%20Portability-RFI-Responses_for_humans.pdf.; Macgillivray, A., Summary of Comments Received Regarding Data Portability, 10.01.2017. URL: https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability

15 Vgl., Stellungnahme von ONECUB, siehe Anlage.

Kritische Reaktionen

Es gibt viele Stimmen, die der neuen Regelung eher skeptisch gegenüberstehen. Da das Recht seinen Ursprung in wettbewerbsrechtlichen Bemühungen habe, „Lock-in-Effekte" zu vermeiden,[16] wird bezweifelt, ob es sich als Instrument des Datenschutzrechts in das System der Betroffenenrechte ohne Weiteres integrieren lasse.[17] Nach Auffassung des Bundesrates ist das Recht auf Datenübertragung „mehr darauf ausgerichtet, den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen, als ihre Persönlichkeit zu schützen"[18]. In einer Analyse des Instituts der deutschen Wirtschaft Köln wird u.a. dargestellt, dass die Datenportabilität zwar förderlich für die Datensouveränität des Einzelnen sei, sich aber in bestimmten Fällen vor allem auf den Wettbewerb von Start-ups und kleineren Unternehmen schädlich auswirken könne.[19] Die Hoffnung des Normgebers, dass ein erweitertes Selbstbestimmungsrecht des Betroffenen über seine Daten zu leichterem Wechsel zu anderen Anbietern führt und damit große Marktmonopole und „Netzwerkeffekte" aufbricht, erscheint einigen Beobachtern als nicht hinreichend begründet.[20] Außerdem wird bemängelt, dass der ursprünglichen Stoßrichtung der Regelung, nämlich einer Vermeidung von „Lock-in-Effekten" bei sozialen Netzwerken, von Art. 20 DSGVO nur begrenzt genützt werde, weil ebendort größtenteils Rechte Dritter beeinträchtigt werden würden (etwa der Facebook-„Freunde").[21]

Weiterhin wird kritisiert, dass vom Anwendungsbereich des Art. 20 DSGVO auch Branchen erfasst würden, in denen die erwähnten „Lock-in-Effekte" gar keine Rolle spielten. Obwohl die Vorschrift für dortige Geschäftsmodelle „zu weit" reiche, könne sie gleichwohl Probleme bei der ausnahmslos notwendigen Umsetzung bereiten.[22] Außerdem werden oft Sorgen geäußert, dass die Umsetzung der Norm (insbesondere für KMU) mit hohen Kosten und Risiken verbunden sein könne, bei gleichzeitig geringem Wert für die Nutzer.

Nicht zuletzt wird auch kritisiert, dass die Anforderungen an die technische Realisierbarkeit der Datenportabilität nur vage seien. Dies betrifft einerseits die rechtliche Unsicherheit bezüglich der Formulierung „soweit technisch realisierbar", da von Fall zu Fall schwer zwischen fehlender Realisierbarkeit und ungerechtfertigter Behinderung unterschieden werden könne.[23] Andererseits geht es um das Verständnis dessen, was eigentlich ein „gängiges Format" sei und wie die Interoperabilität zwischen unterschiedlichen „gängigen", jedoch nicht interoperablen Formaten[24] gewährleistet werden solle.[25]

16 Herbst, in Kühling/Buchner, DS-GVO, Art. 20, Rn4; Hennemann, Datenportabilität, PinG 01.17, S. 6.

17 Sperlich, T., Das Recht auf Datenübertragbarkeit, DuD 6/2017, S. 377; Moos, Datenportabilität – Eine Gefahr für daten-getriebene Unternehmen?, eu-datareg v. 2.3.2016, aufrufbar unter: http://eudatareg.com/datenschutz-im-unternehmen/datenportabilitaet-eine-gefahr-fuer-daten-getriebene-unternehmen/; Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, S. 74. BITKOM, Stellungnahme zum Recht auf Datenübertragbarkeit nach Art. 20 Datenschutz-Grundverordnung, 14.03.2017. S. 4.

18 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, 21. Dezember 2016; www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf

19 https://policyreview.info/articles/analysis/data-portability-among-online-platforms; https://www.iwkoeln.de/studien/iw-kurzberichte/beitrag/barbara-engels-nicht-immer-gut-datenportabilitaet-zwischen-online-plattformen-300089.

20 Kühling/Martini, EuZW 2016, 451; Hennemann, Datenportabilität, PinG 01.17, S. 8.

21 Hennemann, Datenportabilität, PinG 01.17, S. 8; Jülicher, Röttgen, v. Schönfeld, Das Recht auf Datenübertragbarkeit, ZD 8/2016, S. 359, 361.

22 Moos, Datenportabilität – Eine Gefahr für daten-getriebene Unternehmen?, eu-datareg v. 2.3.2016, aufrufbar unter: http://eudatareg.com/datenschutz-im-unternehmen/datenportabilitaet-eine-gefahr-fuer-daten-getriebene-unternehmen/; Jülicher, Röttgen, v. Schönfeld, Das Recht auf Datenübertragbarkeit, ZD 8/2016, S. 361.

23 Moos, Datenportabilität – Eine Gefahr für daten-getriebene Unternehmen?, eu-datareg v. 2.3.2016, aufrufbar unter: http://eudatareg.com/datenschutz-im-unternehmen/datenportabilitaet-eine-gefahr-fuer-daten-getriebene-unternehmen/

24 Hennemann, Datenportabilität, PinG 01.17, S. 7.

25 Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, S. 74.

II. Empfehlungen der Artikel-29-Datenschutzgruppe

1. Zusammenfassung der Empfehlungen

Die Artikel-29-Datenschutzgruppe hat am 13. Dezember 2016 Empfehlungen zum Recht auf Datenübertragbarkeit verabschiedet und am 5. April 2017 eine überarbeitete Version beschlossen.

Aus Sicht der Artikel-29-Datenschutzgruppe beinhaltet das Recht auf Datenportabilität im Wesentlichen die Möglichkeit für Betroffene, auf einfache Art und Weise „ihre" Daten für ihre Zwecke behalten, kontrollieren und wiederverwenden zu können, und zwar auch beim Wechsel zwischen unterschiedlichen Dienstleistern. Nach den Empfehlungen der Artikel-29-Datenschutzgruppe sollen davon nicht nur solche persönlichen Daten der Betroffenen umfasst sein, die auf Grundlage einer Einwilligung oder eines Vertrages automatisiert verarbeitet werden und von den Betroffenen aktiv zur Verfügung gestellt wurden (etwa E-Mail-Adresse, selbstgewählter Benutzername, Alter). Es sollen vielmehr gleichermaßen Daten erfasst sein, die anhand der Nutzungsaktivitäten eines Service oder Gerätes festgestellt werden (z.B. Protokolle der Nutzeraktivitäten oder Webseitennutzung). Allerdings macht die Artikel-29-Datenschutzgruppe deutlich, dass das Recht auf Datenübertragbarkeit keine Nutzerprofile betrifft, da diese regelmäßig nicht vom Betroffenen bereitgestellt, sondern vom Datenverantwortlichen erstellt werden. Im Hinblick auf persönliche Daten von Dritten, die von der Datenportierung betroffen sind, wird klargestellt, dass der Empfänger der Daten diese nur verarbeiten darf, sofern eine entsprechende gesetzliche Grundlage besteht.

Das Recht auf Datenübertragbarkeit soll gemäß den Empfehlungen der Artikel-29-Datenschutzgruppe insgesamt ohne Behinderung sowie systemunabhängig mit der Möglichkeit ausgeübt werden können, Daten zu kopieren, in einem eigenen privaten Gerät zu speichern oder auch von einer IT-Umgebung in die eines anderen Datenverantwortlichen zu übertragen. Die Datenverantwortlichen sollten dementsprechend Prozesse etablieren, die dem Betroffenen sowohl das Gesuch auf Datenübertragung ermöglichen als auch dessen Authentifizierung sicherstellen. Die darauffolgende Datenübermittlung solle entweder in der direkten Übertragung des gesamten Datensatzes erfolgen oder durch ein automatisiertes Tool, welches das Herausfiltern der relevanten Daten ermöglicht. In den Bereichen, in denen es keine gängigen Formate gibt, sollten offene Formate verwendet und mit möglichst vielen Metadaten auf bester Granularitätsstufe bereitgestellt werden. Es wird darauf verwiesen, dass ein Format gewählt werden solle, welches sämtliche Metadaten beibehält, die für eine effektive erneute Verwendung der Daten relevant sind. Der Datenverantwortliche solle dabei bedenken, ob das gewählte Format den Betroffenen an der Wiederverwendung seiner Daten hindern könnte (wie z.B. ein bloßes PDF vom Posteingang eines E-Mail-Postfachs).

Im Übrigen legt die Artikel-29-Datenschutzgruppe den Fokus nicht auf ein bestimmtes, sondern vielmehr auf ein interoperables Datenformat; sie fordert keine Kompatibilität der Systeme der Datenverantwortlichen. Sie betrachtet die Vorgabe der Datenschutzgrundverordnung, Daten in einem strukturierten, gängigen und maschinenlesbaren Format bereitzustellen, als Mindestvoraussetzung für die Umsetzung der Interoperabilität und fordert zwecks Entwicklung von interoperablen Standards und Formaten eindringlich zu Kooperationen zwischen Industrie und Wirtschaftsverbänden auf.

In zeitlicher Hinsicht soll das Recht auf Datenübertragbarkeit durch den Betroffenen gemäß den Empfehlungen der Artikel-29-Datenschutzgruppe so lange ausgeübt werden können, wie der Datenverantwortliche die Daten verarbeitet. Der Datenverantwortliche solle in Abhängigkeit vom Einzelfall bis zu drei Monate nach Eingang des Gesuchs Zeit haben, Informationen über die ergriffenen Maßnahmen zur Verfügung zu stellen. Gemäß Art. 12 Abs. 3 Datenschutzgrundverordnung sei zwar eine Monatsfrist vorgesehen. Bei komplexen Sachverhalten könne diese jedoch verlängert werden, sofern der Datenverantwortliche den Betroffenen innerhalb eines Monats über die Verzögerung und deren Gründe informiere.

Die Artikel-29-Datenschutzgruppe verweist zudem darauf, dass mit der Datenübertragung die Servicedienstleistung des Datenverantwortlichen nicht automatisch ende, sondern die Betroffenen den Dienst weiterhin nutzen könnten. Damit sei weder eine Löschung der Daten verbunden, noch habe die Ausübung dieses Rechts Einfluss auf die Speicherfrist. Die verantwortliche Stelle habe auch nicht die Möglichkeit, die Ausübung anderer Rechte (etwa Auskunftsrechte oder Widerrufsrechte) hinauszuzögern oder zu verweigern, sofern die Betroffenen die Datenübertragung verlangen.

Im Rahmen der Informationspflichten aus Art. 13 Abs. 2b und Art. 14 Abs. 2c DSGVO solle der Datenverantwortliche deutlich über die unterschiedlichen Arten von Daten informieren, hinsichtlich derer ein Recht auf Datenübertragbarkeit oder ein Recht auf Auskunft (Art. 15 und Erwägungsgrund 63) besteht. Die Information über das Recht auf Datenübertragbarkeit soll gemäß der Empfehlung der Artikel-29-Datenschutzgruppe von den Datenverantwortlichen auch stets explizit gegeben werden, bevor die Betroffenen einen möglichen Account schließen. Klarstellend führt das Gremium in seinen Empfehlungen außerdem aus, dass der Datenverantwortliche hinsichtlich der portierten Daten nicht mehr für die Einhaltung der Grundsätze der Datenschutzgrundverordnung verantwortlich sei, nachdem er der Anfrage auf Datenübertragbarkeit nachgekommen ist. Zuvor müsse er allerdings sicherstellen, dass nur Daten übertragen werden, die die Betroffenen auch übertragen möchten. Der Empfänger der Daten müsse dann als neuer Verantwortlicher die Pflichten gemäß Art. 5 DSGVO erfüllen (faire und transparente Datenverarbeitung, Zweckbindung, Datenminimierung, Richtigkeit, Integrität und Vertraulichkeit, Speicherbegrenzung und Rechenschaftsverpflichtung). Der ursprüngliche Datenverantwortliche solle zudem dafür Sorge tragen, dass nur solche Daten bereitgestellt werden, die für den neuen Datenverarbeitungsprozess beim Datenempfänger erheblich sind, und dass die Betroffenen auch darüber vollständig informiert werden. Vor einem Gesuch auf Datenübertragung müsse der Datenempfänger schließlich über den Zweck des neuen Datenverarbeitungsprozesses informieren. Die Artikel-29-Datenschutzgruppe verwendet die Formulierungen „clearly and directly“ sowie „state“.[26] Hier stellt sich zukünftig die Frage, ob diese Begriffe in allen Mitgliedsstaaten der Europäischen Union einheitlich ausgelegt bzw. mit derselben inhaltlichen Bedeutung übersetzt werden.

26 „Therefore, the „new“ receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14.“

2. Vergleich der Fassungen von Dezember 2016 und April 2017

Obwohl in der vorangestellten Zusammenfassung der revisionierten Fassung vom 5. April 2017 auf die Förderung des Wettbewerbs zwischen den Datenverantwortlichen weiterhin Bezug genommen wird, wurde dieser Punkt insgesamt in den Empfehlungen der Artikel-29-Datenschutzgruppe entfernt. Nunmehr wird betont, dass es im Rahmen der Datenportabilität hauptsächlich um die Verbesserung der Kontrollrechte der Betroffenen über ihre persönlichen Daten gehe. Damit wurde der Fokus klar auf datenschutzrechtliche Aspekte verlagert.[27]

Die Artikel-29-Datenschutzgruppe hat ihre Entscheidung, wonach Datenverantwortliche nach einer Datenübertragung nicht für die weitere Verarbeitung sowie die Einhaltung der Verordnung durch den Empfänger verantwortlich seien, dahingehend präzisierend begründet, dass sich die vormals Verantwortlichen den Empfänger nicht ausgesucht hätten (S. 5 und S. 6/neu).

Weiterhin wurde zur Wahrung der Betroffenenrechte ergänzt, dass ein Vertrag zur Auftragsdatenverarbeitung (Art. 28 DSGVO) die Verpflichtung des Auftragsverarbeiters beinhalten müsse, den Verantwortlichen bei der Durchführung von Datenportierungen durch geeignete technische und organisatorische Maßnahmen zu unterstützen. Beide sollten daher gemeinsam Prozesse einführen, um Anfragen zur Datenportabilität zu beantworten. Im Falle einer gemeinsamen Verantwortlichkeit sollten die einzelnen Aufgaben im Hinblick auf die Bearbeitung der Anfrage auf Datenportabilität klar zugeteilt sein (S. 6/neu).
Außerdem wurde betont, dass diejenigen, die Daten gemäß einer Datenportabilitätsanfrage eines Betroffenen erhalten sollen, nicht verpflichtet seien, dies zu akzeptieren. Somit bestehe keine Verpflichtung, Daten zu verarbeiten (S. 7/neu).

In Bezug auf die Geltung der Grundsätze der Datenportabilität wurde in der überarbeiteten Fassung herausgestellt, dass diese nicht zur Anwendung gelangen, wenn klar ist, dass der Betroffene nicht dieses Recht, sondern ein anderes bereichsspezifisches Recht auf Datenübertragung ausüben möchte. Beispielhaft wird die EU-Richtlinie 2015/2366 des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt (PSD2) genannt (S. 7/8 neu).

Ergänzt wurden weiterhin Hinweise zum Umgang mit Mitarbeiterdaten. Die Artikel-29-Datenschutzgruppe weist darauf hin, dass in vielen Fällen eine Betrachtung des Einzelfalls notwendig sei. Als Beispiele für ein Recht auf Datenportabilität werden etwa der Zahlungsverkehr oder die betriebsinterne Personalbeschaffung („internal recruitment“) genannt (S. 8/9 neu).

Die Empfehlungen der Artikel-29-Datenschutzgruppe stellen außerdem klar, dass die Datenportabilität im B2B-Bereich keine Anwendung findet (S. 8/neu).

Weiterhin wurden die Pflichten des Datenempfängers und damit neuen Datenverantwortlichen gem. Art. 5 DSGVO durch deren explizite Aufzählung betont (S. 10/neu: „faire und transparente Datenverarbeitung, Zweckbindung, Datenminimierung, Richtigkeit, Integrität und Vertraulichkeit, Speicherbegrenzung und Rechenschaftsverpflichtung“).

27 “Therefore, the ”new” receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14.”to another, thus enhancing competition between services (by making it easier for individuals to switch between different providers). It also enables the creation of new services in the context of the digital single market strategy” oder “This right aims to foster innovation in data uses and to promote new business models linked to more data sharing under the data subject’s control.”

Zudem hat die Artikel-29-Datenschutzgruppe konkretisiert, welche Daten von der Datenportabilität erfasst sein sollen. Explizit werden nun Protokolle von Nutzeraktivitäten, Chroniken der Webseitennutzung oder Suchanfragen genannt (S. 10/neu). Erläuternd wurde hinzugefügt, dass der Betroffene durch eine solche Abfragemöglichkeit seiner Nutzungsaktivitäten Kenntnis über die Wahrung seiner Privatsphäre erhalte und demzufolge wählen könne, welche Daten er für einen ähnlichen Dienst bereitstellen möchte.

In den Portierungsvorgang involvierte dritte Personen dürften keine Nachteile erleiden. Beispielhaft weist die Artikel-29-Datenschutzgruppe in diesem Zusammenhang darauf hin, dass weder Nutzerprofile von Dritten ohne deren Wissen und Einwilligung angereichert noch Informationen zu ihnen abgefragt und spezifische Profile erstellt werden dürften. Vorsichtig drückt die Artikel-29-Datenschutzgruppe aus, dass eine solche Datenverarbeitung unrechtmäßig und unfair sein dürfte („is likely to be…"). Dies bedeutet, dass hier noch Auslegungsbedarf besteht (S. 12/neu).

Hinsichtlich der bereitzustellenden Information über das Recht auf Datenübertragbarkeit wird in der überarbeiteten Version der Artikel-29-Datenschutzgruppe nunmehr zwischen den Vorgaben von Art. 13 Abs. 2b DSGVO (wenn Daten bei der betroffenen Person erhoben wurden) und Art. 14 Abs. 2c DSGVO (wenn Daten nicht bei der betroffenen Person erhoben wurden) deutlicher unterschieden. Bei Letzteren wird klarstellend ergänzt, dass die Information nicht später als einen Monat nach Erhalt der Daten zur Verfügung zu stellen sei. Im Gegensatz zur ursprünglichen Fassung vom Dezember 2016 empfiehlt die Artikel-29-Datenschutzgruppe nun als „leading practice" (statt zuvor „best practice"), dass den Betroffenen Informationen zur Verfügung gestellt werden und nicht mehr, dass die Empfänger der Daten als neue Datenverantwortliche die Informationen bereitstellen.[28] Insgesamt wird betont, dass die Bereitstellung von Informationen den Prozess einer fairen Datenverarbeitung untermauere (S. 13/neu).

In der überarbeiteten Fassung wird durch Einfügung eines neuen Absatzes zur Authentifizierung der Nutzer nochmals betont, dass die entsprechenden Prozesse oftmals schon bereitstünden und etwa entsprechende Log-in-Daten und das Passwort zur Identifizierung des Betroffenen ausreichen könnten. Gleichzeitig wird darauf verwiesen, dass die für den Datenverantwortlichen bestehende Möglichkeit, zusätzliche Informationen zur Feststellung der Identität des Betroffenen zu verlangen, nicht zu einer Sammlung von persönlichen Daten führen dürfe.

Das Gremium empfiehlt in der neuen Fassung zwei Möglichkeiten der Datenportabilität. Wurde in der ursprünglichen Fassung unter dem Punkt „Data Portability Tools" noch auf unterschiedliche Umsetzungsmöglichkeiten und beispielhaft auf den direkten Download sowie auf die Programmierschnittstelle API (Application Programming Interface) verwiesen, so werden in der überarbeiteten Version nun ausdrücklich zwei unterschiedliche und kostenlose Wege der Datenübertragung genannt: die direkte Übertragung des gesamten Datensatzes oder ein automatisiertes Tool, welches das Herausziehen der relevanten Daten ermöglicht. Die Entscheidung solle vom Einzelfall abhängig sein. So führt die Artikel-29-Datenschutzgruppe aus, dass der zweite Weg bei großen und komplexen Datensätzen bevorzugt werden könnte (S. 16/neu).

28 So wurden Aussagen gestrichen wie „Indeed, the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services (by making it easier for individuals to switch between different providers). It also enables the creation of new services in the context of the digital single market strategy" oder "This right aims to foster innovation in data uses and to promote new business models linked to more data sharing under the data subject's control."

Die Vorgabe in der ursprünglichen Fassung, dass möglichst viele Metadaten in höchster Granularität bereitzustellen seien, wurde in der korrigierten Fassung insoweit präzisiert, als gängige und offene Formate zu verwenden seien, sofern nicht in einer bestimmten Industrie oder einem Kontext ein anderes Format gebräuchlich wäre. Beispielhaft werden die Formate XML, JSON, CSV genannt (S. 18/neu).

Im Hinblick auf die Sicherheit bei der Datenübertragung wurde ergänzt, dass eine Risikominimierung dadurch erreicht werden solle, dass zusätzliche Authentifizierungsinformationen eingesetzt werden, wie etwa eine geheime Antwort auf eine bestimmte Frage oder ein einmaliges Passwort (S. 19/neu).

3. Auswirkung der Änderungen

Die Änderungen in der überarbeiteten Fassung vom Frühjahr 2017 haben häufig lediglich klarstellenden und präzisierenden Charakter, ohne jedoch den Inhalt der ursprünglichen Aussage wesentlich zu verändern. So wurden Begründungen hinzugefügt, die die anfänglichen Aussagen untermauern oder konkretisieren. Dies betrifft etwa Feststellungen zur Verantwortlichkeit, Ergänzungen zu Art. 5 DSGVO durch Aufzählen der dort enthaltenen einzelnen Pflichten, Hinzufügungen bei den Authentifizierungsmaßnahmen oder im Hinblick auf Informationspflichten.

Im Einzelnen ist Folgendes herauszustellen:

Die Artikel-29-Datenschutzgruppe hat die Wahrung des informationellen Selbstbestimmungsrechts der Datensubjekte als Zweck des Rechts auf Datenportabilität deutlicher in den Vordergrund gerückt; Aussagen zur Förderung des Wettbewerbs entfielen.

In der überarbeiteten Fassung wurde zudem eine Empfehlung für zwei durchführbare Wege der Datenportabilität abgegeben.

Eine Präzisierung betrifft die Abgrenzung des Rechts auf Datenportabilität zu anderen gesetzlichen Regelungen in den einzelnen Mitgliedsstaaten. Hier sollten zukünftig klare Kriterien entwickelt werden, inwieweit die Voraussetzungen des Rechts auf Datenportabilität erfüllt sein müssen oder nicht zur Anwendung gelangen, etwa wie im Rahmen der PSD2-Richtlinie, auf die die Artikel-29-Datenschutzgruppe beispielhaft verweist.

Dies gilt gleichermaßen für Mitarbeiterdaten, die in der überarbeiteten Fassung erstmalig erwähnt werden. Auch hier fehlen noch eindeutige Kriterien, in welchen Konstellationen das Recht auf Datenübertragbarkeit ausgeübt werden kann.

Deutlich gemacht wurde in der neuen Fassung auch die Verpflichtung eines Auftragsverarbeiters, den Datenverantwortlichen bei der Durchführung der Datenportabilität durch geeignete technische und organisatorische Maßnahmen zu unterstützen und diese Pflicht vertraglich zu fixieren.

Im Hinblick auf die Informationspflichten des Datenempfängers als neuen Datenverantwortlichen ist fraglich, ob mit der Änderung der Formulierung von „best practice“ zu „leading practice“ eine qualitative Änderung verbunden ist.

Dies gilt gleichermaßen in Bezug auf die grammatikalische Umformung einer aktiven Verpflichtung in einen unpersönlichen Passivsatz.[29] Letzteres hat rein vom Wortlaut her insoweit Relevanz, als dass nun nicht mehr vom Empfänger der Daten als neuem Verantwortlichen unmittelbar die Bereitstellung der Informationen verlangt wird. Allerdings ist in diesem Zusammenhang ebenso zu berücksichtigen, dass vom Datenempfänger an anderer Stelle verlangt wird, dass er klar und unmittelbar den Zweck der neuen Datenverarbeitung angeben muss (S. 7/neu).[30]

4. Stellungnahmen zu den Empfehlungen[31]

Die meisten Reaktionen folgten auf das Erscheinen der ersten Fassung der Guidelines der Artikel-29-Datenschutzgruppe vom 13. Dezember 2016, nicht zuletzt, weil im Rahmen der öffentlichen Konsultation die Stakeholder aufgefordert waren, ihre Sicht auf die Auslegung und Umsetzung der neuen Regelung darzulegen. Daraufhin gingen mehr als 90 (nur teilweise öffentlich zugängliche) Stellungnahmen ein.

Viele Stakeholder zeigten sich wegen der zahlreichen strikten Anforderungen an Datenverarbeiter beunruhigt, da es zugleich an klaren Anleitungen zum Umgang mit diesen Anforderungen fehlen würde. Einer der wesentlichen Kritikpunkte der Stellungnahmen betraf die Auslegung des Begriffs des „Bereitstellens“, da dieser in der DSGVO nicht legal definiert ist. So sei es unklar, ob nur Daten umfasst seien, die für die Funktionalität des Dienstes (und damit für die mögliche Übertragung) relevant sind, oder auch Verkehrsdaten wie die Suchhistorie, Lokationsdaten etc.[32] Es wurde von mehreren Akteuren nähere Klarstellung gefordert, was im Kontext der Regelung unter von der Person „bereitgestellten“ („provided“) personenbezogenen Daten in Abgrenzung zu „abgeleiteten“ („inferred“/ „derived“) zu verstehen sei.

Außerdem wurde gefordert klarzustellen, dass das Recht auf Datenübertragbarkeit nicht sensible Unternehmensdaten umfasse, wenn diese Geschäftsgeheimnisse des Unternehmens offenbaren und ggf. der Konkurrenz zugänglich gemacht werden würden. Unklarheit besteht außerdem bezüglich derjenigen Daten, welche im Rahmen der Geschäftsbeziehung gesammelt wurden – wie z.B. das Surf-Verhalten des Arbeitnehmers am Arbeitsplatz, geschäftlicher Mailverkehr, Videoüberwachungsmaterial etc.[33] Als wünschenswert wurde außerdem eine Klarstellung erachtet, dass nur diejenigen Daten von der Regelung erfasst wären, welche einen tatsächlichen Mehrwert für die informationelle Selbstbestimmung des Nutzers darstellen würden.[34]

29 Siehe oben: 13.12.2016: “...as a best practice for “receiving” data controllers, the WP29 recommends that they provide data subjects with complete information about the nature of personal data which are relevant for the performance of their services.” 05.04.2017: “...as leading practice for “receiving” data controllers, the WP29 recommends that data subjects are provided with complete information about the nature of personal data which are relevant for the performance of their services“ (S. 13 der Empfehlungen).

30 Siehe oben: “Therefore, the ”new” receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14.” (S. 7 der Empfehlungen).

31 Auf einzelne Stellungnahmen wird ausführlicher im Abschnitt B. eingegangen.

32 Vgl., BITKOM. Position Paper. Bitkom views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242), 31.01.2017, S. 2; https://www.nautadutilh.com/en/information-centre/news/2017/1/gdpr-series-part-4-the-right-to-data-portability-including-article-29-working-party-guidelines/; Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s “Guidelines on the right to data portability”, S. 7.

33 Vgl., Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s “Guidelines on the right to data portability”, S. 7.

34 Vgl., Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s “Guidelines on the right to data portability”, S. 1-2.

Auf der Seite der technischen Umsetzung betraf der größte Diskussionsbedarf die Frage nach Standardisierung und Kompatibilität von Formaten sowie die Sicherstellung der Interoperabilität von Datensätzen.[35] Eine klare Unterscheidung zwischen Kompatibilität und Interoperabilität würde begrüßt werden.[36] Hier wurde ebenfalls eine nähere Klärung des Begriffs „strukturiertes, gängiges und maschinenlesbares Format" gefordert.

Zusammenfassend lässt sich feststellen, dass die Regelung des Art. 20 DSGVO viele Fragen, vor allem zu ihrem Anwendungsbereich, aufgeworfen hat. Es erscheint eine vertiefte Abstimmung zwischen unterschiedlichen Stakeholdern aus Wirtschaft, Datenschutzaufsicht und der EU-Kommission erforderlich. Besonders gefragt sind Problemlösungsansätze aus der Wirtschaft und ein sektorübergreifender Diskurs zwischen Vertretern unterschiedlicher Branchen.

III. Klärungsbedürftige Fragen

Mit dem datenschutzrechtlichen Instrument der Portabilität sollen die Nutzer bessere Kontrolle über ihre Daten erhalten. Wie dieser theoretisch plausible Mechanismus in der Praxis funktionieren kann, ist jedoch noch nicht konkretisiert. In Bezug auf die praktische Umsetzung bedürfen vor allem folgende Fragen einer Klärung:

a) Zielrichtung der Norm

- Ist die neue Norm auch praktisch dazu geeignet, für die Verbraucherschaft ein echtes Mehr an informationeller Selbstbestimmung zu schaffen?
- Können Netzwerk- und „Lock-in-Effekte" durch die Norm tatsächlich aufgebrochen werden?
- Ergibt sich ein Standortvorteil für den europäischen Datenschutz oder bleibt es schlimmstenfalls bei regulatorischem Wunschdenken?
- Welche Vor- und Nachteile bringt die neue Norm für Nutzer und datenverarbeitende Unternehmen?
- Was bedeutet die Norm für Branchen und Unternehmen, die von „Lock-in-Effekten" gar nicht betroffen sind?
- Bedarf es gesetzgeberischer Konkretisierungen oder anderer flankierender Maßnahmen, um die Wirksamkeit der Norm und ihren Mehrwert für die informationelle Selbstbestimmung der Verbraucher sicherzustellen?

35 Vgl., https://medium.com/mydata/comments-on-data-portability-guidelines-2102d447f73b; https://www.nautadutilh.com/en/information-centre/news/2017/1/gdpr-series-part-4-the-right-to-data-portability-including-article-29-working-party-guidelines/; BITKOM. Position Paper. Bitkom views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242), 31.01.2017, S. 3. https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwifko_95uLUAhUCmrQKHSsQAmcQFggrMAA&url=https%3A%2F%2Fetno.eu%2Fdatas%2Fpositions-papers%2F2017%2F170131%2520ETNO_Data%2520Portability_Memo%2F170131%2520ETNO_D ata%2520Portability_Memo.pdf&usg=AFQjCNHC5Cwe6fHkpMMclYJw5Duqoy7IXw&cad=rja. Vgl., Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", S. 12.

36 Vgl., Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", S. 12.

b) Bestimmung des Anwendungsbereichs

- Wie eng oder wie weit sollte das Merkmal des „Bereitstellens von Daten“ i.S.v. Art. 20 Abs. 1 DSGVO interpretiert werden? Kann und sollte man die von dem Recht auf Datenübertragbarkeit betroffenen Daten-Arten kategorisieren?
- In welchen Fällen ist eine Verweigerung der Datenübertragung gerechtfertigt (Geschäftsgeheimnisse)?
- Wie sollten angesichts der Vorgabe „soweit es technisch machbar ist“ Fälle faktischer Unmöglichkeit von Fällen ungerechtfertigter Behinderung einer Datenübertragung abgegrenzt werden?

- Sollte eine Pflicht zur Ermöglichung von Interoperabilität und Kompatibilität gefordert werden? Wo könnte diese verankert werden?

- Ist es hilfreich, das Merkmal des Bereitstellens auf den jeweiligen Dienst zu beschränken und damit auf Daten, die für die Inanspruchnahme eines vergleichbaren Dienstes notwendig sind?

- Soll das Merkmal des Bereitstellens weiter eingeschränkt werden und lediglich Daten erfassen, die für einen beabsichtigten Anbieterwechsel notwendig sind?

c) Umsetzungsstrategien

- Welche Strategien für die strukturelle Umsetzung des Rechts auf Datenübertragbarkeit bieten sich für Einzelunternehmen und Unternehmensgruppen an? Welche Kooperationsformen wären hilfreich (Verbände i.S.v. Art. 40 Abs. 2 DSGVO, Verbünde, Arbeitsgemeinschaften)?

- Inwiefern ist ein plattformunabhängiger/ branchenübergreifender Lösungsansatz denkbar? Sind sektorspezifische Ansätze zielführender?

- Welche besonderen Anforderungen an das Datenschutzmanagement des Unternehmens können entstehen (z.B. Einbindung des Datenschutzbeauftragten)?

d) Technische Gestaltung

- Was genau ist unter einem „gängigen Format“ zu verstehen? Welche konkreten Anforderungen sollen an ein kompatibles Format gestellt werden?

- Wie könnte eine sektorübergreifende Verschränkung bestimmter Dienste im Format abgebildet werden (z.B. Automobilwirtschaft/ Versicherungswirtschaft: Portierung von Fahr(zeug)daten und Versicherungsdaten)?

- Welche technischen Tools könnten für die Ermöglichung der Datenübertragbarkeit herangezogen werden?

- Wie sollte die Überprüfung der Identitäten des anfragenden Kunden sichergestellt werden?

B. Umsetzung der Regelung in Art. 20 DSGVO

I. Stellungnahmen

1. Wissenschaft

Als Antwort auf den Call for Papers der Stiftung Datenschutz setzten sich **Armin Gerl und Dirk Pohl von der Universität Passau** mit rechtlichen Anforderungen und technischen Umsetzungsmöglichkeiten des Rechts auf Datenübertragbarkeit auseinander:[37]

Rechtliche Erwägungen

Die Autoren unterscheiden zwischen dem Recht auf Kopie der Daten (Art. 20 Abs. 1) und dem Recht auf Datentransfer zu einem anderen Verantwortlichen (Art. 20 Abs. 2). Dabei wird das Recht auf Erhalt einer Kopie in die Nähe des Auskunftsrechts gemäß Art. 15 gerückt. Beide Rechtsansprüche werden als Verhandlungsprozesse beschrieben und Art. 20 Abs. 1 als „Data Subject Negotiation“ und Art. 20 Abs. 2 als „Controller Negotiation“ bezeichnet.

Hinsichtlich der rechtlichen Anforderungen betonen die Autoren, dass ein wirkliches Recht auf Datenübertragbarkeit nicht mit den anderen Rechten der Datenschutzgrundverordnung wie dem Auskunftsrecht aus Artikel 15 deckungsgleich sein dürfe. Daher plädieren die Autoren für einen weiten Anwendungsbereich der Regelung, da auch nicht-personenbezogene Daten einen wirtschaftlichen Wert haben könnten, sodass diese von dem Recht ebenso erfasst sein sollten. Beim Recht auf Datenportabilität müssten außerdem nicht nur das Wettbewerbsrecht und die Interoperabilität in die Betrachtung einbezogen werden. Es sei vielmehr ein konsistentes Recht in der Europäischen Union erforderlich, welches die rechtliche Eigenschaft von Daten definiere und das Eigentumsrecht an Daten kläre, vor allem, wenn mehrere Personen betroffen wären. Hier sei zu berücksichtigen, dass jeder Datenverantwortliche entscheiden müsse, welche Eigenschaften als persönliche Daten eingestuft und vom Betroffenen bereitgestellt werden würden und welche Daten außerdem Bezug zu Dritten hätten.

Im Zusammenhang mit den rechtlichen Anforderungen diskutieren die Autoren zudem, ob eine Verpflichtung zur Entgegennahme der Daten wünschenswert sei. Sie verweisen darauf, dass die betroffene Person die Datenübertragung initiiere, aber das Recht insgesamt dadurch erheblich beschränkt sei, dass es keine korrespondierende Pflicht des neuen Datenverantwortlichen gebe, die Daten entgegenzunehmen, und es zudem auf die Fälle der technischen Machbarkeit limitiert sei. Zum Interessenausgleich wird vorgeschlagen, die Verantwortlichen zu verpflichten zu veröffentlichen, welche Formate empfangende Stellen für den Datenimport verwenden können.

37 *Siehe Abschnitt D.*

Technische Erwägungen

Im Hinblick auf die technische Machbarkeit der Datenportabilität sind die Autoren der Auffassung, dass es unwahrscheinlich sei, dass die Übertragung an sich signifikante technische Probleme bereite. Die Autoren definieren den Begriff der Interoperabilität als Fähigkeit, Informationen austauschen und gemeinsam die ausgetauschten Informationen nutzen zu können. Die Interoperabilität als Minimalforderung in der Datenschutzgrundverordnung würde allerdings weder Kompatibilität sicherstellen noch ein Ergebnis garantieren, welches interoperable Systeme ermögliche. Es müsse hier gleichermaßen die wettbewerbsrechtliche Sichtweise in die Betrachtung einbezogen werden.

Daher beschreiben die Autoren in ihrer Stellungnahme auch keine konkrete technische Lösung für ein mögliches Format, sondern entwickeln unterschiedliche Szenarien, die die rechtlichen Voraussetzungen in Einklang mit den technischen Anforderungen bringen sollen. Dabei legen sie die eingangs beschriebene Unterscheidung von Art. 20 Abs. 1 als „Data Subject Negotiation“ und Art. 20 Abs. 2 als „Controller Negotiation“ zugrunde. Hinsichtlich des Prozesses „Data Subject Negotiation“ wird eine Nutzer-Schnittstelle vorgeschlagen, sodass die betroffene Person bei der Datenübertragung unterstützend, prüfend und korrigierend eingreifen kann. Dazu müsste das Format aber weiterhin menschenlesbar sein.

Der zweite Fall „Controller Negotiation“ wird als Verhandlung zwischen den Verantwortlichen beschrieben, und auch hier soll nach Ansicht der Autoren eine zumindest „minimalistische“ Nutzer-Schnittstelle berücksichtigt werden. Insgesamt sollte unter der Annahme, dass es ein gängiges Format gibt, dieses bei der Verhandlung zwischen den Verantwortlichen verwendet werden. Allerdings wird im Hinblick auf ein „gängiges“ Format von den Autoren erklärt, dass dieses kein technisches Merkmal sei, sondern vielmehr von den Marktbedingungen abhänge. Es könne sich aufgrund der rasanten technischen Entwicklung schnell ändern. Sofern es ein solches nicht gibt, müssten sich der bisherige Datenverantwortliche und der neue Datenverantwortliche daher auf ein Format einigen und die betroffene Person über das Ergebnis der Datenübertragung entsprechend informieren. Diese Information könnte auch von beiden erfolgen, wobei sich die Anforderungen für den bisherigen Datenverantwortlichen aus Art. 12 Abs. 3 DSGVO und die des neuen Datenverantwortlichen aus Art. 13 DSGVO ergeben sollen.

Diese beiden Verhandlungsprozesse beschreiben die Autoren detailliert anhand von mehreren möglichen Szenarien, die beim Datenabgleich oder der Datenübertragung entstehen können. Zur besseren Veranschaulichung wird eine Datenbank skizziert, und die dort gespeicherten personenbezogenen Daten werden dabei als Einheit von Attributen mit einzelnen Kennungen (etwa: Vorname/ Nachname/ Geburtstag) und den entsprechenden konkreten Werten (dementsprechend etwa: Erika/ Mustermann/ 12.08.1964) dargestellt. Eine weitere Untergliederung der Attribute könne hinsichtlich des Formats erfolgen (z.B. als „Text” oder „Zahl”).

Die Autoren weisen darauf hin, dass es am einfachsten sei, wenn bei den Attributen die Kennung („Nachname“) und das Format („Text“) bei Quelle und Ziel jeweils übereinstimmten, da in diesem Fall der Wert der Ausgangsquelle ohne Änderung migriert werden könne. Bei Abweichungen der Kennungen von Quelle und Ziel müsse aber ein Format einer Datenübertragung verschiedene Bezeichnungen bieten, die vom Verantwortlichen jederzeit erweitert werden können, wenn eine Kennung unbekannt ist. Es trete dann zusätzlich die Frage auf, wer für die Erhaltung und Administration einer solchen zentralen Datenablage verantwortlich sei.

Zudem sei entscheidend, dass ein Format zur Datenübertragung in der Lage ist, die unterschiedlichen konkreten Werte bei den personenbezogenen Daten zu trennen (z.B. Unterteilung der Adresse in „Straße“ und „Hausnummer“) und/oder zu verbinden (z.B. Zusammenführung von „Straße und Hausnummer“ in eine Adresse), semantische Beziehungen zwischen den Kennungen zu berücksichtigen (z.B. Berechnung des Alters anhand des Geburtstags) sowie eine Änderung des Formats zuzulassen (z.B. Umwandlung eines Textes in eine Zahl). Dazu sei unter anderem eine granulare Beschreibungsmöglichkeit des Attributs einschließlich unterschiedlicher „Sub-Kennungen“ und „Sub-Formate“ erforderlich. Es wird außerdem die Möglichkeit erwähnt, dass die jeweiligen Quellen und Ziele nicht zwangsläufig die gleichen Attribute enthalten müssten, sodass auch für diesen Fall ein angemessenes Handling gefunden werden müsse.

Konsequenz der rechtlichen und technischen Erwägungen

Die Autoren sind insgesamt der Auffassung, dass die Zukunft der Datenportabilität hauptsächlich durch die technische Entwicklung angetrieben werde. Für die technische Realisierung sei es notwendig, ein gängiges und ausdrücklich beschriebenes Portabilitätsformat mit Eigenschaften zu finden, die den Verhandlungsprozess für die beschriebenen Szenarien ermöglichen und unterstützen. Codes of Conduct (gemäß Art. 40 DSGVO) sind nach Meinung der Autoren ein hilfreiches Instrument, um das Recht auf Datenportabilität zu erleichtern. Insgesamt müssten die Schnittstellen für die Verantwortlichen definiert werden, um proprietäre Lösungen zu vermeiden. Außerdem sei für die Umsetzung des Verhandlungsprozesses erforderlich, dass ausreichende Metadaten enthalten sind. Hinsichtlich der informationellen Selbstbestimmung sei es im Übrigen wünschenswert, die Lesbarkeit für den Menschen als Anforderung für das Portabilitätsformat einzuführen, um die betroffene Person zu informieren und den Verhandlungsprozess durch manuelle Intervention zu unterstützen.

Dennoch bewerten die Autoren die Frage kritisch, ob die wirtschaftlichen Vorteile stark genug sind, um ein entsprechendes Marktverhalten zu gewährleisten. Kritisch wird ebenso hinterfragt, ob es (sogar) innerhalb derselben Branche aus technischer Sicht immer möglich sei, wechselseitig die Datenportabilität anzubieten. Beispielhaft werden die beiden Dienste Twitter und Facebook genannt. So begrenze Twitter die Textlänge auf 140 Zeichen, während Facebook deutlich längere Nachrichten erlaube.

In einer auf den Call for Papers der Stiftung Datenschutz eingereichten Analyse befasst sich der Verein **Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF)** mit der Datenportabilität im Bereich der medizinischen Forschung. Unter anderem wird erörtert, inwiefern durch die Regelung ein „Empowerment“ von Patienten erreicht werden kann und welche Probleme und offenen Fragen damit verbunden sind.[38] Es wird dargestellt, dass die Datensammlung in der Medizinforschung sehr umfangreich und sehr detailliert sei und über eine reine Erfassung und Beschreibung von Krankheiten weit hinausgehe. In Bezug auf den „Mehrwert“ für die Datensouveränität wird unterstrichen, dass die Bereitstellung eigener Daten für die Forschung bzw. der Transfer der Daten von einer Stelle zu einer anderen grundsätzlich im Interesse des Betroffenen sein kann. Insbesondere bei Erkrankungen, für die noch keine ausreichende und standardisierte Therapie existiere – wie beispielsweise im Bereich der Onkologie – könnten Forschungsergebnisse dem Patienten unmittelbar nutzen. Jedoch nicht alle Anwendungsfälle in der Forschung würden von einer besser unterstützten Datenportabilität gleichermaßen profitieren, und auch der Nutzen für die Betroffenen könne sehr unterschiedlich sein. Oft werde bereits die Komplexität der Gesundheitsdatensätze deren Nutzen für Datensubjekte stark einschränken.

38 Siehe Abschnitt D.

Des Weiteren gehen die Autoren auf die Datenarten in der Medizinforschung ein und fragen nach der Unterscheidung zwischen von Patienten „bereitgestellten“ und „interpretierten“ Daten. Es wird ausgeführt, dass Unsicherheit bestehe, ab wann Daten nicht mehr als vom Betroffenen selbst bereitgestellt angesehen werden können. Denn auch den Beobachtungsdaten, die von der Regelung des Art. 20 DS-GVO umfasst seien, liege häufig bereits eine mehr oder weniger umfassende Analyse zugrunde. Am Beispiel der genetischen Diagnostik, welche Rückschlüsse auch auf die Gesundheit der Verwandten erlaube, wird die Problematik der Berührung von Rechten Dritter aufgezeigt.

Im Hinblick auf die Kompatibilität wird ausgeführt, dass es im Gesundheitswesen zwar eine Reihe branchen- und sektorspezifischer Formate gebe. Ein Datenaustausch über diese Grenzen hinweg sei damit jedoch nicht gelöst, was die Frage nach der Anforderung des Kriteriums der Interoperabilität aufwerfe. Interoperabilität erfordere ihrerseits die Verwendung abgestimmter Standards – gerade dieser Abstimmungsprozess sei aber komplex, da viele Interessensvertreter eingebunden werden müssten und die Heterogenität der Daten berücksichtigt werden müsse. Es müssten außerdem verschiedene Ebenen einbezogen werden: die strukturelle Interoperabilität (ein gemeinsames Datenmodell), die syntaktische Interoperabilität (eine gemeinsame Syntax) und die semantische Interoperabilität (ein gemeinsames Verständnis der Dateninhalte). Eine Interoperabilität bei unterschiedlichen Formaten lasse sich nur erreichen, wenn diese sinnvoll ineinander übersetzt werden könnten. Hierzu müssten die beteiligten Formate ausreichend detailliert beschrieben und dokumentiert sein. Eine besondere technische Herausforderung bei der Umsetzung bestehe außerdem in der Auftrennung von „bereitgestellten“, „beobachteten“ und sonstigen Daten.

Es wird schließlich herausgestellt, dass elektronische Gesundheitsakten eine geeignete technische Basis für die Umsetzung der Anforderungen der Datenübertragbarkeit sein könnten. Elektronische Gesundheitsakten sammeln alle medizinischen Informationen der Betroffenen in strukturierter Form und können vom Betroffenen hinsichtlich der Inhalte und Zugriffe gesteuert werden. Bisher sei allerdings weitgehend unklar, wer auf Basis eines nachhaltigen Geschäftsmodells als dauerhafter Betreiber solcher Gesundheitsakten in Frage komme und nach welchem Strukturierungsschema und auf Basis welcher Standards die Daten zwischen behandelnden Einrichtungen und solchen elektronischen Gesundheitsakten ausgetauscht werden könnten. Außerdem müsse berücksichtigt werden, dass klinische und Forschungseinrichtungen in der Medizin besonders sensible Gesundheitsdaten verarbeiten und daher besondere Maßnahmen für die Gewährleistung von Datenschutz- und Datensicherheitsanforderungen – wie z.B. der Aufbau eines sicheren Webportals zum verschlüsselten Download der Daten nach sicherer Authentifizierung – getroffen werden müssen.

Das Problem der sogenannten „Lock-in-Effekte“ in sozialen Netzwerken wird in dem an die Stiftung Datenschutz eingereichten Artikel „The Importance of Data Portability and Interoperability in the Social Web“ von **Sebastian Göndör von der TU Berlin Service-centric Networking** behandelt.[39] Es wird dargestellt, dass soziale Netzwerke heute ein Kommunikationsmedium von enormer Bedeutung und Reichweite seien. Soziale Netzwerke sind allerdings meist als abgeschottete Insellösungen konzipiert und profitieren von Netzwerkeffekten, durch welche sie kontinuierlich neue Benutzer anziehen. Kleinere Wettbewerber werden dadurch aus dem Markt oder in Nischenlösungen gedrängt, wodurch Wettbewerb und Innovation im sozialen Netz massiv behindert werden. Betreiber sozialer Netzwerke und Kommunikationsplattformen binden Nutzer an ihre Dienste. Eine freie Kommunikation mit anderen Diensten ist nicht möglich.

39 *Siehe Abschnitt D.*

Der Benutzer verliert hierdurch die Kontrolle über seine Daten und deren Verwendung. Datenportabilität und Interoperabilität seien dabei geeignete Maßnahmen, um ein offenes und freies soziales Netz zu ermöglichen, in dem Nutzer die Kontrolle über ihre Daten behalten und frei kommunizieren können. Um dieses Ziel zu erreichen, müssten geeignete Protokolle und Datenformate geschaffen werden.

Der Rechtsanwalt **Michael Strubel** setzt sich in einem Aufsatz mit dem Anwendungsbereich des Rechts auf Datenübertragbarkeit auseinander.[40] Im Zuge der Auseinandersetzung mit den Guidelines der Artikel-29-Datenschutzgruppe, mit der Entstehungsgeschichte, mit dem Wesensgehalt der Vorschrift sowie der Analyse ihres Wortlauts beschäftigt er sich insbesondere mit dem Begriff des „Bereitstellens von Daten". Er stellt dabei fest, dass bei der Interpretation des Begriffs eine Diskrepanz zwischen der weiten Auslegung der Artikel-29-Datenschutzgruppe und der Notwendigkeit zur Begrenzung des Anwendungsbereichs des Rechts bestehe. Er betont, dass eine zu weite Auslegung dessen, was als „observed data" als „zur Verfügung gestellt" betrachtet werde, das Tatbestandsmerkmal des Bereitstellens ausufernd und damit schließlich inhaltsleer werden lassen könnte. Als Lösungsansatz bietet er einen Mittelweg an, bei dem Art. 20 DSGVO nicht per se auf alle „observed data" angewendet wird, sondern das Merkmal des Bereitstellens „service-spezifisch" ausgelegt und auf diejenigen abgeleiteten personenbezogenen Daten angewendet wird, welche für die Erbringung des konkreten Dienstes nötig sind.

Die Leiterin des Telemedien-Referats des Bayerischen Landesamtes für Datenschutzaufsicht, **Kristin Benedikt**, betont bezüglich der praktischen Ausgestaltung der Datenübertragung vor allem Aufgaben im Bereich der Authentifizierung.[41] Da die datenherausgebenden Stellen die Identität der die Datenübertragung beantragenden Person im Zweifelsfalle ohnehin nach Art. 12 Abs. 6 DSGVO zu überprüfen hätten, sei jenen zu empfehlen, standardmäßig in jedem Fall eine Identitätsprüfung vorzunehmen, z.B. durch eine Bereitstellung/ Portierung erst nach erfolgreicher Eingabe von Log-in und persönlichem Passwort. Zudem müsse sichergestellt werden, dass die zu portierenden Daten nicht nur an den richtigen Empfänger übermittelt werden würden, sondern dass dies auch in sicherer Weise erfolge. Daher sei mindestens eine Transportwegverschlüsselung zu verlangen.

Von **Barbara Engels vom Institut der deutschen Wirtschaft Köln** wird in einer Analyse[42] dargelegt, dass die Datenportabilität zwar förderlich für die Datensouveränität des Einzelnen sei, sich aber in einigen Fällen schädlich auf den Wettbewerb auswirken könne. Viele der Forderungen des Normgebers lassen aus ihrer Sicht die speziellen Charakteristika von Plattformmärkten außer Acht. Einerseits bringe die Datenportabilität den Nutzern mehr Kontrolle über ihre Daten und lasse Markteintrittsbarrieren sinken und die Etablierungschancen neuer innovativer Unternehmen steigen. Andererseits könnten sich die Umsetzungskosten für die Datenübertragbarkeit zum Nachteil von Start-ups und kleineren Unternehmen auswirken, da die etablierten Unternehmen mit ihren Ressourcen die Marktmacht viel eher ausweiten könnten – zum Nachteil der User. Aus diesem Grund muss aus der Sicht von Barbara Engels das Recht auf Datenportabilität nuanciert interpretiert werden, um dem Wettbewerb und der Innovationsaktivität der Unternehmen nicht zu schaden. Datenportabilität solle in Märkten mit sich ergänzenden Produkten durchgesetzt werden. In anderen Märkten sei sie aus wettbewerbspolitischer Sicht nur da nötig, wo das Risiko des Marktmachtmissbrauchs hoch sei, wie es besonders auf dem Suchmaschinenmarkt der Fall sei.

40 Strubel, Michael, Anwendungsbereich des Rechts auf Datenübertragbarkeit, in: ZD 8/2017, S. 355-361.

41 Benedikt, Kristin, Datenportabilität – das neue Recht des Betroffenen; RDV 2017,189 [190].

42 https://policyreview.info/articles/analysis/data-portability-among-online-platforms; https://www.iwkoeln.de/studien/iw-kurzberichte/beitrag/barbara-engels-nicht-immer-gut-datenportabilitaet-zwischen-online-plattformen-300089.

Aysem Diker Vanberg und Mehmet Bilal Ünver setzen sich im „European Journal of Law and Technology“ kritisch mit der Umsetzbarkeit des Rechts auf Datenübertragbarkeit unter der EU-Datenschutzgrundverordnung auseinander.[43] Es wird ausgeführt, dass der wesentliche Unterschied zwischen der Grundverordnung und europäischen Wettbewerbsregeln darin bestehe, dass die Grundverordnung nur für natürliche Personen gelte, sodass die Regelung des Wettbewerbs zusätzlich durch EU-Wettbewerbsregeln, insbesondere durch Art. 102 TFEU, ergänzt werden könne. Dies erfordere, dass dieses Recht im Rahmen wettbewerbsrechtlicher Regeln und Präzedenzfälle genauer analysiert werde. Es wird außerdem darauf verwiesen, dass das Recht auf Datenportabilität eine Entwicklung von neuen Services verlange, welche Daten in einem bestimmten Format aus einem Dienst exportieren und in einen anderen Dienst importieren würden. Insbesondere viele kleine und mittelständische Unternehmen hätten jedoch oft nicht die notwendigen Ressourcen, um diese Anforderungen der Grundverordnung umzusetzen, während die Kosten für große Unternehmen nicht signifikant hoch seien. Außerdem wird darauf hingewiesen, dass es noch keine Klarheit darüber gebe, ob die Nutzer das Recht auf Datenportabilität auch tatsächlich nutzen würden. Um sicherzustellen, dass das Recht von den Betroffenen effektiv geltend gemacht werden kann, müssten die Betroffenen genauer über die Bedeutung und Tragweite dieses Rechts informiert werden. Daher sollten insbesondere die nationalen Datenschutzbehörden über ihre Webseiten in einer einfachen und verständlichen Sprache die Möglichkeiten der Datenportabilität sowie mögliche Wege für die Einreichung einer Beschwerde erläutern.

2. Datenschutz- und Verbraucherschutzorganisationen

Im Gutachten „Digitale Souveränität“ des Sachverständigenrats für Verbraucherfragen (SVRV) wird der Datenportabilität eine hohe Relevanz für die Ausübung der digitalen Souveränität beigemessen.[44] Da von den sogenannten „Lock-in-Effekten“ die Gefahr eines Missbrauchs von Marktmacht ausgehe, wird vom SVRV die Entwicklung von handhabbaren, einfachen Standards in Bezug auf Interoperabilität empfohlen, welche Kompatibilität zwischen digitalen Diensten sicherstellen und damit eine Öffnung des Marktes für neue, innovative Anbieter ermöglichen. Gleichzeitig wird gefordert, dass das Recht auf Datenportabilität – analog zum digitalen Zahlungsverkehr – schuldrechtlich „als Kündigung des zugrunde liegenden Verbrauchervertrages“ verstanden wird, damit die Verbraucher eine „kostenfreie Rückübertragung der Daten in einem gängigen maschinenlesbaren und interoperablen Format oder ihre Löschung verlangen“ können.[45]

In der Stellungnahme des Verbraucherzentrale Bundesverbands (VZBV) aus dem Herbst 2016 zum Grünbuch des Bundesministeriums für Wirtschaft und Energie wird die Einführung des Rechts auf Datenübertragung positiv beurteilt, da es für die Verbraucher die Wechselkosten bei Plattformwechsel reduziere, „Lock-in-Effekte“ verhindere und damit den Wettbewerb fördere.[46] Einen besonderen Akzent setzt der VZBV auf eine effektive Umsetzung des Rechts und auf die Einhaltung hoher Datenschutzstandards. Als offen betrachtet der Bundesverband die Frage, wie marktmächtige Unternehmen dazu bewegt werden könnten, Nutzern die Datenübertragbarkeit zu ermöglichen.

43 Vanberg, Aysem Diker/Ünver, Mehmet Bilal, The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?, in: European Journal of Law and Technology, Vol 8, No 1, 2017. URL: http://ejlt.org/article/view/546/726.

44 Sachverständigenrat für Verbraucherfragen, Digitale Souveränität, Juni 2017, S. 26.

45 Ebd., S. 27.

46 Grünbuch Digitale Plattformen, Stellungnahme des Verbraucherzentrale Bundesverbands v. 26. September 2016, S. 10, 18.

Es wird außerdem Zweifel daran geäußert, ob reine Ko-Regulierung zum Erfolg führen würde, da marktmächtige Plattformen kein Interesse daran hätten, ihren Nutzern den Wechsel zu Wettbewerbern zu erleichtern.[47]

In der Stellungnahme des Europäischen Datenschutzbeauftragten (EDPS) „Opinion on Personal Information Management Systems" vom September 2016 wird insbesondere die Bedeutung von „Personal Information Management Services" (PIMS) für die Umsetzung des Rechts auf Datenübertragbarkeit betont.[48] Die Idee hinter PIMS-Ansätzen ist, durch eine einheitliche zentralisierte Datenkontrolle an einer Stelle („One-Stop-Shop") dem Nutzer auf einfache und verständliche Art und Weise die Möglichkeit zu geben, seine Daten zu verwalten und bei mehreren Dienstanbietern die Weitergabepräferenzen gleichzeitig zu ändern.[49] So wären die PIMS dazu besonders geeignet, die personenbezogenen Daten zielgerichtet, vollständig und effizient zu übertragen und damit mehr Nutzerkontrolle zu ermöglichen.[50] Viele dieser Ansätze befinden sich allerdings noch in einer Entwicklungs-, Test- oder Implementierungsphase.

3. Weitere staatliche und nicht-staatliche Institutionen

Die **Wissenschaftlichen Dienste des Deutschen Bundestages** haben im Dezember 2016 ihre Arbeit zu der Frage abgeschlossen, inwieweit bei digitalen Plattformen eine Marktkonzentration oder Monopolstellung vorliegen kann.[51] Untersucht wurden die sogenannten OTT-Dienste[52], die dort als Dienste definiert werden, denen kein inhaltliches Angebot zugrunde liegt, sondern die Individual- oder Gruppenkommunikation unter Einsatz des IP-Protokolls (Internet-Protokolls) ermöglichen. Dabei wurde die Betrachtung nochmals auf Messengerdienste wie Skype, WhatsApp und E-Mail-Dienste beschränkt. Insgesamt steht die Frage im Raum, inwieweit diese Dienste reguliert werden müssen, um gleiche Wettbewerbsbedingungen zu schaffen. Ausführungen erfolgen zu § 6 und § 18 Telekommunikationsgesetz,[53] aber ebenso zum Recht auf Datenübertragbarkeit gemäß Art. 20 Datenschutzgrundverordnung. Hier wird auf den Standpunkt der Bundesnetzagentur verwiesen, wonach nach ganz überwiegender Meinung kein zusätzlicher nationaler Regelungsbedarf im Hinblick auf Art. 20 DSGVO bestehe. Ergänzend wird in diesem Zusammenhang die Äußerung des Verbraucherzentrale Bundesverbands zitiert, dass sich die Bundesregierung vielmehr für eine effektive Datenportabilität im Rahmen der Anwendung der Datenschutzgrundverordnung einsetzen sollte. Insgesamt wird zwar die Möglichkeit eines wettbewerbsrelevanten „Lock-in-Effekts" benannt, aber die Wissenschaftlichen Dienste weisen darauf hin, dass die Bundesnetzagentur eine entsprechende Regelung für überflüssig halte. Begründet werde dies mit der lokalen Speicherungsmöglichkeit von Inhalten des E-Mail-Verkehrs sowie von Adressbüchern durch die

47 Ebd., S. 10.

48 European Data Protection Supervisor, Opinion 9/2016 „EDPS Opinion on Personal Information Management Systems", S. 9.

49 Dazu: Stiftung Datenschutz, „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen", S. 7 ff. URL: https://stiftungdatenschutz.org/themen/pims-studie/

50 European Data Protection Supervisor, Opinion 9/2016 „EDPS Opinion on Personal Information Management Systems", S. 12-13.

51 Hintergrund sei der sogenannte „Netzwerkeffekt", der aufgrund der wachsenden Nutzerzahlen und der Zugriffsmöglichkeit auf große Datenmengen eintreten könne.

52 Da es bislang noch keine einheitliche Definition für die verschiedenen digitalen Plattformen (Over-the-Top-(OTT-)Dienste) gibt, legen die Wissenschaftlichen Dienste die durch den Zusammenschluss der europäischen Regulierungsbehörden (GEREK) vorgenommene Gruppeneinteilung zugrunde.

53 Im Hinblick auf die grundsätzliche Anwendbarkeit des Telekommunikationsgesetzes wird die Frage aufgeworfen, ob dies bei Messengerdiensten überhaupt sinnvoll sei, u.a. wegen der Unterschiede bei den datenschutzrechtlichen Regelungen. Die Wissenschaftlichen Dienste verweisen außerdem bei der umstrittenen Frage, ob ein solcher Dienst im rechtlichen Sinne als Telekommunikationsdienst qualifiziert werden kann, auf die ausstehende Entscheidung des Bundesverwaltungsgerichts oder des Europäischen Gerichtshofs.

Nutzer selbst. Dies solle jedoch auch dann gelten, wenn eine solche Möglichkeit wie bei WhatsApp nicht bestehe. So nutzten die meisten Nutzer OTT-Dienste parallel im sogenannten Multi-Homing und könnten von einem Dienst zum anderen flexibel und ohne Kosten wechseln. Dies entspreche nach den Ausführungen der Wissenschaftlichen Dienste zugleich der Auffassung des Bundesverbands Informationswirtschaft, Telekommunikation und Neue Medien e.V. (Bitkom), der ebenso eine nationale Regelung zur Datenportabilität im Vorgriff auf die Datenschutzgrundverordnung ablehne. Danach sollte nicht der Gesetzgeber Formate zur Datenportabilität vorgeben, sondern die Anforderungen sollten durch die Industrie und mittels internationaler Zusammenarbeit entwickelt werden.

Auch in den USA wird das Thema Datenübertragbarkeit intensiv verfolgt. Im Rahmen einer öffentlichen Konsultation des **White House Office of Science and Technology Policy (OSTP)** zur Datenportabilität wurden 22 Stellungnahmen eingereicht.[54] Von vielen Stakeholdern wurde dabei die Datenübertragbarkeit als ein wichtiges Instrument zur Steigerung des Wettbewerbs und zur Verbesserung der Datenkontrolle durch Nutzer benannt.[55] Insbesondere im Gesundheitsbereich sahen die meisten Kommentatoren die Vorteile der Datenübertragbarkeit. Zugleich betonten viele, dass der Ausbau der Datenübertragbarkeit und die Privatheit der Nutzer in keinem Gegensatz stehen dürften. Die meisten Sorgen wurden bezüglich der Umsetzungskosten und der Gewährleistung des Portabilitätsservice geäußert sowie bezüglich der Tatsache, dass bislang keine Format-Standards existierten. Zugleich wurde vor einer zu strikten Regulierung durch staatliche Stellen gewarnt. Als Empfehlungen wurden eine Entwicklung von Standards in Zusammenarbeit von Industrie, Verbänden und Verbraucherorganisationen vorgeschlagen, Unterstützung der Regierung bei der Implementierung von Pilotprojekten und Förderung von Best-Practice-Ansätzen sowie eine Sensibilisierung der Nutzer für das Thema „Datenübertragbarkeit".

In seinen Kommentaren zu WP29-Guidelines betonte der internationale Think-Tank **Center for Information Policy Leadership (CIPL)**, dass bedacht werden solle, dass es etwa im B2B-Kontext oder in Beschäftigtenverhältnissen Bereiche gebe, in denen die Möglichkeit der Datenportabilität keinen zusätzlichen Mehrwert für die informationelle Selbstbestimmung des Nutzers schaffe.[56] Es wird dabei besonders hervorgehoben, dass das Recht auf Datenübertragbarkeit sich nicht auf den Bereich des Beschäftigtenverhältnisses („human ressources data") erstrecken sollte. Außerdem müsste von den Datenverarbeitern eine Unterscheidung und Kategorisierung von unterschiedlichen Arten von personenbezogenen Daten vorgenommen werden, um eine effektive Datenübertragung zu gewährleisten. Es wird darauf hingewiesen, dass „observed data" nicht automatisch unter die Kategorie „bereitgestellte" („provided") Daten fallen würden, es sei denn, die Verbindung zu diesen Daten stelle einen eindeutigen Mehrwert für die informationelle Selbstbestimmung des Nutzers dar.[57] Darüber hinaus wurde eine Klarstellung gefordert, was unter einem „strukturierten, gängigen, maschinenlesbaren Format" zu verstehen sei und inwiefern die „Interoperabilität" der Daten die „Kompatibilität" unterschiedlicher gängiger Formate einschließen sollte. Schließlich wird von CIPL dafür plädiert, cloud-basierte Lösungsansätze – wie das „pull-modell" – zu unterstützen, da so eine bessere Nutzerkontrolle über die Datenweitergabe an unterschiedliche Service-Anbieter gewährleistet werden könne.[58]

54 White House Office of Science and Technology Policy. Request for Information Regarding Data Portability. 10.01.2017. URL: https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/OSTP-Data%20Portability-RFI-Responses_for_humans.pdf

55 Macgillivray, A., Summary of Comments Received Regarding Data Portability, 10.01.2017. URL: https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability.

56 Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", S. 1-2, 5.

57 Ebd., S. 8.

58 Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", S. 4.

Die **Internet Economy Foundation (IE.F)** setzt sich bei der Beantwortung des Fragenkatalogs für ein Fachgespräch des Ausschusses Digitale Agenda des Deutschen Bundestages mit den Fragen der Interoperabilität und Neutralität auseinander.[59] Es wird betont, dass die Interoperabilität von Plattformen eine wichtige Voraussetzung für das Wertschöpfungspotenzial und die Innovationskraft der Digitalökonomie darstelle, da sie einer „Marktverklumpung" aktiv entgegenwirke und Markteintrittsbarrieren senke. Geschlossene Systeme, die durch „Lock-in-Effekte" Kundenbindung und damit Ausbau und Festigung der Marktmacht erzeugen würden, würden sich durch Marktverschließung für die Internetwirtschaft insgesamt nachteilig auswirken. Definition, Ausbau und Verwendung von Format-Standards würden dagegen die Interoperabilität fördern und Monopolstellungen einzelner Dienstleister vermeiden. Auch die Verbraucher würden von offenen interoperablen Systemen eindeutig profitieren, da sie dadurch an Entscheidungsfreiheit, Autonomie und Komfort gewinnen würden. Um aber die Bereitschaft der Nutzer zu steigern, Portabilitätsangebote aktiv wahrzunehmen, muss aus Sicht der IE.F seitens des Verbraucherschutzes noch viel Aufklärungsarbeit geleistet werden, der den Nutzern vor allem den Wert ihrer Daten verständlich und greifbar macht.[60] Es wird zusätzlich darauf hingewiesen, dass sich die kommenden Regelungen ausschließlich auf personenbezogene Daten beschränken würden, obwohl fehlende Übertragungsfähigkeit auch anderer Datenarten in vielen Fällen ebenso wettbewerbshinderlich sei. Da sich aber ein Anbieterwechsel umso mehr lohne, je mehr Daten übertragen werden können, müssten im Rahmen der Initiative „Freier Datenfluss" der Europäischen Kommission mehr Anreize für den Ausbau der Interoperabilität – auch für nicht-personenbezogene Daten – geschaffen werden.[61]

Open Knowledge Finland (OKFI) ist eine gemeinnützige Nicht-Regierungsorganisation, die sich für einen freien Informationsfluss und eine offene, transparente digitale Gesellschaft engagiert. In ihrer Stellungnahme zum ersten Entwurf der WP29-Guidelines wird von OKFI in Bezug auf „personenbezogene Daten" kritisch gefragt, inwiefern das Verständnis dessen, welche Daten einen Personenbezug aufweisen, sich im Laufe der technischen Entwicklung ändern werde und welche Konsequenzen dies für das Recht auf Datenübertragbarkeit mit sich bringe. Zugleich wurde die Frage aufgeworfen, ob aus der Regelung des Art. 20 DSGVO ein Identifizierbarkeitserfordernis für diejenigen Personen folge, welche bestimmte Plattformen pseudonym nutzen und Datenübertragbarkeit einleiten möchten.[62] Mit dem Verweis auf „rainbow data approach"[63] wurde weiterhin betont, dass die Lösungsansätze für die Datenübertragbarkeit keiner bereichsspezifischen „Insellösungen" – wie z.B. „Blue Button"[64] – bedürften, sondern grundlegende Standards für Download und Übertragung von personenbezogenen Daten zeitigten. Schließlich wird hervorgehoben, dass die Diskussion über die Datenportabilität sich auf die Möglichkeiten einer verbesserten Datenkontrolle durch Nutzer konzentrieren müsse, und nicht etwa auf die Frage eines Dateneigentums.

59 Deutscher Bundestag, Ausschuss Digitale Agenda, Ausschussdrucksache 18(24)120, 13.12.2016.

60 Deutscher Bundestag, Ausschuss Digitale Agenda, Ausschussdrucksache 18(24)120, 13.12.2016., S. 11.

61 Ebd., S. 14, 17.

62 https://medium.com/mydata/comments-on-data-portability-guidelines-2102d447f73b.

63 Dazu, siehe unten, Kap. B. II.

64 Zu „Blue Button" siehe unten, Kap. B. II.

4. Branchenverbände und Unternehmen

In einer auf den Call for Papers der Stiftung Datenschutz eingereichten Stellungnahme vertritt die **Deutsche Telekom AG (DTAG)**[65] die Auffassung, dass die Leitlinie der Artikel-29-Datenschutzgruppe über den gesetzlichen Rahmen des Art. 20 DSGVO hinausgehe. Nach Ansicht der Deutschen Telekom sind von dem Recht auf Datenübertragbarkeit nur solche Daten umfasst, die für die betroffene Person nützlich sind.

Gemäß dieser Stellungnahme versucht die Artikel-29-Datenschutzgruppe den Rahmen und das Ziel der Regelung von Art. 20 DSGVO erheblich auszuweiten. Die Artikel-29-Datenschutzgruppe habe aber weder das Recht noch das Mandat, willkürlich den Anwendungsbereich der Datenschutzgrundverordnung zu erweitern. Die DTAG argumentiert mit der Historie des Gesetzgebungsverfahrens, wonach sich die EU-Gesetzgeber durch Änderung des Wortlautes bewusst dazu entschieden hätten, die durch Art. 20 DSGVO betroffenen personenbezogenen Daten einzuschränken. Es müsse sich um Daten handeln, die die betroffene Person einem Verantwortlichen „bereitgestellt hat“, und nicht generell um „verarbeitete personenbezogene Daten“.

Daher sollte jede Auslegung von Art. 20 DSGVO eng am Wortlaut haften, um nicht der Intention der EU-Gesetzgeber zu widersprechen. Die Formulierung meine daher nicht Nutzungsdaten und auch nicht die für den Vertragsabschluss erforderlichen Daten. Damit sei der Datenverantwortliche nicht verpflichtet, Daten bereitzustellen, die automatisch während der Nutzung des Dienstes generiert werden (z.B. Logfiles, Verkehrs- oder Standortdaten). Der DTAG zufolge kann die Formulierung „bereitgestellt“ damit nur Daten betreffen, die die betroffene Person während der Vertragsdurchführung kontrolliert und darauf Zugriff hat (z.B. Fotos, E-Mails).

Die von der Artikel-29-Datenschutzgruppe vorgenommene Erweiterung des Anwendungsbereichs von Art. 20 DSGVO führe zu unlösbaren Problemen für die Datenverantwortlichen. Besonders für die Daten der elektronischen Kommunikation mit Löschungspflichten rufe das Recht auf Datenübertragbarkeit unzählige rechtliche Unsicherheiten hervor. Im Falle von Verkehrs- und Standortdaten seien die Konsequenzen für die betroffene Person und den neuen Datenverantwortlichen vollkommen unklar, auch unter Berücksichtigung der ePrivacy-Richtlinie. Außerdem betreffe die Portierung von Verkehrsdaten die Rechte Dritter und stelle damit eine Verletzung von Art. 20 Abs. 4 DSGVO dar. Der Empfänger der portierten Daten wäre zudem mit rechtlichen Unsicherheiten konfrontiert, wenn er zur Prüfung verpflichtet wäre, ob die übermittelten Daten von einer Einwilligung oder einer vertraglichen Verpflichtung gedeckt sind und die Datenverarbeitung damit rechtmäßig ist. Telekommunikationsdaten seien besonders betroffen (etwa Verkehrs- oder Standortdaten), da hier eine Verarbeitung aufgrund eines be-rechtigten Interesses nicht erlaubt sei. Weiterhin sei die von der Artikel-29-Datenschutzgruppe beschriebene Praxis, vollständige Datensätze zu übermitteln, um zu prüfen, ob alle Daten tatsächlich benötigt werden, aus der Perspektive des Datenschutzes sehr besorgniserregend.

65 Siehe Abschnitt D.

Argumentiert wird jedoch auch aus technischer Sicht. So unterhielten die meisten Anbieter keine getrennten Datenbanken für die Rohdaten, die leicht von den Algorithmen zur Kundenanalyse getrennt werden könnten. Dies führe dazu, dass von einem Datentransfer zu einem anderen Anbieter detaillierte Hintergrundinformationen über den technischen Aufbau und die verwendeten Algorithmen umfasst sein könnten. Damit wären auch Grundlagen des Unternehmens enthüllt, sowie geistiges Eigentum und Geschäftsgeheimnisse betroffen. Die Artikel-29-Datenschutzgruppe habe zwar das Recht, die Entwicklung von allgemeinen Standards und interoperablen Systemen zu fördern, um einfache Wege für die Durchführung der Datenportabilität zu bereiten. Diese Entwicklung von technischen Standards benötige aber Zeit und Arbeitsaufwand einer Vielzahl involvierter Parteien, einschließlich der Datenschutzaufsichtsbehörden und der Institutionen des öffentlichen Sektors.

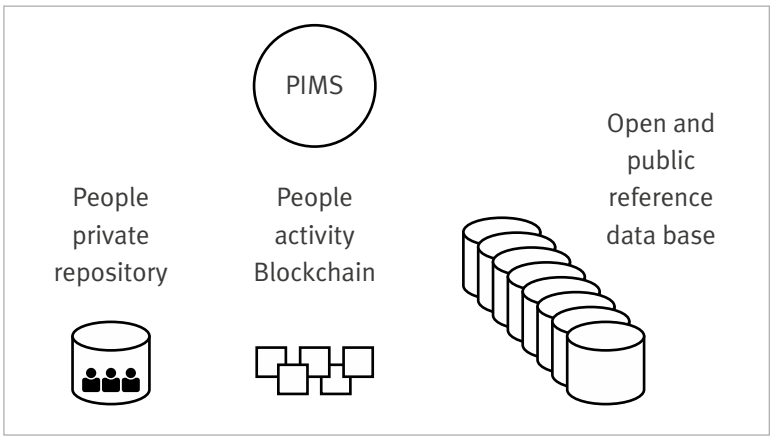
- In einer bei der Stiftung Datenschutz eingegangenen Stellungnahme von **Google**[66] betont das Unternehmen, dass die Datenportabilität bei richtiger Umsetzung sowohl mehr Nutzerkontrolle ermögliche, als auch sich als innovationsfördernd erweisen könne. Dabei sollte die Umsetzung folgenden vier Grundsätzen folgen: benutzerfreundliche Gestaltung, Datensicherheit, reziproke Nutzbarkeit sowie Beschränkung auf nutzer- und nicht auf unternehmensinterne Daten. Des Weiteren wird betont, dass sich die Investitionen in den Ausbau der Portabilitätsinfrastruktur langfristig auszahlen würden und dass Open Source-Lösungen dazu einen erheblichen Beitrag leisten könnten. Bei der praktischen Umsetzung solle jedoch nicht die Festlegung eines universellen Formats im Vordergrund stehen, sondern vielmehr die Suche nach zukunftsoffenen Möglichkeiten, bereits bestehende, bereichsspezifische sowie neue Formate miteinander zu verbinden. Dazu empfiehlt Google, keine starren Standards festzulegen, sondern die Entwicklung von offenen, interoperablen branchenüblichen Standards seitens der Unternehmen zu fördern. Außerdem sollten die Nutzer zur sicherheits- und datenschutzfreundlichen Datenpflege verstärkt ermutigt und über die Portabilitätsmöglichkeiten aufgeklärt werden. Schließlich wird in der Stellungnahme die gegenwärtige Entwicklung eines eigenen Prototyps erwähnt, mit dem der Import und Export von Daten zwischen zwei öffentlich zugänglichen Produktschnittstellen und damit eine direkte Übertragung zwischen unterschiedlichen Plattformen ermöglicht werde. Dazu wolle das Unternehmen 2018 detaillierte Informationen präsentieren.

- Das französische Start-up **ONECUB**, das sich 2011 auf Datenübertragbarkeit auf PIMS-Basis spezialisiert hat, geht in seiner der Stiftung Datenschutz eingereichten Stellungnahme[67] auf die besondere Bedeutung von Personal Information Management Systems (PIMS) für die Umsetzung des Rechts auf Datenübertragbarkeit ein. Es werden zunächst drei Wege für die Umsetzung der Datenportabilität identifiziert: direkte B2C-Übertragung, direkter B2B-Transfer und die Datenübertragung mit einem zwischengeschalteten Tool. Die ersten beiden Möglichkeiten hätten den Nachteil, dass sie entweder aufgrund der Komplexität für die Nutzer nicht handhabbar seien (bei B2C), oder auch (bei B2B) bei dem Transfer unterschiedlicher Datensätze zu einem Anbieter (z.B. Übermittlung von Ernährungsdaten aus mehreren Diensten an einen E-Health-Anbieter) dem Nutzer mehrfache Einwilligungen abverlangten und einen hohen Umsetzungsaufwand für die Anbieter bedeuteten. Eine Alternative dazu biete die Datenübertragung mittels Tool, mit dem die Weiterverwendung von Daten durch den Nutzer gemanagt wird. Die Nutzung eines solchen PIMS würde dabei dem User einen verbesserten Zugriff und die individualisierte Erfassung und Wiederverwertung eigener Daten ermöglichen. Außerdem würden Dienstanbietern Kosten für die Umsetzung der Datenübertragbarkeit erspart. Die Nutzung von PIMS bringe jedoch das Problem der Konzentration von vielen sensiblen Daten an einer zentralen Stelle und die damit verbundenen Sicherheitsgefahren mit sich.

66 Siehe Abschnitt D.

67 Siehe Abschnitt D.

Daher wird in dem Paper der Weg vorgeschlagen, die Daten dezentral beim Nutzer zu speichern und die einzelnen Nutzer-Depots mittels des Blockchain-Verfahrens miteinander zu verbinden. Bei diesem Lösungsansatz würden durch PIMS zwar alle technischen Aspekte verwaltet, jedoch keine personenbezogenen Daten gespeichert:



- In einer bei der Stiftung Datenschutz eingegangenen Stellungnahme des **Gesamtverbands der Deutschen Versicherungswirtschaft e.V. (GDV)** wird ausgeführt, dass als „bereitgestellte" Daten in erster Linie diejenigen Daten zu verstehen seien, die der verarbeitenden Stelle vom Kunden aktiv zur Verfügung gestellt werden, wie z.B. im Rahmen einer Antragsstellung oder der Abrechnung eines Leistungsfalles. Bei der Verletzung von Geschäftsgeheimnissen, Urheberrechten sowie Freiheiten anderer Personen komme eine Datenportierung dagegen nicht in Betracht. Die Erfüllung des Rechts auf Datenübertragbarkeit sollte des Weiteren möglichst in bestehende Datenschutzmanagementsysteme integriert werden. Da die Versicherungswirtschaft zum Teil hochsensible Daten verarbeite, wird hervorgehoben, dass Datenportabilität nicht seinerseits zum Risiko für den Datenschutz werden dürfe. Mit der eindeutigen Authentifizierung des Datenempfängers sowie der Gewährleistung eines gleichwertigen Datenschutz- und Datensicherheitsniveaus könne dem entgegengewirkt werden. Dabei könne es jedoch nicht in der Verantwortlichkeit des übertragenden Unternehmens liegen, zu prüfen, ob und welche Daten ein drittes Unternehmen benötigt. In Bezug auf technische Standardisierung wird in der Stellungnahme herausgestellt, dass die Entwicklung allgemeiner verbindlicher Standards angesichts der vielfältigen Datennutzung in unterschiedlichen Branchen und Sektoren nur schwer leistbar sei. Vielmehr wären allgemeine Eckdaten wünschenswert – wie Interoperabiliät, plattformübergreifende Nutzbarkeit, offene Standards und Schnittstellen.

- Die auf den Call for Papers der Stiftung Datenschutz eingereichte Stellungnahme des **Deutschen Dialogmarketing Verbands (DDV)** geht auf den Unterschied zwischen Auskunftsrecht und Datenübertragbarkeitsrecht ein und auf die praktische Umsetzung der Norm.[68] Es wird dargestellt, dass die Umsetzung des Anspruches auf Datenportabilität schon deshalb keinen erheblichen Aufwand im Bereich des Dialogmarketings (wo es vor allem um Daten zu Rechnungs- und Lieferanschriften, Bestellhistorie und Informationen zur Zahlungsabwicklung gehe) verursachen sollte, weil er dem Auskunftsanspruch weitgehend gleiche. Die Daten, die in elektronischer Form zu übermitteln sind, stellten nur eine Untergruppe der Daten dar, die eine betroffene Person im Rahmen eines Auskunftsanspruches erhalten kann. Das Besondere am Recht auf Datenübertragbarkeit sei, dass diese Untergruppe von Daten in einem strukturierten, gängigen und maschinenlesbaren Format übertragen werden muss.

68 *Siehe Abschnitt D.*

Um dem Anspruch auf Datenübertragbarkeit zu genügen, seien daher in der Praxis des Dialogmarketings nur wenige Anpassungen erforderlich – zum einen die Ermittlung der zu übertragenden Daten und zum anderen die Festlegung des technischen Verfahrens und des Formats (hier sind aus der Sicht des DDV sowohl einfache Formate (wie ASCII) als auch PDF-Formate denkbar).

- In der auf den Call for Papers der Stiftung Datenschutz eingereichten Stellungnahme des **Bundesverbands Deutscher Inkasso-Unternehmen e.V. (BDIU)**[69] wird dargestellt, dass für den Bereich der Inkassodienstleistungen das Recht auf Datenübertragbarkeit weder praxistauglich noch erforderlich sei. Die Inkassodienstleister kommunizierten im Auftrag eines anderen Unternehmens mit den Kunden und erhielten personenbezogene Daten grundsätzlich vom Auftraggeber. Da die Daten größtenteils vom Auftraggeber stammen würden, ergebe sich für die Inkassobranche eine Relevanz des neuen Rechts der Datenportabilität nur dann, wenn im weiteren Inkassoverfahren die Daten direkt von der betroffenen Person „bereitgestellt" werden würden. Dies könne beispielsweise bei telefonisch mitgeteilten Adressänderungen der Fall sein. Während ein Kunde den Überblick über die vorhandenen personenbezogenen Daten bereits aufgrund seines Auskunftsrechts nach Art. 15 DSGVO erhalten kann, würde die Übermittlung von Daten gemäß Art. 20 DSGVO nur die aus dem direkten Kundenkontakt „bereitgestellten" bruchstückhaften Informationen betreffen. Aus der Sicht des Branchenvertreters ermöglicht die Datenportabilität in solchen Fällen keinen „Mehrwert" für die informationelle Selbstbestimmung des Kunden und bedeutet zugleich einen erheblichen Aufwand für die einzelnen Dienstleister (insbesondere für KMUs). Die Inkassobranche sieht sich daher nicht als primärer Adressat des Art. 20 DSGVO und erhofft eine Klarstellung bezüglich des Anwendungsbereichs der Regelung.

- Stellvertretend für den **Energiesektor** – wo die Frage der Datenübertragbarkeit vor allem die Energielieferanten betrifft – stellt der Geschäftsführer der **regiocom GmbH**, Klemens Gutmann, in seinem an die Stiftung Datenschutz eingereichten Positionspapier[70] die bereichsspezifischen Herausforderungen bei der Umsetzung der Datenportabilität vor. Insbesondere die anstehende Einführung des Smart Metering führe zu erweiterten Formen der Erhebung von Kundendaten, deren Weiterleitung grundsätzlich ein Mehr an informationeller Selbstbestimmung darstellen könnte. Da es dazu jedoch nur wenige richtungsweisende Beispiele gebe und Deutschland bei der Umsetzung eines flächendeckenden Smart Meter-Rollout erst am Anfang stehe, ergäben sich viele offene Fragen. Es müsse zunächst die Frage des Inhalts, des Umfangs und des Formats der weiterzuleitenden Daten geklärt werden. Eine branchenspezifische Formatfestlegung hätte hierbei den Vorteil, die bereits praxisbewährten Beispiele zu Rate ziehen und kundenspezifische Daten relativ redundanzarm übermitteln zu können. Es müsse außerdem ein endkundenpraktikables Format festgelegt werden. Darüber hinaus müsse die Frage nach der Schnittstellenbildung bei der Verzahnung von klassischen Energiedaten mit anderen haushaltsnahen Anwendungsbereichen, wie es bspw. im Smart-Home der Fall sein dürfte, geklärt werden. Auch die Abgrenzung zwischen „bereitgestellten" und „verarbeiteten" Daten würde vor dem Hintergrund der zukünftigen Situation mit Smart Meter-Geräten immer komplexer.

69 Siehe Abschnitt D.
70 Siehe Abschnitt D.

- In einer an die Stiftung Datenschutz eingereichten Stellungnahme wird vom IT-Branchenverband **Bitkom**[71] betont, dass der Begriff „bereitstellen“ („provided“) in der DSGVO nicht legal definiert sei und somit viele Unklarheiten bereite. Die Vorschrift solle daher gemäß ihrem Wortlaut interpretiert werden, wonach von der Regelung nur diejenigen Daten umfasst sind, welche von einer Person einem Verantwortlichen „bereitgestellt“ wurden. Demnach solle es ausreichend sein, nur diejenigen Daten zu berücksichtigen, die der Betroffene kontrolliert und über die er selbst verfügt. Dies schließe die Nutzungsdaten bzw. Daten, die bei der Nutzung des Dienstes automatisch generiert werden, aus. Bezüglich der technischen Umsetzung wird die Entwicklung von sektorübergreifenden Einheitslösungen als unverhältnismäßig abgelehnt und die Ausarbeitung von branchenspezifischen Standards und Formaten begrüßt.

- Im Rahmen der öffentlichen Konsultation des White House Office of Science and Technology Policy (OSTP) zur Umsetzung der Datenportabilität hat unter anderen der Branchenverband **Software & Information Industry Association (SIIA)** Stellung genommen.[72] Bei der Auseinandersetzung mit der Umsetzung der Datenübertragbarkeit plädierte SIIA je nach Service und Datenverarbeitungskontext für eine striktere Differenzierung zwischen unterschiedlichen Arten von personenbezogenen Daten sowie für die Beachtung kollidierender Rechtsgüter wie Lizenzvereinbarungen, geistiges Eigentum und Persönlichkeitsrechte Dritter. Es wird außerdem auf die Schwierigkeiten der praktischen Implementierung der Portabilität verwiesen, wie z.B. Entwicklung kompatibler Produkt-Formate (mitunter auch durch miteinander konkurrierende Unternehmen), Etablierung strategischer Partnerschaften sowie in Bezug auf begrenzte Ressourcen und Kapazitäten bei kleinen und mittelständischen Unternehmen. Nach Ansicht von SIIA soll bei den politischen Forderungen nach Datenportabilität daher besonders die Verhältnismäßigkeit zwischen dem Umsetzungsaufwand und dem tatsächlichen Mehrwert für die Verbraucher berücksichtigt werden. Die Datenübertragbarkeit solle in erster Linie in Bereichen gefördert werden, in denen deren Mehrwert und Nutzen evident ist (z.B. im E-Health-Bereich). Bei der Implementierung der Datenportabilität sieht SIIA die US-Regierung vor allem in der Rolle der Vermittlerin, Förderin und Moderatorin im Entwicklungsprozess. Die Ausarbeitung von Lösungsansätzen und Entwicklung von technischen Standards solle dagegen durch Marktteilnehmer vorangetrieben werden.

71 Siehe Abschnitt D.

72 White House Office of Science and Technology Policy. Request for Information Regarding Data Portability. 10.01.2017, Respondent 14, S. 23-28. Siehe auch: http://www.siia.net/LinkClick.aspx?fileticket=L8dzKaK9Mx8%3d&tabid=577&portalid=0&mid=17113.

II. Bestehende Lösungsansätze

Für die praktische Umsetzung des Rechts auf Datenübertragbarkeit und Datenübertragung existieren bislang nur wenige Beispiele. Darunter gibt es kaum Ansätze, welche explizit im Hinblick auf die Umsetzung der Anforderungen der Grundverordnung entwickelt wurden. Zwar bemühen sich viele Unternehmen, sich auf die neue Rechtslage zur Datenportabilität vorzubereiten.[73] Dennoch bereitet das neue Instrument vielen noch Sorge[74]. Vor diesem Hintergrund ist es lohnend, die bereits bestehenden Ansätze näher zu betrachten. Im Folgenden werden einige Ansätze zur Datenübertragbarkeit kurz vorgestellt:

- Gerade im Hinblick auf die ursprüngliche Intention des Gesetzgebers, durch Art. 20 DSGVO den Nutzer von „Lock-in-Effekten" bei großen sozialen Netzwerken zu befreien, ist die Initiative **Give Me My Data** (http://givememydata.com) bemerkenswert. Ab 2009 half der kostenlose Dienst aus den USA, Nutzerdaten aus Facebook in einem wiederverwendbaren Format abzurufen, zu archivieren und entsprechend wiederzuverwerten. Ende 2010 hat Facebook einen eigenen Dienst entwickelt und verlangte von Apps, welche Zugriff auf den Dienst des Netzwerks hatten, ein Update, nach dessen Durchführung das Unternehmen eigens bestimmen konnte, welche Drittanbieter-Apps den Zugriff auf die Nutzerdaten bekommen. Die Zugriffseinschränkungen führten schließlich dazu, dass der Entwickler von „Give Me My Data" 2016 seinen Dienst einstellte.[75] Mit einem Video klärt er allerdings die Nutzer weiterhin auf, wie man eigenständig den Zugriff auf von Facebook gespeicherte Daten bekommt[76]. Die Komplexität des Vorgangs lässt jedoch Zweifel aufkommen, ob Durchschnittsnutzer den vorgeschlagenen aufwändigen Weg in Anspruch nehmen.

- Google hat bereits 2011 für angemeldete Nutzer mit Google-Konto mit dem Online-Dienst **„Google Takeout"**[77] die Möglichkeit geschaffen, persönliche Daten aus mehr als 30 von Google angebotenen Online-Diensten wie Maps, Gmail oder Contacts in verschiedenen Formaten zu exportieren. So wird ein Archiv mit den ausgewählten Daten wie Fotos von Google+, Videos von YouTube, Mails und Positionsdaten von Latitude erstellt und zum Download angeboten. Takeout verwendet Standardformate, wodurch den Nutzern zusätzliche Optionen für den Umgang mit exportierten Daten eröffnet werden. Sie können diese Daten für Backups oder andere Zwecke verwenden oder zu Diensten anderer Anbieter wie Dropbox und Microsoft OneDrive direkt portieren. Mit MyAccount (www.myaccount.google.com) wird außerdem ein zentraler Hub angeboten, um Privatsphäreeinstellungen vorzunehmen und einen Überblick über gespeicherte Daten und Zugriffsrechte zu verschaffen. Nach Angabe von Google verzeichnet der Dienst gegenwärtig mehr als eine Million Export-Vorgänge monatlich.

73 Vgl., euobserver, New EU right to data portability to case headaches, 24.05.2017. URL: https://euobserver.com/digital/137977.

74 Laut einer Umfrage des Softwareherstellers SAS sehen 58 der befragten Unternehmen Probleme mit der Umsetzung der Datenportabilität (www.pressetext.com/news/20171004025).

75 http://givememydata.com/. Siehe auch: White House Office of Science and Technology Policy. Request for Information Regarding Data Portability. 10.01.2017, Respondent 9, S. 12.

76 www.youtube.com/watch?v=WteK95AppF4&feature=youtu.be.

77 Siehe Abschnitt D, Stellungnahme von Google, https://takeout.google.com/settings/takeout

- Auch in Europa existieren bereits erwähnenswerte Ansätze zur Umsetzung der Datenportabilität. So bietet das französische Start-up ONECUB[78] einen Datenübertragungsdienst auf PIMS-Basis an, den **„ONECUB Connect Button“**.[79] Das Portabilitäts-Tool verwaltet den Austausch von personenbezogenen Daten, indem es dem Einzelnen ermöglicht, seine persönlichen Daten zu sammeln und über eine API-Schnittstelle zwischen externen Webseiten oder Online-Diensten sicher zu übertragen. So können ONECUB-Nutzer ihre Daten mit Drittanbietern austauschen, während sie ihre Privatheitseinstellungen in vollem Umfang kontrollieren. Der Service ist bereits von einigen Unternehmen integriert, so von der Verkaufsplattform „MyTroc“, dem Fluggast-Entschädigungsservice „Air Indemnité“ und dem Fitness-Coach „Umanlife“. ONECUB ist außerdem seit über sieben Jahren in der amerikanischen VRM (Vendor Relationship Management) Community und in der französischen MesInfo Community beteiligt und diskutiert regelmäßig die grundlegenden Aspekte der Datenschutzgrundverordnung und der Datenportabilität mit französischen Start-ups, großen Unternehmen, Beratungsfirmen und der französischen Aufsichtsbehörde CNIL.

- Ende 2016 wurde von dem französischen Think-Tank **Fondation Internet Nouvelle Génération (FING)** und acht führenden Unternehmen (Crédit Coopératif, Enedis, Engie, GRDF, Maif, Mgen, Orange, Société Générale) das Open Source-Projekt **„Rainbow Button“** (Arbeitstitel) initiiert, um einen gemeinsamen Rahmen für die Umsetzung des Rechts auf Datenübertragbarkeit zu erarbeiten.[80] Inzwischen gehört auch die französische Datenschutzbehörde CNIL zu den Projektteilnehmern. Ziel des Projekts ist es, durch die Erarbeitung von gemeinsamen Spezifikationen, Richtlinien und Design die Komplexität der Umsetzung der Datenportabilität zu reduzieren, die Handhabbarkeit für die Nutzer zu ermöglichen, Missbrauch zu verhindern sowie einen Rahmen für die Entwicklung von innovativen Services zu schaffen. Dazu wird von den Projektteilnehmern ein Prototyp entwickelt, um die Vorteile des Portabilitätsdienstes zu demonstrieren und verschiedene Einsatzszenarien zu erproben. Unter der Beachtung von DSGVO-Anforderungen zur Datenportabilität werden im Projekt insbesondere zwei Einsatzszenarien erarbeitet: zum einen der „Download“ von Daten aus einem Nutzerkonto, zum anderen die Übertragung von Daten zwischen unterschiedlichen Daten-Controllern.

78 https://www.onecub.com/

79 Siehe Abschnitt D.

80 http://mesinfos.fing.org/wp-content/uploads/2017/03/RButton_Perimetre_english.pdf.

- In den USA sind bereits einige Ansätze zur Datenübertragbarkeit entwickelt worden. So setzt sich die seit 2010 gestartete **My Data-Initiative des Weißen Hauses** für die Verbesserung des Zugangs der Nutzer zu ihren personenbezogenen Daten ein.[81] Die Initiative stellt einen kollaborativen Vorstoß dar, in Zusammenarbeit mit öffentlichen und privaten Organisationen Lösungsvorschläge für die Ermöglichung der Datenübertragbarkeit zu entwickeln. In Kooperation mit dem privaten Sektor wurden dabei vielfältige Ansätze entwickelt, wie zum Beispiel **„Green Button"** für die Stromversorgungsdaten[82] oder „My Student Data" für Studierenden-Daten. Dazu gehört auch die „My Data Healthcare"-Initiative **„Blue Button"** für den verbesserten Zugang, Kontrolle und Übertragung von medizinischen Daten.[83] „Blue Button" ist dabei ein Symbol auf einer Website, wie zum Beispiel einem Online-Patientenportal, mit dessen Hilfe die Patienten ihre Gesundheitsinformationen herunterladen können. Abhängig von der Implementierung können die Nutzer eine Vielzahl von Informationen in mehreren Formaten, einschließlich Text und PDF, herunterladen. „Blue Button" bietet außerdem den Ärzten eine einfache Möglichkeit, Patientendaten zu übertragen. Die Verwaltung von Blue Button Trust Bundle wurde der gemeinnützigen **Trust-Community NATE** übertragen.[84] Genauso wie „Blue Button" finden sich weitere funktionsfähige Portabilitätsansätze insbesondere im US-Gesundheitssektor.

So ist beispielsweise **DirectTrust.org** Inc. eine Organisation, die vom US-Amerikanischen Office of the National Coordinator for Health Information Technology (ONC) als eine „trust community" gegründet wurde. Als unabhängige gemeinnützige Vereinigung von 124 Gesundheits-IT- und Gesundheitsdienstleistern unterstützt sie einen sicheren, interoperablen Austausch von Gesundheitsinformationen über Direct-Message-Protokolle. DirectTrust hat ein „Trust Framework" geschaffen, das die Nutzung von Direct-Exchange auf über 94.000 Gesundheitsorganisationen und mehr als 1,4 Mio. Direktadressen und Konten erweitert.[85] Vor Kurzem erarbeitete DirectTrust außerdem einige Vorschläge zur technischen Standardisierung im Gesundheitsbereich.[86] Auch die bereits erwähnte Trust-Community NATE setzt sich in einer transsektoralen Zusammenarbeit mit Verbraucherschutzorganisationen, Healthcare-Experten, Technologieunternehmen und ehemaligen Politikern für die Verbesserung der Datenübertragbarkeit im Gesundheitswesen ein. Zusammenfassend lässt sich feststellen, dass die Datenportabilität von Gesundheitsinformationen innerhalb des US-Gesundheitssystems sich bereits in einem fortgeschrittenen Entwicklungsstadium befindet, was nicht zuletzt auf neue Kooperationsformen von Staat, Wirtschaft und Non-Profit-Organisationen zurückzuführen ist.

81 https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access

82 http://www.greenbuttondata.org/

83 http://www.myphr.com/Resources/blue_button.aspx

84 http://nate-trust.org/?s=Blue+button

85 https://www.directtrust.org/about-directtrust/

86 DirectTrust, Comment to ONC on Draft 2017 Interoperability Standards Advisory, S. 4-6. URL: https://www.directtrust.org/wp-content/uploads/2016/11/DirectTrusts-Comments-to-ONC-on-Draft-2017-Interoperability-Standards-Advisory.pdf

C. Bewertung und Handlungsempfehlungen

I. Bewertung

1. Zielrichtung der Norm

Chancen und Risiken der Datenportabilität

Die Auseinandersetzung mit dem Recht auf Datenübertragbarkeit, mit Stellungnahmen relevanter Stakeholder und die Betrachtung von bestehenden Lösungsansätzen lässt zuvörderst die Frage aufkommen, in welchem Umfang die neue Norm für die Verbraucher einen Zuwachs an informationeller Selbstbestimmung bedeutet. Dabei muss bedacht werden, dass die Übermittlung der Daten gemäß der Regelung des Art. 20 DSGVO lediglich **eine Kopie des Datensatzes** betrifft und keinen Anspruch auf Löschung begründet.

Einerseits würden die Nutzer tatsächlich **von der Flexibilität profitieren,** ihre Daten vereinfacht unterschiedlichen Dienstanbietern zur Verfügung zu stellen. Das Recht auf Datenübertragung wäre insbesondere im sogenannten Internet-of-Things hilfreich, wenn die Menschen die Daten aus der Nutzung vernetzter Geräte nicht nur im Verhältnis zum Anbieter eines bestimmten Produkts, sondern auch für andere Zwecke nutzen und Daten unterschiedlicher Service-Anbieter miteinander verknüpfen könnten.

Andererseits könnte die mit der Datenübertragung einhergehende Vervielfältigung von personenbezogenen Daten eine **Steigerung von Datenschutzrisiken** bedeuten. Dies gelte jedenfalls für die möglichen Fälle, in denen Anspruchsinhaber vom Adressaten des Übertragungsanspruches nicht zugleich ihr Recht aus Art. 17 DSGVO (Löschung) geltend machen. Die Datenübertragung erfolgt somit nicht im Sinne einer echten „Daten-Mitnahme“, sondern vielmehr als „Daten-Duplizierung“. Die Nutzung personenbezogener Daten wird damit nicht nur etwa minimiert, sondern eher ausgedehnt – mit all den allgemein bestehenden Unsicherheiten[87] bezüglich der Datennutzung durch datenverarbeitende Stellen.

Das Ziel der Regelung, die informationelle Selbstbestimmung zu fördern, könnte sich insbesondere dann ins Gegenteil verkehren, wenn Verbraucher durch Setzung finanzieller Anreize, wie etwa vergünstigter Vertragskonditionen, dazu verleitet werden, ihre Rechte aus Art. 20 DSGVO übermäßig wahrzunehmen. Das „Recht auf Datenübertragbarkeit“ könnte sich damit de facto als eine latente **„Pflicht“ zur Vervielfältigung von Datensätzen** erweisen. Es könnten sich Geschäftsmodelle etablieren, welche das Portabilitätsrecht der Verbraucher bewusst für die Akkumulation personenbezogener Daten und die Erstellung sektorübergreifender Kundenprofile nutzen. Diese Befürchtung greift offensichtlich auch der Schweizer Bundesrat auf, wenn er feststellt, das Recht auf Datenübertragung sei „mehr darauf ausgerichtet, den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen, als ihre Persönlichkeit zu schützen“.[88]

87 Zum Problemfeld der „informierten Einwilligung“ siehe Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“, URL: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/.

88 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, 21. Dezember 2016, S. 22. www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf

Datenschutz- und Datensicherheitsrisiken sind vor allem dann hoch, wenn es sich um besonders sensible Daten handelt – wie beispielsweise bei Versicherungs- und Gesundheitsdaten. Hier muss insbesondere auf eine **eindeutige Authentifizierung** von Datenempfängern sowie auf die Gewährleistung eines gleichwertigen Datenschutz- und Datensicherheitsniveaus geachtet werden, da ansonsten missbräuchliche Datenübertragungsbitten leicht möglich werden.

Eine **Missbrauchsgefahr** könnte beispielsweise dann entstehen, wenn ein Unternehmen (z.B. eine größere Kfz-Werkstattkette) seine Kunden zur Ausübung ihrer Portierungsansprüche gleichsam anstiftet, um durch exzessive Datenabfragen (z.B. bei einer kleineren Kfz-Werkstatt) die Konkurrenzfähigkeit des Mitbewerbers zu beeinträchtigen. Mit Blick auf derartige Konstellationen muss gleichwohl darauf verwiesen werden, dass Fälle exzessiver oder anderweitig missbräuchlicher Anfragen von Art. 12 Abs. 5 DSGVO (Weigerungsmöglichkeit bei offenkundig unbegründetem oder exzessivem Charakter) erfasst sein dürften.

Bei vielen Akteuren bestehen außerdem Sorgen, dass sich das Recht auf Datenübertragbarkeit zum **Wettbewerbsnachteil** entwickeln könnte. So sind beispielsweise einige spendensammelnde Organisationen (NGOs) besorgt, dass sie im Fall der Anwendung des Art. 20 DSGVO die gesamte Historie eines Spenders an konkurrierende NGOs übertragen müssten und dass sich aus diesen Daten die Arbeitsweise der betreffenden NGO ablesen lasse und so Betriebsgeheimnisse preisgegeben würden. Außerdem könnten sich die Umsetzungskosten für die Datenübertragbarkeit zum Nachteil von Start-ups und kleineren Unternehmen auswirken, da die etablierten Unternehmen mit ihren Ressourcen die Marktmacht viel eher ausweiten könnten – zum Nachteil der User.

Nicht zuletzt scheinen Zweifel darüber berechtigt zu sein, dass die Norm große Marktmonopole und **„Netzwerkeffekte“** aufzubrechen vermag. Zwar könnten Datenportabilität und Interoperabilität grundsätzlich geeignete Maßnahmen darstellen, um ein offenes und freies soziales Netz zu ermöglichen, in dem Nutzer die Kontrolle über ihre Daten behalten und frei kommunizieren können.[89] Ob jedoch allein die Implementierung eines Portabilitätsservice in der Praxis zum Aufbrechen von „Lock-in-Effekten“ führt, bleibt offen. Insbesondere bietet das Beispiel des seit sechs Jahren bestehenden „Google Takeout“-Services, das in seinem Wesenskern den Anforderungen des Rechts auf Datenübertragbarkeit entspricht, keinen Anhaltspunkt dafür, dass durch das Angebot der „Daten-Mitnahme“ die marktdominierende Stellung von Google in irgendeiner Weise „aufgebrochen“ wäre. Vor allem bei sozialen Netzwerken ist der Zweifel an der Wirksamkeit der Norm groß, da die Portierung der für die Nutzer wahrscheinlich interessantesten Daten – erstellte Nutzer-Analysen, Nutzer-Profile, aber auch die Daten mit dem Bezug zu Dritten (z.B. zu Facebook-„Freunden“) – von der Regelung des Art. 20 DSGVO ausgenommen ist. Gleichwohl muss angemerkt werden, dass die Wirksamkeit der Regelung bei denjenigen Anbietern abzuwarten ist, welche „Netzwerkeffekte“ aus der Verbindung von Online-Diensten mit der Nutzung bestimmter Hardware-Produkte erzeugen, wie beispielsweise im Ökosystem von Apple.

89 Vgl., Göndör, Sebastian, siehe Abschnitt D.

Förderung der Datensouveränität

Um die Förderung der informationellen Selbstbestimmung durch das Recht auf Datenübertragbarkeit zu gewährleisten, muss die **Wirksamkeit der Norm** sichergestellt werden. Denn die Datensubjekte werden das Recht auf Datenübertragbarkeit erst dann nutzen, wenn ihnen der Mehrwert ersichtlich ist und ihnen der damit verbundene Aufwand verhältnismäßig zum Nutzen erscheint. Zum einen muss daher die Wirksamkeit konkreter Lösungsansätze einem Praxistest unterzogen werden. Das beinhaltet u.a. verhaltensökonomische Untersuchungen, inwieweit die Möglichkeit der Datenübertragung von den Nutzern tatsächlich in Anspruch genommen wird.

Zum anderen muss bei der Implementierung der Norm präzisiert werden, dass von dem Recht auf Datenübertragbarkeit explizit nur diejenigen Daten erfasst sind, deren Übertragbarkeit effektiv einen **Beitrag zur Förderung der informationellen Selbstbestimmung** leistet. Eine zu weite Auslegung der Norm kann unter Umständen Datenschutzrisiken ausweiten und zugleich unverhältnismäßig großen Aufwand beim Kategorisieren und Herausziehen von Datensätzen bei den datenverarbeitenden Stellen verursachen. Daher muss bei der Interpretation des Art. 20 DSGVO die ursprüngliche Intention des Gesetzgebers in den Vordergrund gerückt werden, nämlich mehr Datenkontrolle zu ermöglichen. Der Anwendungsbereich der Norm sollte daher auf für den Anbieterwechsel erforderliche Datensätze fokussiert werden. Auch sollte der Nutzer zur Kontrollermöglichung die erhaltenen Datensätze grundsätzlich verstehen und zu seinem Vorteil verwenden können. Dies gilt zumindest bei Fällen eigenen Erhalts der Daten (Art. 20 Abs. 1 DSGVO), weniger bei veranlasster Direktübertragung nach Absatz 2. Die **Verhältnismäßigkeit** zwischen dem Aufwand der Normumsetzung und der praktischen Wirksamkeit von Einzelmaßnahmen für die Datensouveränität darf außerdem nicht aus dem Blick geraten.

Die praktische Ausgestaltung der Norm muss sich an ihrer ursprünglichen und durch die zweite Empfehlungs-Fassung der Artikel-29-Datenschutzgruppe wieder in den Vordergrund gerückten Intention orientieren: der Stärkung der informationellen Selbstbestimmung der Verbraucher. Dies heißt im Kontext des Rechts auf Datenportabilität, dem Nutzer **mehr Kontrolle über die Weitergabe von persönlichen Daten** zu ermöglichen.

Fazit

Zusammenfassend lässt sich feststellen, dass das Recht auf Datenportabilität den Nutzerinnen und Nutzern grundsätzlich bessere Kontrollmöglichkeiten über personenbezogene Daten verschaffen kann. Allerdings dürfen die Risiken, welche die neue Regelung mit sich bringen kann, nicht unterschätzt werden: Zum einen kann die Vervielfältigung von Datensätzen zur Steigerung von Datenschutzrisiken führen. Insbesondere dann, wenn Verbraucher durch Setzung finanzieller Anreize wie vergünstigte Vertragskonditionen dazu verleitet werden, ihre Rechte aus Art. 20 DSGVO übermäßig wahrzunehmen und das Portabilitätsrecht der Nutzer bewusst für die Akkumulation personenbezogener Daten und die Erstellung sektorübergreifender Kundenprofile instrumentalisiert wird. Zum anderen kann die Norm ins Leere laufen oder sich sogar als wettbewerbshemmend erweisen, wenn einem tatsächlich geringen praktischen Verbrauchernutzen der zu übertragenden Datensätze ein hoch intensiver Aufwand bei deren Aufbereitung und Übermittlung durch datenverarbeitende Stellen gegenübersteht und jenen nur die großen Marktteilnehmer bewältigen können. Schließlich scheinen bei der Betrachtung von bisherigen Ansätzen auch Zweifel berechtigt zu sein, ob die Implementierung eines Portabilitätsservice in der Praxis zwangsläufig zum Aufbrechen von Marktmonopolen und „Lock-in-Effekten“ führen würde. Zu bedenken ist, dass sich hohe Umsetzungskosten für die Datenübertragbarkeit zum Nachteil von Start-ups und kleineren Unternehmen auswirken können.

2. Bestimmung des Anwendungsbereichs[90]

Bereitgestellte Daten

Der Begriff **„bereitgestellte Daten“** in Art. 20 ist in der Datenschutzgrundverordnung nicht legal definiert. Die Artikel-29-Datenschutzgruppe legt diesen Begriff in ihren Stellungnahmen (Guidelines on the right to data portability) weit aus und fasst unter den Anwendungsbereich sowohl **Vertrags- als auch Nutzungsdaten.**[91] Damit sind ebenso die sogenannten „observed data“ umfasst, also die Daten, die aufgrund der Inanspruchnahme eines Dienstes erzeugt werden.[92] Diese Ausweitung, die gleichermaßen Verkehrs- und Standortdaten umfasst, wird mit Verweis auf den Wortlaut abgelehnt.[93] Im Sinne einer solchen engen Auslegung des Merkmals „Bereitstellen“ wären lediglich Daten erfasst, die die betroffene Person aktiv und bewusst zur Verfügung stellt und die für die Vertragserfüllung erforderlich sind, jedoch keine Nutzungsdaten.[94] In diesem Zusammenhang wird außerdem darauf verwiesen, dass sowohl die Historie des Gesetzgebungsverfahrens als auch das Regelungsziel des Art. 20 DSGVO für diese enge Auslegung sprächen.[95] Daten, die der Verantwortliche erst aufgrund der bereitgestellten Daten selbst ausgewertet und erzeugt hat („inferred data“, etwa Score-Werte), sind nach einhelliger Auffassung allerdings nicht vom Anwendungsbereich erfasst.[96]

Im Hinblick auf die **Daten Dritter** müssen gemäß Art. 20 Abs. 4 DSGVO deren Schutzrechte beachtet werden. Hier beschreibt die Artikel-29-Datenschutzgruppe, dass die personenbezogenen Daten Dritter für den privaten und persönlichen Gebrauch zu einem neuen Verantwortlichen übertragen werden dürfen, sofern sie unter der ausschließlichen Kontrolle der übertragenden Person bleiben.[97] Die Datenschutzgrundverordnung findet zwar keine Anwendung, wenn die Datenverarbeitung „durch natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht“ erfolgt. Zu berücksichtigen ist hier jedoch, dass personenbezogene Daten zu einem kommerziellen Anbieter übertragen werden. Daher ist die Umsetzung in der Praxis seitens dieser neuen Verantwortlichen fraglich.

90 Das folgende Kapitel basiert auf der Stellungnahme von Anne Riechert, siehe Kap. D. III.

91 Artikel-29-Datenschutzgruppe, WP 242 “Guidelines on the right to data portability” vom 13.12.2016 und Artikel-29-Datenschutzgruppe, WP 242 “Guidelines on the right to data portability” vom 05.04.2017

92 Artikel-29-Datenschutzgruppe, WP 242, S. 5; Benedikt, RDV 2017, S. 190; Jülicher/Röttgen/v. Schönfeld, ZD 2016, S. 359, die ein aktives Tun als Voraussetzung ablehnen.

93 Siehe Bitkom, Stellungnahme Datenportabilität (Stellungnahme zum Recht auf Datenübertragbarkeit nach Art. 20 Datenschutzgrundverordnung) vom 14.03.2017, S. 7 sowie Stellungnahme Deutsche Telekom AG (Statement on the “Guidelines on the right to data portability“ of the Article 29 Data Protection Working Party), S. 2. Siehe auch Bitkom, Stellungnahme Datenportabilität, S. 11 mit dem Hinweis, dass Telekommunikations- und Standortdaten nicht vom Anwendungsbereich erfasst sind. Anders allerdings Artikel-29-Datenschutzgruppe, WP 242, S. 10, die dies befürwortet.

94 Siehe Strubel, ZD 8/2017, S. 357/358, der darlegt, dass ein „Geschehenlassen“ nicht ausreichen soll und damit die Direkterhebung gemeint sei. Siehe auch Stellungnahme Deutsche Telekom AG, S. 2, die das Merkmal auf „nützliche“ und vom Nutzer kontrollierte Daten begrenzt. Darüber hinaus wird vorgeschlagen, das Merkmal des Bereitstellens service-spezifisch auszulegen und damit den Anspruch lediglich auf die Daten anzuwenden, die für die Nutzung eines vergleichbaren Dienstes erforderlich sind (siehe hierzu Strubel, ZD 8/2017, S. 360, der danach trennt, ob die Daten notwendig sind, um einen vergleichbaren Service anbieten zu können).

95 Strubel, ZD 8/2017, S. 357 ff., außerdem in der rechtlichen Stellungnahme von Anne Riechert ausführlich unter Punkt 1.1, siehe Kap. D. III.

96 Artikel-29-Datenschutzgruppe, WP 242, S. 10.

97 Artikel-29-Datenschutzgruppe, WP 242, S. 11 ff. Die Artikel-29-Datenschutzgruppe führt zwar einerseits aus, dass ein neuer Verantwortlicher die übermittelten Daten Dritter nicht für seine eigenen Zwecke (z.B. zur Anpreisung von Marketingprodukten und Diensten) verwenden dürfe. Aber andererseits hält sie eine solche Verarbeitung auch nur mit hoher Wahrscheinlichkeit für unrechtmäßig und unfair, insbesondere wenn die betroffenen anderen Personen nicht darüber informiert würden und nicht von ihrem Recht als betroffene Personen Gebrauch machen könnten. Eine mögliche weitere Verarbeitungsmöglichkeit durch den neuen Verantwortlichen muss von daher vor allem unter einer zulässigen und gemäß Wortlaut der Datenschutzgrundverordnung mit allen Verarbeitungstatbeständen auf gleicher Stufe stehenden Verarbeitung aufgrund „berechtigter Interessen“ gesehen werden, hinsichtlich derer jedoch bislang noch keine europaweit einheitlichen Auslegungsregeln entwickelt wurden.

Dies gilt insbesondere im Hinblick auf die Möglichkeit, Daten aufgrund berechtigter Interessen gemäß Art. 6 Abs. 1f DSGVO oder aufgrund einer Zweckänderung gemäß Art. 6 Ab. 4 DSGVO zu verarbeiten. Mangels entsprechender europaweit einheitlicher Auslegungskriterien für diese Verarbeitungstatbestände wäre daher für betroffene Dritte das Ausmaß einer möglichen Datenverarbeitung zurzeit noch nicht absehbar. Hauptsächlich ist zu berücksichtigen, dass die Dritten sich zuvor bewusst gegen einen Dienstleister entschieden haben könnten, sodass hier grundsätzlich außerdem zivilrechtliche Ansprüche, etwa auf Unterlassung, in Betracht kommen könnten. Von außerordentlicher Bedeutung ist daher insgesamt ebenso die Sicherstellung von ausreichender **Transparenz**. Die jeweils betroffene Person darf nicht den Überblick über die Datenverantwortlichen und die ihr zustehenden Löschungsansprüche verlieren.

Gemäß dem Wortlaut sind auch **Arbeitnehmerdaten** vom Anwendungsbereich des Art. 20 DSGVO erfasst. Da aber die Anwendbarkeit im Einzelfall strittig ist, sind demzufolge auch für diesen Aspekt entsprechende Auslegungskriterien zu entwickeln.[98]

Interoperables Format

Art. 20 DSGVO enthält keine Definition für ein **interoperables Format.** Gemäß der Intention der Datenportabilität ist es jedoch wichtig, dass ein Format genutzt wird, welches die sinnvolle Weiterverwendung der Daten durch den Betroffenen oder den neuen Verantwortlichen ermöglicht. Ein solches soll zukünftig entwickelt werden.[99] Daher könnten einzelne Formate wie etwa ein PDF-Dokument als maschinenlesbares Format ausgeschlossen sein, auch wenn dieses Format im Rahmen des Auskunftsrechts als elektronisches Format ausreichend ist.

Außerdem ist strittig, ob die Übersendung von **Metadaten** für die Datenportabilität vorteilhaft und notwendig ist[100] oder aber gerade den Interessen des Datenschutzes zuwiderläuft.[101] Die Artikel-29-Datenschutzgruppe ist der Auffassung, dass mit den personenbezogenen Daten möglichst viele Metadaten bereitgestellt werden sollten.[102] Allerdings erfolgt keine nähere Konkretisierung, was Metadaten in Abgrenzung zu personenbezogenen Daten auszeichnet. Auch aus technischer Sicht werden ausreichende Metadaten gefordert.[103] Im Sinne dieser Sichtweise können Metadaten zwar einerseits personenbezogen sein, jedoch andererseits gleichermaßen ein Attribut näher konkretisieren und beispielsweise Beschränkungen (z.B. der Textlänge) festlegen.

98 Hennemann, PinG 01.17, S. 5; Bitkom, Stellungnahme Datenportabilität, S. 8. Die Artikel-29-Datenschutzgruppe bezieht sich auf die jeweilige Prüfung im Einzelfall und schließt die Anwendbarkeit nicht generell aus (Artikel-29-Datenschutzgruppe, WP 242, S. 8/9).

99 Artikel-29-Datenschutzgruppe, WP 242, S. 18. Siehe außerdem Schätzle, PinG 02.16, S. 74/75; Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries, wobei diese Autoren in ihrer Stellungnahme die allgemeinen Bedingungen für ein entsprechendes Datenübertragungsformat anhand von unterschiedlichen Szenarien beschreiben und in der Übertragbarkeit an sich keine technische Hürde sehen. Siehe auch Hennemann, PinG 01.17, S. 8, der darauf hinweist, dass die Interoperabilität von Art. 20 Datenschutzgrundverordnung gerade nicht gefordert wird. Diese Voraussetzung ist lediglich in Erwägungsgrund 68 der Datenschutzgrundverordnung enthalten.

100 Siehe Artikel-29-Datenschutzgruppe, WP 242, S. 18, die Metadaten auf bester Granularitätsstufe vorschlägt; Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries, siehe Abschnitt D.

101 Siehe Stellungnahme Deutsche Telekom AG, in der darauf verwiesen wird, dass die Übersendung eines vollständigen Datensatzes mit der anschließenden Prüfung, ob tatsächlich alle Daten benötigt werden, aus Sicht des Datenschutzes sehr beunruhigend sei.

102 Artikel-29-Datenschutzgruppe, WP 242, S. 18.

103 Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries, siehe Abschnitt D.

Im Entwurf der E-Privacy-Verordnung[104] ist darüber hinaus für Kommunikationsmetadaten sogar eine gesetzliche Definition enthalten, die sich auf diejenigen Daten bezieht, aus denen sich Schlussfolgerungen über das Privatleben der an der elektronischen Kommunikation beteiligten Personen ziehen lassen.[105] Diese Metadaten können unter anderem Verkehrs- und Standortdaten sein, die allerdings von der Artikel-29-Datenschutzgruppe als „von der betroffenen Person bereitgestellte personenbezogene Daten" eingeordnet werden, was von Unternehmensseite wie oben dargestellt wiederum abgelehnt wird.

Daher empfiehlt sich die Prüfung, ob ein einheitliches technisches und juristisches Verständnis des Begriffs „Metadaten" besteht. Dies gilt insbesondere auch, um entscheiden zu können, welche Metadaten aus technischer Sicht für eine erfolgreiche Umsetzung der Datenportabilität sowie im Rahmen der Entwicklung des Formats erforderlich und aus rechtlicher Sicht zulässig sind.

Bei der technischen Machbarkeit der direkten Übertragbarkeit von Daten zwischen den Verantwortlichen wird im Übrigen darauf hingewiesen, dass dieses Merkmal sowohl subjektiv als auch objektiv ausgelegt werden könne.[106] Hier müssen also Kriterien dahingehend entwickelt werden, inwieweit die individuelle Leistungsfähigkeit der Unternehmen eine Rolle spielen kann.

Wettbewerbsrechtliche Gesichtspunkte

Bei Art. 20 DSGVO spielt die wettbewerbsrechtliche Sichtweise aus dem Grunde eine Rolle, da zum einen stets auf den wettbewerbsrechtlichen Charakter Bezug genommen wird[107] und zum anderen bewertet werden muss, inwieweit die Regelung eine Marktverhaltensregel darstellen kann. So könnte bei Nichtumsetzung der Interoperabilität sowie der mangelnden Bereitstellung einer mühelosen Übertragungsmöglichkeit der Daten ein Verstoß gegen § 3a UWG[108] (Rechtsbruch) und § 4 Nr. 4 UWG[109] (gezielte Behinderung der Mitbewerber) in Betracht kommen.[110]

104 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017 (E-Privacy-Verordnung). Gemäß Art. 95 der Datenschutzgrundverordnung werden natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auferlegt, soweit sie besonderen, in der Richtlinie 2002/58/EG festgelegten, Pflichten unterliegen, die dasselbe Ziel verfolgen. Die E-Privacy-Verordnung ist die Nachfolgeregelung und präzisiert und ergänzt durch die Festlegung besonderer Vorschriften die Datenschutzgrundverordnung.

105 Siehe die Begriffsdefinition von Metadaten der elektronischen Kommunikation auf S. 13 sowie unter Art. 4 Abs. 3 c der Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-Verordnung). Hierzu zählen beispielsweise angerufene Nummern, besuchte Websites, der geografische Standort, Uhrzeit, Datum und Dauer eines von einer Person getätigten Anrufs, aus denen sich präzise Schlussfolgerungen über das Privatleben der an der elektronischen Kommunikation beteiligten Personen ziehen lassen könnten, z. B. in Bezug auf ihre sozialen Beziehungen, Gewohnheiten und ihren Lebensalltag, ihre Interessen, ihren Geschmack.

106 Hennemann, PinG 01.17, S. 8.

107 Siehe etwa Hennemann, PinG 01.17, S. 6, der auf den wettbewerblichen Ansatz sowie auf das Gesetzgebungsverfahren hinweist, in welchem angeregt wurde, dieses Recht nicht im Zuge der Verordnung zu regeln.

108 § 3a UWG regelt den Rechtsbruch. Danach handelt unlauter, wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln, und der Verstoß geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen.

109 § 4 UWG regelt den Mitbewerberschutz. Danach handelt unlauter, wer Mitbewerber gezielt behindert.

110 In der deutschen Rechtsprechung ist umstritten, inwieweit datenschutzrechtliche Regelungen gleichzeitig Marktverhaltensregeln im Sinne des UWG darstellen. Verneinend etwa OLG München, Urteil vom 12. Januar 2012, Az. 29 U 3926/11: Das Datenschutzrecht sei Ausfluss des Persönlichkeitsrechts und schütze ganz allgemein diese Individualrechtsposition, und es gehe dabei nicht konkret um den Schutz in der Rolle als Marktteilnehmer. Die Bestimmungen des Bundesdatenschutzgesetzes stellten ungeachtet dessen, dass sich ihre Verletzung im Geschäftsleben durchaus auswirken kann, grundsätzlich keine Marktverhaltensregelungen dar (unter Verweis auf die Ausnahme des § 28 Abs. 4 S. 2 BDSG). Siehe außerdem OLG Köln, Urteil vom 19. November 2010, Az. 6 U 73/10; Kammergericht Berlin, Beschluss vom 29. April 2011, Az. 5 W 88/11; OLG Stuttgart, Urteil vom 22. Juli 2007, Az. 2 U 132/06.

Ein abmahnungsfähiger Wettbewerbsverstoß wurde in der Vergangenheit bei der Verletzung datenschutzrechtlicher Informationspflichten bejaht. [111]

Der Bundesgerichtshof nimmt etwa beim Vorwurf einer gezielten, wettbewerbswidrigen Behinderung eine Gesamtwürdigung der Umstände des Einzelfalls unter Berücksichtigung der Interessen der Mitbewerber, Verbraucher und sonstiger Marktteilnehmer sowie der Allgemeinheit vor.[112] Erforderlich hierfür sei, dass beide Parteien gleichartige Waren oder gewerbliche Leistungen absetzen würden, wobei jedoch keine Branchengleichheit vorliegen müsse.[113] Dagegen gewährt Art. 20 DSGVO „pauschal" das Recht zur Datenübertragbarkeit und beinhaltet keine Einschränkung und Interessensabwägung, etwa im Hinblick auf Branchen oder vergleichbare Dienstleistungen.

Das Gesetz gegen den unlauteren Wettbewerb und das Datenschutzrecht stehen gleichberechtigt nebeneinander. Fraglich ist daher, ob es zukünftig zu unterschiedlichen Bewertungen und Sanktionsmöglichkeiten kommen kann. Dies steht im Zusammenhang mit der Uneinigkeit über Sinn und Zweck des Art. 20 DSGVO, der zwar einerseits das informationelle Selbstbestimmungsrecht stärken soll, aber andererseits einschränkend dahin ausgelegt wird, dass (nur) die Datenübertragung von einem Dienstleister zum anderen erleichtert und „Lock-in-Effekte" vermieden werden sollen.[114] Letztere treten allerdings nicht zwangsläufig ein und ein Zwang zur Interoperabilität könnte ebenso wettbewerbshemmend wirken, insbesondere bei neuen innovativen Diensten, und einen erheblichen Eingriff in die unternehmerische Freiheit darstellen.[115]

Fazit

Das Recht auf Datenportabilität muss gewahrt werden, fraglich ist jedoch, ob nicht durch weitere Unterscheidungen und Würdigungen im Einzelfall ein interessengerechteres Ergebnis erzielt werden könnte. Bei der Streitfrage, ob sowohl Vertragsdaten als auch Nutzungsdaten vom Anwendungsbereich erfasst sind, könnte auch der Schutzbereich der Norm eine Rolle spielen, da Nutzungsdaten von der elektronischen Kopie des Auskunftsrechts gemäß Art. 15 Abs. 3 DSGVO vollumfänglich umfasst sind und damit das informationelle Selbstbestimmungsrecht gewahrt ist. Die Frage ist in diesem Zusammenhang ohnehin, ob der Vorteil einer direkten Übertragung sogar eher bei dem neuen Verantwortlichen liegen könnte, der durch Entwicklung neuer Geschäftsmodelle die betroffenen Personen animiert, ihre Nutzungsdaten preiszugeben.[116] Es sollte daher stets im Einzelfall abgewogen werden, unter welchen Umständen die direkte Übertragung von sämtlichen Nutzungsdaten zu einem anderen Dienstleister tatsächlich zur Verbesserung der Kontrollrechte der betroffenen Person beiträgt. Ein interessengerechtes Ergebnis könnte hier etwa durch die Objektivierbarkeit des Begriffs „erforderlich" hinsichtlich der vertragsrelevanten Daten gemäß Art. 20 Abs. 1a i.V.m. Art. 6 Abs. 1b DSGVO erreicht werden. So könnte gleichermaßen der Servicegedanke einfließen und etwa das Anlegen eines Kundenprofils (z.B. einer Kaufhistorie oder Aufzeichnungen einer Fitness-App) als „zur Vertragserfüllung erforderlich" und damit ebenfalls als sinnvolles Kundeninteresse gewertet werden.

111 OLG Hamburg, Urteil vom 27. Juni 2013, Az. 3 U 26/12 mit dem Argument, dass es sich bei § 13 TMG (Informationspflichten) um eine im Sinne des § 4 Nr. 11 UWG das Marktverhalten regelnde Norm handele (nun § 3a UWG) und nicht nur als eine Missachtung einer allein überindividuelle Belange des freien Wettbewerbs regelnden Vorschrift.

112 BGH, Urteil vom 22. 01.2014 – I ZR 164/12.

113 BGH, Urteil vom 24.06. 2004 – I ZR 26/02.

114 Siehe hierzu Hennemann, PinG 01.17, S. 6 mit Verweis auf Erwägungsgrund 68 der Datenschutzgrundverordnung.

115 Arbeit der Wissenschaftlichen Dienste des Bundestages zum Thema „Regulierung von Messengerdiensten, Datenportabilität und Interoperabilität", S. 18, auch unter Verweis auf die Auffassung des Bundeskartellamts. Siehe außerdem Hennemann, PinG 01.17, S. 6, der auf den wettbewerblichen Ansatz hinweist.

116 Siehe oben, C. I. 1 sowie Gutmann, Beispiele aus der Energiewirtschaft, der insgesamt die Frage nach einem „Mehr" an informationeller Selbstbestimmung für die betroffenen Personen kritisch beleuchtet.

In diesem Zusammenhang stellt die Sicherstellung von ausreichender Transparenz eine weitere wesentliche Anforderung dar, da der betroffenen Person alle Informationen, die sich auf die Verarbeitung durch den alten und neuen Verantwortlichen beziehen, bekannt sein müssen.

Im Hinblick auf die Abgrenzung zum Wettbewerbsrecht muss entschieden werden, inwieweit sich beide Rechtsgebiete gegenseitig beeinflussen können und es sich aus diesem Grunde empfehlen könnte, Kriterien zu entwickeln, die eine einheitliche Sichtweise von Wettbewerbsrecht und Datenschutzrecht sowie ein differenziertes Ergebnis erlauben. Bei der Bewertung und der Ausarbeitung von Verhaltensregeln gemäß Art. 40 DSGVO könnte berücksichtigt werden, ob das Interesse der Allgemeinheit sowie das informationelle Selbstbestimmungsrecht als Interesse der Betroffenen einen Anspruch auf „pauschale“ Datenübertragbarkeit umfasst. Zwar ist eine Interessensabwägung nicht vom Wortlaut des Art. 20 DSGVO umfasst. Dennoch könnte die Auslegung der Regelung einer fortwährenden praxisgerechten Prüfung dahingehend unterzogen werden, inwieweit beispielsweise nach Daten, Branchen, Diensten oder vergleichbaren Dienstleistungen im Einzelfall unterschieden werden kann, ohne dass andererseits das informationelle Selbstbestimmungsrecht der betroffenen Personen beeinträchtigt wird. Das wettbewerbsrechtliche Merkmal der Vergleichbarkeit der Dienstleistungen entspricht im Übrigen ebenso der ursprünglichen Gesetzesintention sowie dem Schutzzweck von Art. 20 DSGVO, da hier die sozialen Netzwerke im Fokus standen und der Anbieterwechsel erleichtert werden sollte.[117]

Zu bedenken ist außerdem, dass die Sanktionsmöglichkeiten der Datenschutzaufsichtsbehörden nun durch Erhöhung des Bußgeldrahmens empfindliche Konsequenzen bedeuten können.

3. Umsetzungsstrategien

Strukturelle Umsetzung

Die Ausgestaltung der Norm zur Datenübertragbarkeit spiegelt ein Grunddilemma der Netzregulierung wieder: Die Regulierung hat einerseits den Anspruch, die Rahmenbedingungen legaler Datenverarbeitung möglichst konkret zu gestalten, andererseits muss eine solche Regulierung „ex ante“ angesichts der neu zu entwickelnden Technologien und möglicher innovativer Lösungsansätze auf einem gewissen Allgemeinheitsgrad bleiben.[118] So fordert die Regelung zur Datenübertragbarkeit, dass der Erhalt der Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“ (Art. 20 Abs. 1 DSGVO) erfolgen soll, lässt zugleich allerdings offen, was genau unter einem solchen Format zu verstehen ist, welchen Anforderungen es genügen muss und wie die Interoperabilität zwischen unterschiedlichen „gängigen Formaten“ hergestellt werden könnte. Die einzelnen Normadressaten stehen damit vor der Herausforderung, den Anforderungen der Regelung zu genügen, ohne dafür einen konkreten Leitfaden, allgemeine Standards oder gar etablierte Praxis-beispiele zu haben. Damit offenbart sich in einer besonderen Weise das grundlegende **Problem des Fehlens geeigneter Umsetzungsstrategien datenschutzrechtlicher Regelungen.**

117 Siehe Hennemann, PinG 01.17., S. 6 mit Verweis auf den wettbewerblichen Ansatz sowie auf die Aussage von Jan Albrecht (Berichterstatter des Europäischen Parlaments zur Datenschutzgrundverordnung), der in Artikel 20 einen Katalysator eines Wettbewerbs um datenschutzfreundliche Technologien sieht.

118 Dazu: Horn, Aus Sicht der Stiftung Datenschutz – wie die Regulierung im Datenrecht Schritt halten kann, in PinG 05/17.

Insbesondere zeigen die Umsetzung der Datenportabilität im US-Amerikanischen Gesundheitssektor und das „Rainbow Button"-Projekt der Fondation Internet Nouvelle Génération (FING)[119], dass neue Formen von Public Private Partnership ein durchaus geeignetes Konzept zur praktischen Umsetzung von Anforderungen an die Datenübertragbarkeit und die Ausarbeitung von Standards darstellen können. Die Verwaltung der Zusammenarbeit zwischen Technologieunternehmen, Experten, Verbraucherschutzorganisationen, NGOs, öffentlichen Einrichtungen und politischen Entscheidungsträgern durch gemeinnützige unabhängige Institutionen („trust communities") nach dem Vorbild des US-Amerikanischen Gesundheitssektors[120] bringt dabei das notwendige Potenzial, um bei der Umsetzung des Rechts auf Datenportabilität einerseits den Schutzpflichten des Staates gerecht zu werden und andererseits eine flexible Innovationsentwicklung zu fördern.

Dazu müssen entsprechende Ansätze zur **„regulierten Selbstregulierung"** entwickelt werden, bei denen unter staatlicher Aufsicht ein Rahmen etabliert wird, in dem die staatlichen und nicht-staatlichen Institutionen sowie Unternehmen Umsetzungsstrategien und Standards für die Datenportabilität entwickeln. Für eine effektive Ausgestaltung der Datenübertragbarkeit und Herstellung von Rechtskonformität ist vor allem eine **frühzeitige Einbindung** der voraussichtlich besonders intensiv betroffenen Unternehmen und Branchen in formelle Konsultationsprozesse der Aufsichtsbehörden zur rechtskonformen Umsetzung von Art. 20 dringend wünschenswert.

Ansätze zur praktischen Umsetzung

Der Schwerpunkt der Arbeit in der praktischen Umsetzung des Rechts auf Datenübertragbarkeit liegt vor allem in der Ausarbeitung von Verfahren für den Datentransfer. Wie bereits in der zweiten Empfehlungs-Fassung der Artikel-29-Datenschutzgruppe (S. 16/neu) ausgeführt, bieten sich grundsätzlich **zwei Ansätze** für die Ermöglichung der Datenübertragbarkeit an: eine **direkte Übermittlung** an den Nutzer (Abs. 1) bzw. den Drittanbieter (Abs. 2) oder eine Übertragung mittels einer **zwischengeschalteten, zentralisierten Anwendung.**

Insbesondere in den Fällen, bei denen aufgrund spezifischer Geschäftsmodelle vom Recht auf Datenübertragbarkeit nur wenige, leicht zusammenzutragende und zu übermittelnde Datensätze betroffen sind, kann eine **direkte Übermittlung** von Daten verhältnismäßig leicht, effizient und auch nutzerseitig leicht handhabbar erfolgen. Außerdem ist zum gegenwärtigen Zeitpunkt noch unklar, wie viele Nutzer vom Recht auf Datenportabilität tatsächlich Gebrauch machen werden. Für die einzelnen Branchen und Unternehmen ist die **tatsächliche Nachfrage** nach der Datenübertragung insofern von Bedeutung, als dass damit die Entscheidung zusammenhängen kann, einen besonderen Aufwand zu betreiben und grundlegende Systemanpassungen durchzuführen. Für den Fall einer geringen Nachfrage nach Datenübertragung könnte dagegen einzelfallbezogen und mittels manueller Zusammenstellung und direkter Übertragung von Datensätzen reagiert werden. Gegenwärtig ist allerdings noch nicht absehbar, inwiefern das Interesse an Datenportabilität durch neue Geschäftsmodelle gesteigert wird und wie viele Nutzer im Zuge dessen Ansprüche geltend machen werden.

In Fällen, in denen die Portabilität mehrere heterogene, personenbezogene Datensätze betrifft, welche an unterschiedliche Drittanbieter zu unterschiedlichen Weiterverarbeitungszwecken weitergeleitet werden, kann tendenziell ein **tool-basierter Ansatz** vorteilhaft sein. Dabei müsste zwischen konzernspezifischen, sektorspezifischen und universalistischen Verfahren unterschieden werden:

119 Siehe oben, B. II.
120 Vgl. oben, B. II.

Für die marktdominierenden Konzerne wie Apple, Facebook oder Google kommt eine **konzernspezifische** technische Umsetzung nach dem Vorbild des oben beschriebenen „Takeout"-Services (Kapitel B. II) in Frage. Durch die Bündelung einzelner Online-Dienste und durch die Möglichkeit zum Extrahieren personenbezogener Daten wird den Nutzern in einfacher Weise die Möglichkeit gegeben, die Verwendung und den Transfer der Daten zentral zu verwalten. Am Beispiel von „Takeout" ist insbesondere die Tatsache hervorzuheben, dass dieser Portabilitätsdienst in ein **allgemeines Datenschutz-Dashboard** (hier „MyAccount") eingebunden ist, sodass die Portabilitätsmöglichkeit neben sonstigen Privatsphäreeinstellungen leicht aufzufinden ist. Es bleibt allerdings offen, ob und wie Interoperabilität, Kompatibilität und tatsächliche Einbindungsmöglichkeiten der aus Diensten einzelner „Big-Player" extrahierten Datensätze praktisch gewährleistet sein würden. Eine wirksame und für Verbraucher nutzbare Umsetzung des Rechts auf Datenübertragbarkeit bedarf jedenfalls eines deutlichen Kooperationswillens einzelner marktdominierender Konzerne. Zu bedenken ist dabei, dass im Falle der Einigung auf einen oder mehrere bestimmte Standards durch marktdominierende Konzerne ein „Standard-Monopol" entstehen könnte, das sich negativ auf die Entwicklung und den Wettbewerb alternativer Portabilitätsmodelle auswirken könnte.

Vielversprechend sind **branchenspezifische Umsetzungen** nach dem Vorbild von „Blue-Button"-Services[121] im US-Amerikanischen Gesundheitssektor. Der Vorteil branchenspezifischer Initiativen besteht vor allem darin, dass Datenarten und -formate sowie besondere Datenschutzaspekte etwaigen branchenspezifischen Anforderungen angepasst werden können. Außerdem dürfte die Ausarbeitung und Einigung auf spezifische Tools und Formate innerhalb einzelner Branchensektoren effizienter und zielgerichteter erfolgen als im Falle komplexerer branchenübergreifender Einigungsprozesse. Darüber hinaus bestehen in bestimmten Bereichen bereits vorrangige europarechtliche Portabilitätsvorschriften, wie es beispielsweise bei der Kreditwirtschaft im Hinblick auf Kontoinformationen, den Wechsel des Kreditinstituts und die Aufzeichnungen im Wertpapiergeschäft der Fall ist. Auch die Möglichkeit von Rückgriffen auf bereits bestehende brancheninterne Portabilitätspraktiken (wie bspw. die Übertragung von Stamm- und Belieferungsdaten des Kunden in der Energieversorgung[122]) begünstigt branchenspezifische Angleichungen. Denn in vielen Fällen (insbesondere bei Anbieterwechsel), in denen die Übertragung von Kundendaten für die Verbraucher und Unternehmen sinnvoll ist, gibt es bereits entsprechende Regelungen – z.B. den Nachsendeauftrag, die Rufnummerportierung, den Kontoumzug oder die Übertragung von Schadenfreiheitsrabatten. Darüber hinaus zeigt sich, dass in bestimmten Wirtschaftssektoren der Aufwand zur Umsetzung der Norm verhältnismäßig gering sein kann, wenn von der Regelung nur wenige Daten betroffen sind[123] oder nur mit wenigen Portabilitätsanfragen gerechnet werden muss.

Universelle Lösungsansätze empfehlen sich vor allem für die Anwendung bei sektorübergreifenden und komplementären Services. Bei Diensten, welche sektorübergreifende Datensätze verwenden (z.B. Lokationsdaten, Versicherungsdaten, Gesundheitsdaten, Einkaufsprofile etc.) oder bei den Märkten mit den sich ergänzenden Produkten (z.B. im Bereich Smart-Home) kann die Wertschöpfung gesteigert[124] und der Rahmen für neue innovative Geschäftsmodelle geschaffen werden. Insbesondere können sich dabei universalistische tool-basierte, nutzerzentrierte Lösungsansätze auf der Grundlage von **Personal Information Management Systems (PIMS)** als vielversprechende Umsetzungsstrategien für das Recht auf Datenübertragbarkeit erweisen.[125]

121 Siehe oben, B II.

122 Siehe Abschnitt D., Klemens Gutmann.

123 Vgl. Stellungnahme des Deutschen Datenmarketing Verbands (DDV), siehe Abschnitt D.

124 Vgl. Stellungnahme des Gesamtverbands der Deutschen Versicherungswirtschaft e.V. (GDV), siehe Abschnitt D.

125 Dazu vergleiche auch die Stellungnahme des Europäischen Datenschutzbeauftragten (EDPS) „EDPS: European Data Protection Supervisor, Opinion 9/2016 „EDPS Opinion on Personal Information Management Systems", S. 9.

Durch eine einheitliche zentralisierte Datenkontrolle an einer Stelle („One-Stop-Shop“) wird dem Nutzer auf einfache und verständliche Art und Weise die Möglichkeit gegeben, seine Daten zu verwalten und mit mehreren Dienstanbietern zu teilen.[126] So wären die PIMS dazu besonders geeignet, die personenbezogenen Daten zielgerichtet und effizient zu übertragen und damit mehr Nutzerkontrolle zu ermöglichen.[127] Die Ausarbeitung von PIMS-Ansätzen, wie das bereits beschriebene „Rainbow Button“-Projekt oder „ONECUB-Connect Button“ (Kapitel B. II.), können außerdem eine geeignete Plattform für die Kooperation zwischen unterschiedlichen Anbietern und Branchen bieten.

Fazit

Zusammenfassend lässt sich feststellen, dass für die Umsetzung des Rechts auf Datenübertragbarkeit Ansätze der **„regulierten Selbstregulierung“** genutzt werden sollten, bei denen unter staatlicher Aufsicht ein Rahmen etabliert wird, in dem die Aufsichtsbehörden, NGOs sowie Unternehmen Umsetzungsstrategien und Standards für die Datenportabilität entwickeln. Für eine effektive Ausgestaltung der Datenübertragbarkeit und Herstellung von Rechtskonformität ist vor allem eine **frühzeitige Einbindung** der voraussichtlich besonders intensiv betroffenen Unternehmen und Branchen in formelle Konsultationsprozesse der Aufsichtsbehörden wünschenswert.

Bei der praktischen Gestaltung der Datenportabilität kommen **sowohl branchenspezifische als auch universelle Ansätze** in Betracht. Die Anwendung branchenspezifischer Verfahren empfiehlt sich bei der Verwendung sektorspezifischer Datensätze (z.B. Gesundheits- oder Energieverbrauchsdaten) und in den Fällen, in denen bereits etablierte brancheninterne Portabilitätsverfahren bestehen. Universelle Lösungsansätze auf PIMS-Grundlage empfehlen sich vor allem für die Anwendung bei sektorübergreifenden und komplementären Services, wie im vernetzten Heim und beim vernetzten Fahren. In Fällen, in denen vom Recht auf Datenübertragbarkeit nur wenige, leicht zusammenzutragende und zu übermittelnde Datensätze betroffen sind und/oder mit einer geringen Nachfrage nach Datenübertragung zu rechnen ist, kann allerdings auch auf einzelfallbezogene direkte Übertragung von Datensätzen zurückgegriffen werden.

126 Dazu: Stiftung Datenschutz, „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“, S. 7 ff. URL: https://stiftungdatenschutz.org/themen/pims-studie/

127 European Data Protection Supervisor, Opinion 9/2016 „EDPS Opinion on Personal Information Management Systems”, S. 12-13.

4. Technische Gestaltung[128]

Ausgangslage

Dienstanbieter werden durch das Recht auf Datenportabilität vor die Aufgabe gestellt, bestehende IT-Systeme so anzupassen oder zu ergänzen, dass konkret definierte Datensätze mit personenbezogenen Daten an die betroffenen natürlichen Personen oder an einen von ihnen benannten anderen Dienstanbieter übermittelt werden können. Diese Daten müssen zukünftig in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden.

Die Frage, in welchem Format die Daten zu übermitteln sind, betrifft technische, rechtliche und wirtschaftliche bzw. akzeptanzorientierte Aspekte. Die Anforderungen an die technische Realisierung definiert oder präzisiert der Gesetzgeber nicht. Die Datenschutzgrundverordnung sieht allein vor, dass organisatorische und auch technische Maßnahmen und Verfahren zu schaffen sind, um die Ziele der Vorschriften effektiv umzusetzen. Dabei bleibt das Gesetz technologieneutral. Ein bestimmtes Format oder ein Standard werden nicht vorgegeben. Festgelegt wird vom Wortlaut nur die Verwendung eines „strukturierten, gängigen und maschinenlesbaren“ Formats. Ferner wird zur Entwicklung von interoperablen Formaten aufgefordert (Erwägungsgrund 68), die die Weiterverarbeitung der Daten in anderen Systemen ermöglichen.

Architektur des Datenformats

Die Leitlinie der Artikel-29-Datenschutzgruppe in der ursprünglichen Fassung, nach der möglichst viele Metadaten unter dem bestmöglichen Granularitätslevel bereitzustellen wären, wurde in der korrigierten Fassung dahingehend präzisiert, dass gängige und offene Formate zu verwenden sind, sofern in einer bestimmten Industrie oder einem Kontext kein Format gebräuchlich ist. Beispielhaft werden die Formate XML, JSON und CSV genannt.

Entscheidender als die Auswahl des konkreten Formats ist jedoch zunächst die Architektur bzw. allgemeine Eigenschaft eines „gängigen“ Formats. Es müssen unterschiedliche Ebenen berücksichtigt werden: die strukturelle Interoperabilität (ein gemeinsames Datenmodell), die syntaktische Interoperabilität (eine gemeinsame Syntax) und die semantische Interoperabilität (ein gemeinsames Verständnis der Dateninhalte). Eine Interoperabilität bei unterschiedlichen Formaten lasse sich nur erreichen, wenn diese sinnvoll ineinander übersetzt werden können. Hierzu müssen die beteiligten Formate ausreichend detailliert beschrieben und dokumentiert sein. Im Ergebnis sollten die Daten nach einem nachvollziehbaren Muster bzw. Bauplan in einer Datei angeordnet werden. Die Architektur muss Syntax und Semantik der Daten innerhalb der Datei abbilden. Während syntaktische Informationen festlegen, wie die Daten strukturiert und aufgebaut sind (Metadaten), werden die eigentlichen Inhalte auf der semantischen Ebene einheitlich festgelegt. Aus diesem Aufbau lässt sich ableiten, wie die Datei selbst (Erkennen und Behandeln) und auch wie die Daten in der Datei zu interpretieren sind; eine effiziente Maschinenlesbarkeit der enthaltenen personenbezogenen Daten ist so sichergestellt.[129] Auch eine funktionierende Interoperabilität ist hiermit realisierbar.

128 Das vorliegende Kapitel basiert auf der von der Stiftung Datenschutz in Auftrag gegebenen Expertise von Gunnar Hempel/Karl Schmid, SCRC e.V. Leipzig, Universität Leipzig, Lehrstuhl für Wirtschaftsinformatik, Prof. Dr. Rainer Alt., siehe Kap. D. II.

129 Vgl.: Hempel/Schmid, SCRC e.V. Leipzig, Universität Leipzig, Lehrstuhl für Wirtschaftsinformatik, Prof. Dr. Rainer Alt., siehe Kap. D. II.; Drepper/Schlünder/Buckow, Praktische Umsetzbarkeit der Datenportabilität im Bereich der medizinischen Forschung, siehe Abschnitt D.

Geeignet ist hierbei beispielsweise der XML-basierte Standard für die Strukturierung von personenbezogenen Daten. Mit XML sind unterschiedliche **Granularitätsstufen** ohne Weiteres möglich. Darüber hinaus sind die enthaltenen Informationen im XML-Schema nicht nur maschinenlesbar, sondern können über Standardsoftware von dem Betroffenen selbst gelesen werden. Diese Eigenschaft könnte neben dem Recht auf Datenübertragbarkeit auch die Wahrnehmung der Informationsrechte der betroffenen Person unterstützen.[130]

Die **Mindestvoraussetzung** für Datenportabilität bzw. Interoperabilität ist es, die Daten im einfachsten CSV-Format zu schreiben und eine einfache Beschreibung hinzuzufügen, wie die Daten in der Datei angeordnet sind. Zu beschreiben ist hierbei, an welcher Stelle in der Datei welche Dateninhalte zu finden sind (Name, Vorname, Geburtsdatum etc.) und was ggf. bestimmte Codierungen bedeuten.

Bei der Übertragung via Informationstechnik müssen außerdem ausreichende **Sicherheitsmaßnamen** wie eine Ende-zu-Ende-Verschlüsselung der Daten während des Transports nach dem Stand der Technik gewährleistet werden. Zusätzlich muss in jedem Fall die sichere Identifizierung und Authentifizierung des Betroffenen (Log-in-Verfahren, Double Opt-in) sichergestellt sein.[131] Die Notwendigkeit, die Daten in einer Weise zu verarbeiten, die angemessene Sicherheit gewährleistet, ist unumgänglich und allgemeiner Grundsatz im Datenschutzrecht (u.a. Art. 5 Abs. 1f DSGVO). Davon sind auch die Integrität und Vertraulichkeit der Daten umfasst, die durch geeignete technische und organisatorische Maßnahmen abzusichern sind. In diesem Sinne wird es sinnvoll sein, die betreffenden Daten auch revisionssicher oder signiert zu übermitteln. Dadurch kann im Zweifel nachgewiesen werden, dass der Verantwortliche richtige und unverfälschte Daten exportiert hat. Allgemein besteht ansonsten die Gefahr der Manipulation von Daten im Rahmen der Übermittlung. Um sich hierbei haftungsrechtlich möglichst effektiv abzusichern, sind entsprechende Maßnahmen zu treffen.

Industriestandards

In den Jahren hat sich eine Vielzahl von Industriestandards für den Datenaustausch entwickelt. Einer der bekanntesten Vertreter für spezifischen Datenaustausch ist z.B. **EDIFact.** Über diese Standardkommunikation wird ein großer Teil des Datenaustauschs in Industrie, Dienstleistung und Handel abgewickelt. Standardsysteme wie das ERP von SAP, aber auch weniger verbreitete kommerzielle Anwendungen verfügen über EDIFact-Schnittstellen für Export und Import. Die Implementierung von neuen EDIFact-Schnittstellen erfordert relativ genaue Fachkenntnisse und auch einigen Aufwand. Lesbar im Sinne des Anwenders ist EDIFact kaum. Personenbezogene Daten werden z.B. im Rahmen des Wechsels von Energielieferanten mittels EDIFact ausgetauscht.[132]

130 Ebd.

131 So auch WP 242 Guidelines on the right to data portability. Adopted on 13 December 2016. As last revised and adopted on 5 April 2017. 2017. Article 29 Data Protection Working Party, WP 242, rev.01, http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (Abruf: 2017-07-31)

132 So auch Stellungnahme von Klemens Gutmann, siehe Abschnitt D.

Dasselbe gilt für **DATANORM.** Dieses Format wird zur Übermittlung von Artikelinformationen eingesetzt. DATANORM ist hoch generisch, entsprechend flexibel und bietet ein großes Funktionsspektrum. Aber auch hier gilt, dass dieser Standard für die breiten Anforderungen der Datenportabilität kaum geeignet ist.

In der Medizininformatik hat sich analog der Standard **HL7** durchgesetzt. Aber auch für ihn gelten obige Limitationen im Sinne einer branchenübergreifenden Portabilität.

Die drei Beispiele zeigen, wie sich anwendungs- bzw. branchenspezifisch Austauschstandards entwickelt haben.

Von allgemeinerer Bedeutung ist der **XML** Standard (Extensible Mark-up Language). Die Vorteile des Standards sind:

- Industriestandard mit hoher Verbreitung
- Nutzung durch viele IT-Lösungen, plattformübergreifend, flexibel und einfach erweiterbar
- Grundlage für moderne Übertragungstechniken wie Webservices
- Schnelle Reaktion auf Gesetzesanforderungen möglich
- Standardisierung verhindert individuelle Lösungen
- Auch tief verschachtelte Ebenen lassen sich relativ leicht lesen
- XSLT steht für die Transformation in verschiedene Formate zur Verfügung.

XML hat den Vorteil, dass diese Technik sowohl Daten selbst als auch die Metadaten für die Beschreibung der Daten, für Plausibilitäten und Weiterverarbeitung mitliefern kann; auf diese Weise wird die Datenbeschreibung im Austauschformat direkt mitgeliefert. Darüber hinaus können Daten im XML-Format einfach, z.B. mittels MS-EXCEL oder eines beliebigen Editors, lesbar angezeigt werden. XML eignet sich in Verbindung mit Webservices hervorragend zur Kommunikation zwischen unterschiedlichen Systemen. Natürlich befreit diese Technik nicht von der Festlegung, welche Daten überhaupt übertragen werden – dies gilt für alle Austauschformate.

In jüngerer Zeit kommt immer mehr **JSON** (JavaScript Object Notation) zum Einsatz. Es ist relativ einfach für den Menschen lesbar:

- Einfache, minimalistische Syntax
- Geringes Datenvolumen
- Eignet sich besser für AJAX-Applikationen
- Unterstützung einer Vielzahl von Programmiersprachen
- Weniger geeignet für Dokumente und mediale Daten

Generell stellen sowohl XML als auch JSON offene Schnittstellentechniken dar, die die Anforderung an die Interoperabilität sicherstellen.

Fazit

Die Mindestvoraussetzung für Datenportabilität bzw. Interoperabilität ist es, die Daten im CSV-Format zu schreiben und eine einfache Beschreibung hinzuzufügen, wie die Daten in der Datei angeordnet sind. Zu beschreiben ist hierbei, an welcher Stelle in der Datei welche Dateninhalte zu finden sind (Name, Vorname, Geburtsdatum etc.) und was ggf. bestimmte Codierungen bedeuten. Für umfangreichere Lösungen bieten sich XML oder JSON an. Beide Standards erfüllen die Anforderungen an die Maschinenlesbarkeit sowie Interoperabilität. Sie enthalten die Daten sowie die beschreibenden Metadaten und haben aufgrund ihrer Struktur die entsprechende Tiefe, um auch komplexe Datengerüste abzubilden. Schließlich ist die Notwendigkeit, die Daten zu verschlüsseln, unumgänglich. Davon sind auch die Integrität und Vertraulichkeit der Daten umfasst, die durch geeignete technische und organisatorische Maßnahmen abzusichern sind.

II. Handlungsempfehlungen

1. Zielrichtung der Norm

- Die Umsetzung der Norm sollte im Sinne ihrer ursprünglichen Intention erfolgen – der Stärkung der informationellen Selbstbestimmung der Verbraucher. Dies meint primär Kontrollmöglichkeiten über die Weitergabe personenbezogener Daten.

- Vom Recht auf Datenübertragbarkeit müssen zumindest diejenigen Daten erfasst sein, deren Übertragbarkeit tatsächlich die informationelle Selbstbestimmung fördert und die vom Nutzer entsprechend verwendet werden können. Der Aufwand für die Normumsetzung muss verhältnismäßig sein, auch im Hinblick auf die tatsächliche Wirksamkeit für die Datensouveränität der Verbraucher.

- Die Wirksamkeit der Norm muss einem Praxistest unterzogen werden. Das beinhaltet u.a. verhaltensökonomische Untersuchungen zur tatsächlichen Nutzerbereitschaft, die Datenportabilitätsmöglichkeiten in Anspruch zu nehmen. Die Ergebnisse sollten in die Evaluation der EU-Datenschutzgrundverordnung einfließen.

- Die Einführung des Rechts auf Datenübertragbarkeit sollte von Informationskampagnen über dessen Reichweite und Möglichkeiten begleitet werden (z.B. durch nationale Datenschutzbehörden oder Informationsplattformen).

2. Bestimmung des Anwendungsbereichs

- Bei der Bestimmung des Anwendungsbereichs sollte der Verbrauchernutzen im Vordergrund stehen, um Akzeptanz und Erfolg des neuen Rechts zu erhöhen.

- Die Definition der „bereitgestellten Daten“ sollte sich an Sinn und Zweck der Norm ausrichten.

- Die Aufsichtsbehörden sollten über die Stellungnahme der Artikel-29-Datenschutzgruppe hinaus präzisieren, was „bereitgestellte Daten“ sind, und Beispiele für umfasste Datenkategorien geben.

- Bei der Frage, ob sowohl Bestandsdaten als auch Nutzungsdaten vom Anwendungsbereich erfasst sind, sollte im Einzelfall und dienstbezogen entschieden werden können. Es ist zu prüfen, in welchen Fällen die Übertragung aller „bereitgestellten“ Nutzungsdaten zu einem anderen Anbieter tatsächlich die Kontrollrechte der betroffenen Person stärkt.

- Hinsichtlich des Datenformats und der geforderten Interoperabilität ist das Wettbewerbsrecht zu berücksichtigen. Es ist zu prüfen, inwieweit Kriterien entwickelt werden müssen, um eine europaweit einheitliche Sichtweise sowie ein differenziertes Ergebnis im Hinblick auf Wettbewerbsrecht und Datenschutzrecht zu schaffen. Kartellrechtliche Probleme bei Einigungen zu Verfahren der Datenübertragung sind zu vermeiden. Der Schutzzweck der Norm, nämlich die Erleichterung des Anbieterwechsels, muss zum Tragen kommen.

- Im Hinblick auf Schutzrechte Dritter ist ebenfalls bei Datenverarbeitung durch eine natürliche Person zu ausschließlich persönlichen oder familiären Zwecken zu berücksichtigen, ob personenbezogene Daten zu einem kommerziellen Anbieter übertragen werden oder auf einem eigenen privaten Gerät verarbeitet werden. Hier müssen Verhaltensregeln dahingehend ausgearbeitet werden, inwieweit zukünftig eine weitere Verarbeitung aufgrund berechtigter Interessen oder Zweckänderung durch kommerzielle Anbieter tatsächlich ausgeschlossen ist.

- Es empfiehlt sich die Prüfung, ob ein einheitliches technisches und juristisches Verständnis des Begriffs „Metadaten“ besteht. Dies gilt insbesondere auch, um entscheiden zu können, welche Metadaten aus technischer Sicht für eine erfolgreiche Umsetzung der Datenportabilität sowie der Entwicklung eines Formats erforderlich und aus rechtlicher Sicht zulässig sind.

- Bei der Ausübung des Rechts auf Datenübertragbarkeit sollten die beteiligten Stellen stets Transparenz herstellen. Die jeweils betroffene Person darf nicht den Überblick über die Datenverantwortlichen und die ihr zustehenden Löschungsansprüche verlieren. Ihr müssen alle Informationen, die sich auf die Verarbeitung durch den alten und neuen Verantwortlichen beziehen, bekannt sein.

- Hinsichtlich der Forderung „soweit technisch machbar“ muss entschieden werden, ob objektive Kriterien entwickelt werden können oder ob die individuelle Leistungsfähigkeit des jeweiligen Datenverantwortlichen (subjektiver Maßstab) zugrunde gelegt wird.

- Auch bei der Auslegung von Art. 20 DSGVO sowie im Rahmen der Ausarbeitung der Verhaltensregeln gemäß Art. 40 DSGVO ist auf eine europäische Harmonisierung und konsistente Interpretation hinzuwirken.

3. Umsetzungsstrategien

- Es sollten Ansätze einer „regulierten Selbstregulierung“ entwickelt werden, bei denen unter staatlicher Aufsicht ein Rahmen etabliert wird, in dem die Aufsichtsbehörden, NGOs sowie Unternehmen Umsetzungsstrategien und Standards für die Datenportabilität entwickeln.

- Für eine effektive Ausgestaltung der Datenübertragbarkeit und Herstellung von Rechtskonformität sollten besonders betroffene Unternehmen und Branchen in formelle Konsultationsprozesse der Aufsichtsbehörden eingebunden werden.

- Ein branchenspezifisches Vorgehen empfiehlt sich bei Übertragung sektorspezifischer Datensätze innerhalb einer Kategorie von verantwortlichen Stellen und in Fällen, in denen bereits etablierte brancheninterne Portabilitätsverfahren bestehen.

- Lösungsansätze auf Grundlage von Personal Information Management Systems (PIMS) erscheinen bei sektorübergreifenden Sachverhalten vielversprechend.

- In Fällen, in denen voraussichtlich mit einer geringen Nachfrage nach Datenübertragung zu rechnen ist, könnte auf einzelfallbezogene direkte Übertragung von Datensätzen zurückgegriffen werden.

- Zur Schaffung von Orientierung sollte auf die Entwicklung von Verhaltensregeln zur Portabilitätspraxis hingewirkt werden (Art. 40 DSGVO).

4. Technische Gestaltung

- Mindestvoraussetzung für Datenportabilität und Interoperabilität sollte die Nutzung des CSV-Format sein. Es ist eine einfache Beschreibung hinzuzufügen, wie die Daten in der Datei angeordnet sind.

- Für umfangreichere Lösungen sollten die Formate XML oder JSON genutzt werden. Diese Formate ermöglichen feinere Granularitätsstufen, enthalten sowohl Inhaltsdaten als auch beschreibende Metadaten und haben aufgrund ihrer Struktur ausreichende Tiefe, um auch komplexe Datengerüste abbilden zu können. Die enthaltenen Informationen sind nicht nur maschinenlesbar, sondern können über Standardsoftware von dem Betroffenen selbst gelesen werden, was zugleich die Wahrnehmung der Informationsrechte der Nutzer unterstützt.

- Die Datenschutzbehörden sollten definieren, welche konkreten Anforderungen an die Authentifizierung gestellt werden, damit Rechtsunsicherheiten für die Verantwortlichen und Risiken für die Betroffenen vermieden werden.

- Sowohl bei Einzelfalllösungen als auch bei branchenspezifischen oder branchenübergreifenden und universellen Ansätzen muss sichergestellt werden, dass die technischen Lösungsansätze durch offene Schnittstellen grundsätzlich untereinander interoperabel sind.

- Im Hinblick auf die effektive Weiterverwendung der portierten Daten sollte das PDF-Format im Bereich der Datenübertragbarkeit regelmäßig nicht zum Einsatz kommen, auch wenn es im Rahmen des Auskunftsrechts mit Blick auf die transparente Information als elektronisches Format ausreichend ist.

Practical Implementation of the Right to Data Portability

Legal, Technical and Consumer-Related Implications

Dr. Nikolai Horn, Prof. Dr. Anne Riechert,
Stiftung Datenschutz

Practical Implementation of the Right to Data Portability

Legal, Technical and Consumer-Related Implications

Executive Summary

With the reform of European data protection law, a legal instrument will be introduced which creates new practical requirements for the processing of personal data. Article 20 of the European General Data Protection Regulation gives every individual the "right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format".

This means that in the future, users will have the right to transfer the personal data concerning them to another organisation without being prevented to do so by the first organisation. The aim of this new data protection instrument is to prevent monopolies and to "free" users from large networks. The legislative authorities of this reform hope that this possibility of transfer for their "own" data will lower the barriers for consumers to change their providers of digital services and will give them better means of control over their personal data.

However, it has not been specified yet how this theoretically plausible mechanism can be implemented in practice. Until now, neither business enterprises nor regulatory authorities have any experience because there are no previous regulations or existing development of the law by judges on this topic, as is for example the case with the "right to be forgotten" which was developed by the European Court of Justice and which is referred to in this regulation.

Because of this, Stiftung Datenschutz has examined legal, technical and consumer-related implications of the new legislation in this study and gives recommendations on the practical utilisation of this new instrument. First of all, we will explain the subject matter of Art. 20 GDPR and illustrate essential problem areas in the implementation of the regulation. After this, we will present national and international solutions suggested for data portability and assess the submissions which reached us after our Call for Papers[1] as well as the recommendations of external experts. Finally, the study gives recommendations with respect to the objectives of the regulation, the determination of its scope of application as well as to possible implementation strategies and its technical realisation.

With respect to the objectives of the regulation, it is illustrated how the right to data portability can basically give the users better means of control over their personal data. However, if the interpretation of the regulation is too broad, data protection risks could even increase and it could result in a disproportionately high amount of work for the data controllers regarding the categorisation and extraction of data sets. Therefore, the interpretation of Art. 20 GDPR should only include such data where portability actually serves the protection of data privacy ("informational self-determination"). The efforts and expenses required for the implementation of the regulation have to be proportionate, also with respect to its actual benefits for the consumers.

1 https://stiftungdatenschutz.org/themen/projekt-datenportabilitaet.

Regarding the issue of the legal scope of application, we suggest that the regulatory authorities should precisely specify and narrow down the meaning of the concept “data provided” in addition to the statement of the Article 29 Working Party. Concerning the issue whether the scope of application includes contract as well as user data, it should be decided for each individual case and for each specific service whether this would actually improve the possibilities of control for the person concerned. In addition, it is very important to guarantee sufficient transparency with respect to data processing by the previous and the new controller and to distinguish this clearly from the right of access to the data. With respect to the data format and the requested interoperability, issues of competition law have to be considered, as well. All decisions must be based on the protective purpose of the regulation, which is intended to make a switch to another provider easier. To support an orientation, it is important to achieve a European harmonisation for the country-specific interpretation of Art. 20 GDPR.

In our analysis of suitable implementation strategies for the right to data portability, we illustrate that a framework can especially be established with approaches of “regulated self-regulation”, in which regulatory authorities, NGOs, and businesses develop implementation strategies and standards for data portability. For an effective definition and arrangement of data portability and realisation of legal compliance, companies and industries which will presumably be particularly affected should be involved in formal consultation processes of the regulatory authorities from an early stage. For the practical implementation of data portability, industry-specific as well as universal approaches to solutions can be considered depending on the respective field of application and context of processing. For cross-sectoral approaches, Personal Information Management Systems (PIMS) could be used. In case there is only a low demand for data transfers acc. to Art. 20 GDPR, an individual, direct transfer of data sets could be applied.

Regarding the issue of the technical definition and arrangement of data portability and the requirements for a suitable compatible and interoperable data format, we will explain that the minimum requirement is to write the data into a basic CSV format and to add a simple description of how the data is arranged in the file. For more complex solutions, XML or JSON would be suitable. Those two standards fulfil the requirements of machine readability and interoperability. They contain the data as well as descriptive metadata and have sufficient depth due to their structure so that they are able to represent even complex data structures. In addition, the contained information can be read by the concerned persons themselves using standard software, which also supports the exercise of information rights by the users. In any case, it will be necessary to encrypt the transferred data. The technical implementation of data portability will also have to ensure that different solutions are generally interoperable due to open interfaces.

Index

A. Subject Matter of the Provisions in Art. 20 GDPR

I. The Right to Data Portability

1. Objective of the Regulation

In late May 2018, the citizens of the EU will be given a new legal instrument – the right to transfer their personal data between different service providers (Art. 20 GDPR). While the existing data protection law only contained a disclosure obligation for the responsible bodies in this regard, the new regulations shall make it possible for a person "to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format" or to have the data directly transferred to another data controller. The idea behind this regulation is to allow the users to freely choose between competing internet services so that they are not "locked in" by their previously selected service (so-called "lock-in effect"). The aim of the regulation is that such personal data which is made available to a controller within the scope of a contract or otherwise with the consent of the user, can be transferred to another controller upon the user's request and without any fees or obstacles. This is mainly meant to remove any asymmetries which prevent the customers from switching to another service provider. The aim is to loosen customer retention by means of proprietary processing formats – for example inside the "Apple ecosystem" –[2] and to allow the users more freedom of choice in their decision between different service providers in terms of "data sovereignty". The right to data portability is meant to allow for a transfer of personal data as it is for example already the case for mail forwarding, porting of mobile phone numbers, bank account changes or transfer of the no-claims bonus when switching car insurances. This means that in the future, situations would be possible in which for example a lessee of a car could request the information about his driving behaviour to be transferred to another lessor in order to benefit from better conditions.[3]

2. Contents of the Regulation

The right to data portability shall give users the possibility to transfer their personal data, which they have provided to one institution, to another organisation without being prevented to do so by the first data recipient. In detail, there are the following essential requirements for the right to data portability according to Art. 20 GDPR:

- The data has to be personal data in terms of Art. 4, para. 1 GDPR and the right is limited to individual persons.

- Data processing is based on the user's consent or a contract with the user (Art. 20, para. 1a GDPR).

2 *Sperlich, T., Das Recht auf Datenübertragbarkeit, DuD 6/2017, p. 377.*

3 *Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, p. 73.*

- The user has "provided" the concerned data to the controller, i.e. such data over which the person has control and which they access themselves: The regulation does not apply to data which has been generated by the data recipient by means of data processing.

- The processing is carried out by means of automated processes (Art. 20, para. 1b GDPR).

With respect to technical feasibility, the regulation emphasises that the transfer of data has to take place in a "structured, commonly used and machine-readable format" (Art. 20, para. 1 GDPR), and that "data controllers should be encouraged to develop interoperable formats that enable data portability" (Recital 68). In addition, the person concerned can demand that the transfer takes place directly from one controller to another "where technically feasible" (Art. 20, para. 2 GDPR).

The right to data portability shall also not affect the right to erasure according to Art. 17 GDPR (Art. 20, para. 3, sentence 1 GDPR; Recital 68). Therefore, the right to data portability is no direct right to erasure and hence does not result in a separate duty to delete data. This means that there is basically a right to keep a "copy"[4] of the personal data provided. Furthermore, the request for a data transfer by the user does not constitute an implied termination of an existing contract.[5]

Art. 20, paragraph 3, sentence 2 GDPR also clarifies that the right to data portability does not apply to any processing "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". This means, if the personal data is processed for the fulfilment of public services (such as archiving, statistic or research purposes), this right cannot be exercised with respect to the responsible controller.[6] In addition, the right to data portability does not apply to personal data of third parties (Art. 20, para. 4 GDPR) because in this case, the informational self-determination of other persons is concerned.

According to Art. 13, para. 2b and Art. 14, para. 2c GDPR, respectively, the controller is obliged to inform about the right to data portability. According to Art. 13, para. 2b GDPR, the information must be given at the time of the data collection.

If the person concerned exercises their right to data portability, this does not affect any applicable storage periods. Their right of access to personal data (Art. 15 GDPR) shall remain unaffected, as well. This right refers to any personal data even if the person concerned did not provide them in terms of Art. 20 GDPR. This way the right to data portability and the right of access according to Art. 15 GDPR can complement one another.

If the person concerned asserts their right to withdraw their consent according to Art. 7, para. 3 GDPR or their right to object according to Art. 21 GDPR, they can exercise their right to data portability as long as the controller processes the data and provided they are not at the same time subject to a request for erasure. According to the recommendations of the Article 29 Working Party, the persons concerned should therefore be expressly advised of their right to data portability before they terminate an account.

4 Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, p. 74.

5 cf. Hennemann, Datenportabilität, PinG 01.17, p. 7.

6 Recital 68 GDPR.

3. Expectations and Reactions[7]

Positive Expectations

There have been different reactions to the introduction of the right to data portability. Supporters of the new regulation consider Art. 20 GDPR a catalyst for a competition for data protection-friendly technologies.[8] For example, the new right was evaluated as positive in the green paper "Digitale Plattformen" ("Digital Platforms") by the Federal Ministry of Economics and Technology (BMWi) because "the competition in innovation as well as the competition on conditions are promoted" when a change of platforms is facilitated[9] (however, this would be subject to a practicable implementation[10]). The Federation of German Consumer Organisations also expressly appreciated the introduction of this regulation in their statement regarding the BMWi green paper because it would – subject to an efficient realisation – create an effective means to support data sovereignty in the digital world as well as the competition between the platforms.[11] The first version of the guidelines by the Article 29 Working Party from 13 December 2016 emphasised that the regulation aimed for the promotion of new business models with more data control.[12] The newly published report by the board of experts for consumer affairs (Sachverständigenrat für Verbraucherfragen) also confirms the high relevance of the right to data portability for the exercise of digital sovereignty. The report even called for considering the right to data portability a right of termination.[13]

Not only in Europe, but also in the USA, the topic of data portability is considered very important. For example, many stakeholders at the public consultation of the White House Office of Science and Technology Policy (OSTP) listed data portability as an important instrument for promoting competition and improving the users' control.[14]

The positive expectations regarding the effects of data portability have also been emphasised by the developers of Personal Information Management Services (PIMS): According to them, data portability and the reuse of already existing data sets allow for the expansion and increased efficiency of personalised online services, while at the same time, the possibilities of data control for the users are improved.[15]

7 Individual statements as well as statements regarding the guidelines of the Article 29 Working Party are illustrated in more detail in Section B.

8 Albrecht, CR 2016, 88, 93.

9 Grünbuch Digitale Plattformen. Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe, p. 61. URL: http://www.de.digital/DIGITAL/Redaktion/DE/Publikation/gruenbuch.pdf?__blob=publicationFile&v=10.

10 Weissbuch Digitale Plattformen. Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe, p. 76 f. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.pdf?__blob=publicationFile&v=22

11 Grünbuch Digitale Plattformen, Stellungnahme des Verbraucherzentrale Bundesverbands, dated 26 September 2016, p. 18.

12 Article 29 Data Protection Working Party, Guidelines on the right to data portability, 13 December 2016, p. 5.

13 Sachverständigenrat für Verbraucherfragen, Digitale Souveränität, June 2017, p. 26.

14 White House Office of Science and Technology Policy. Request for Information Regarding Data Portability. 10/01/2017. URL: https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/OSTP-Data%20Portability-RFI-Responses_for_humans.pdf.; Macgillivray, A., Summary of Comments Received Regarding Data Portability, 10/01/2017. URL: https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability.

15 cf. Statement by ONECUB, see annex.

Critical Reactions

There are also a lot of sceptical opinions regarding the new regulation. As the right is based on competition law efforts to prevent "lock-in effects"[16], some are questioning whether it can be smoothly integrated in the system of rights of affected persons as an instrument of data protection law.[17] In the opinion of the Federal Council of Germany, the right to data portability "has the objective of allowing the persons concerned to reuse their data in order to support competition rather than to protect their privacy"[18]. An analysis by the German Economics Institute in Cologne (Institut der Deutschen Wirtschaft Köln) for example illustrates that while data portability might be supporting the data sovereignty of the individual, it could in certain cases prove detrimental to the competition of start-ups and smaller businesses.[19] Some observers think that the hopes of the legislator that an increased self-determination of the persons concerned over their data will result in an easier switch to other service providers and thus break down market monopolies and "network effects" are not sufficiently justified.[20] In addition, it is criticised that the original aim of the regulation, i.e. avoiding "lock-in effects" in social networks, is only realised in Art. 20 GDPR to a limited extent, because this would mainly affect the rights of third parties (for example "friends" on Facebook).[21]

In addition, it is criticised that the scope of application of Art. 20 GDPR would also include industries where the previously mentioned "lock-in effects" are not even an issue. Although the regulation would be too "far-reaching" for these business models, it could nevertheless cause problems due to its implementation being required without exception.[22] Some parties also expressed concerns that the implementation of the regulation could involve high costs and risks (in particular for SME) while at the same time being of little value for the users.

Another point of criticism is that the requirements regarding technical feasibility of data portability were too vague. This refers on one hand to the legal uncertainty concerning the wording "where technically feasible", because it would be difficult to distinguish between a lack of practicability and unjustified obstacles in individual cases.[23] On the other hand, the question is what could be considered a "commonly used format" and how interoperability between different formats which are "commonly used" but not interoperable[24] should be guaranteed.[25]

16 *Herbst, in Kühling/Buchner, DS-GVO, Art. 20, marginal 4; Hennemann, Datenportabilität, PinG 01.17, p. 6.*

17 *Sperlich, T., Das Recht auf Datenübertragbarkeit, DuD 6/2017, p. 377; Moos, Datenportabilität – Eine Gefahr für daten-getriebene Unternehmen?, eu-datareg as of 2/3/2016, available under: http://eudatareg.com/datenschutz-im-unternehmen/datenportabilitaet-eine-gefahr-fuer-daten-getriebene-unternehmen/; Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, p. 74. BITKOM, Statement concerning the right to data portability acc. to Art. 20 General Data Protection Regulation, 14/03/2017. p. 4.*

18 *Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, 21 December 2016; www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf*

19 *https://policyreview.info/articles/analysis/data-portability-among-online-platforms; https://www.iwkoeln.de/studien/iw-kurzberichte/beitrag/barbara-engels-nicht-immer-gut-datenportabilitaet-zwischen-online-plattformen-300089.*

20 *Kühling/Martini, EuZW 2016, 451; Hennemann, Datenportabilität, PinG 01.17, p. 8.*

21 *Hennemann, Datenportabilität, PinG 01.17, p. 8; Jülicher, Röttgen, v. Schönfeld, Das Recht auf Datenübertragbarkeit, ZD 8/2016, p. 359, 361.*

22 *Moos, Datenportabilität – Eine Gefahr für daten-getriebene Unternehmen?, eu-datareg as of 2/3/2016, available under: http://eudatareg.com/datenschutz-im-unternehmen/datenportabilitaet-eine-gefahr-fuer-daten-getriebene-unternehmen/; Jülicher, Röttgen, v. Schönfeld, Das Recht auf Datenübertragbarkeit, ZD 8/2016, p. 361.*

23 *Moos, Datenportabilität – Eine Gefahr für daten-getriebene Unternehmen?, eu-datareg as of 2/3/2016, available under: http://eudatareg.com/datenschutz-im-unternehmen/datenportabilitaet-eine-gefahr-fuer-daten-getriebene-unternehmen/*

24 *Hennemann, Datenportabilität, PinG 01.17, p. 7.*

25 *Schätzle, Ein Recht auf Fahrzeugdaten, PinG 02.16, p. 74.*

II. Recommendations by the Article 29 Working Party

1. Summary of the Recommendations

On 13 December 2016, the Article 29 Working Party adopted recommendations concerning the right to data portability and then passed a revised version on 5 April 2017.

In the opinion of the Article 29 Working Party, the right to data portability essentially includes the possibility for persons concerned to easily keep, control and reuse "their" data for their own purposes, even when they switch between different service providers. According to the recommendations of the Article 29 Working Party, this shall not only include the personal data of the persons concerned which are automatically processed based on their consent or a contract and have been actively provided by the data subjects (such as email address, user name chosen by themselves, age). The scope shall rather also include data which is collected based on the user activities of a service or a device (e.g. protocols of user activity or use of websites). However, the Article 29 Working Party underlined that the right to data portability does not apply to user profiles because these are usually not provided by the persons concerned but generated by the data controller. With respect to personal data of third parties, which are affected by the data transfer, it is made clear that the recipient of the data is only allowed to process them if there is a valid legal basis for this.

According to the recommendations of the Article 29 Working Party, data subjects should generally be able to exercise the right to data portability without any obstacles and irrespective of the system, with the possibility to copy data, save it to their own private devices or transfer it from one IT environment to the environment of another data controller. As a consequence, data controllers shall establish appropriate processes which enable the persons concerned to request a data transfer and at the same time ensure their authentication. The subsequent data transfer should either be carried out with a direct transfer of the entire data set or by means of an automatic tool which allows for filtering out the relevant data. In areas in which there are no commonly used formats, open formats should be used and be made available with as much metadata as possible at the highest level of granularity. It is pointed out that a format should be chosen which maintains all of the metadata that is relevant for an effective reuse of the data. In this context, the data controller should consider whether the chosen format could prevent the person concerned from reusing their data (for example a simple PDF from the inbox of an email account).

Apart from that, the Article 29 Working Party does not focus on one specific data format but rather on an interoperable format; they do not require the systems of the data controllers to be compatible. They consider the demand of the General Data Protection Regulation, to make data available in a structured, commonly used and machine-readable format, the minimum requirement for the realisation of interoperability and urged industry and commercial associations to cooperate in order to develop interoperable standards and formats.

With regard to time limits, the Article 29 Working Party recommends that the persons concerned shall be able to exercise their right to data portability as longs as the data controller is processing the data. Depending on the individual case, the data controller shall be given up to three months time from the receipt of a request to provide information about the measures taken. Although Art. 12, paragraph 3 General Data Protection Regulation provides for a period of one month, this period could however be extended for complex circumstances if the data controller notifies the person concerned about the delay and its reasons within one month.

In addition, the Article 29 Working Party pointed out that the services of the data controller do not automatically end with the data transfer but that the persons concerned could continue to use the respective service. This would not entail the deletion of the data, nor did the exercise of the right affect the storage period. Moreover, the controller is not allowed to delay or deny the exercise of other rights (such as rights of access or withdrawal) if the persons concerned request a transfer of data.

Within the scope of the information requirements according to Art. 13, para. 2b and Art. 14, para. 2c GDPR, the data controller shall expressly inform about the different types of data to which a right to data portability or a right of access (Art. 15 and Recital 63) applies. The Article 29 Working Party on Data Protection recommends that information about the right to data portability shall always factored in by the data controller before the persons concerned close any existing account. To avoid any doubt, the committee also explained in its recommendations that the data controller would not continue to be responsible for complying with the principles of the General Data Protection Regulation with respect to the transferred data after they have carried out the request for data portability. However, they had first to make sure that only such data is transferred which the person concerned actually wanted to transfer. Subsequently, the recipient of the data had to fulfil the duties according to Art. 5 GDPR as the new data controller (fair and transparent data processing, purpose limitation, data minimisation, accuracy, integrity and confidentiality, storage limitation and accountability). The previous controller shall also make sure that only such data is made available which is relevant for the new data processing activities by the data recipient and that the persons concerned are comprehensively informed about this procedure. Finally, the data recipient has to inform about the purposes of the new data processing activities before a data transfer is requested. In this context, the Article 29 Working Party used the wording “clearly and directly” as well as “state”.[26] The question is, whether in the future these terms will be consistently interpreted in all member states of the European Union or translated with the same basic meaning.

26 “Therefore, the ”new” receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14.”

2. Comparison of the Versions from December 2016 and April 2017

Although the above summary of the revised version from 5 April 2017 still mentions the stimulation of competition between the data controllers, this general issue has been removed from the recommendations of the Article 29 Working Party. Now, it is emphasised that the main objective of data portability is to improve the control rights of the persons concerned over their personal data. Thus, the focus is clearly shifted to data protection aspects.[27]

The Article 29 Working Party justified their decision that data controllers were not responsible for the further processing as well as the compliance with the regulation by the recipient after a data transfer specifying that the previous controllers did not choose the recipient themselves (p. 5 and p. 6/new).

With respect to the exercise of the rights of the persons affected, they added that a contract for commissioned data processing (Art. 28 GDPR) had to include the obligation of the processor to support the controller in carrying out data transfers with suitable technical and organisational measures. Therefore, both of them had to jointly adopt processes for carrying out data portability requests. In case of their joint responsibility, the individual tasks should be clearly assigned with respect to the processing of the data portability request (p. 6/new).
Moreover, they pointed out that any bodies who are to receive data following a data portability request of a person concerned would not be obligated to accept this request. Hence, there would be no obligation to process data (p. 7/new).

Regarding the application of the principles of data portability, the revised version emphasises that these principles are not applied if it is clear that the person concerned does not wish to exercise this right but another specific right to data transmission. As an example, it mentions EU directive 2015/2366 of the European Parliament and the Council regarding payment services in the internal market (PSD2) (p. 7/8 new).

The new version was also supplemented by advice on the handling of employee data. The Article 29 Working Party pointed out that often, application cases had to be assessed individually. As examples for a right to data portability, they for instance listed payment transactions or internal personnel recruitment (p. 8/9 new).

The recommendations of the Article 29 Working Party) also made it clear that data portability does not apply to the B2B area (p. 8/new).

Furthermore, the obligations of the data recipient and thus the new data controller according to Art. 5 GDPR were emphasised by expressly listing them (p. 10/new: “fair and transparent processing, purpose limitation, data minimisation, accuracy, integrity and confidentiality, storage limitation and accountability”).

27 For example, statements such as the following were deleted: “Indeed, the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services (by making it easier for individuals to switch between different providers). It also enables the creation of new services in the context of the digital single market strategy” or “This right aims to foster innovation in data uses and to promote new business models linked to more data sharing under the data subject’s control.”

In addition, the Article 29 Working Party specified which data shall be included by data portability. In detail, they listed protocols of user activities, chronicles of website usage or search requests (p. 10/new). As an explanation, they added that the ability to enquire about their user activities would give the person concerned knowledge about the protection of their privacy and would therefore enable them to choose which data they want to provide for a similar service.

Any disadvantages for third parties involved in the transfer process had to be avoided. As an example, the Article 29 Working Party pointed out that no user profiles of third parties shall be accumulated without their knowledge or consent, nor shall information about them be queried or specific profiles be created. The Article 29 Working Party carefully expressed the opinion that such data processing might be unlawful and unfair ("is likely to be..."). This means that there is still a need for interpretation in this regard (p. 12/new).

With respect to the information to be provided about the right to data portability, the revised version by the Article 29 Working Party now differentiates more clearly between the provisions of Art. 13, para. 2b GDPR (if data was collected from the person concerned) and Art. 14, para. 2c GDPR (if data was not collected from the person concerned). For the latter, it is clarified that the information has to be provided at the latest within one month after receipt of the data. In contrast to the original version from December 2016, the Article 29 Working Party now recommends as "leading practice" (previously "best practice") that the persons concerned should be provided with data and not that the recipients of the data shall provide information as the new controllers.[28] In general, it is emphasised that the provision of information supports the procedure of fair data processing (p. 13/new).

In the revised version, a paragraph regarding the authentication of the user was added which again emphasises that the corresponding processes were often already available and that for instance the respective log-in data and password could be sufficient for the identification of the person concerned. At the same time, it is pointed out that the data controller's possibility to request additional information in order to determine the identity of the person concerned should not result in a collection of personal data.

In its revised version, the committee recommends two alternatives for data portability. While in the original version, the section "Data Portability Tools" referred to different implementation possibilities, for example the direct download, as well as to the application programming interface (API), the revised version now expressly indicates two different ways of data transmission which are also free of charge: The direct transfer of the entire data set or an automatic tool which allows for an extraction of relevant data. The decision between these alternatives shall be made based on the individual case. The Article 29 Working Party explained that the second alternative could be more suitable for extensive and complex data sets (p. 16/new).

The provision of the original version that as much metadata as possible shall be made available at the highest level of granularity was clarified in the revised version indicating that commonly used and open formats shall be used, unless another format was customary in a certain industry or a certain context. As examples, the formats XML, JSON, CSV were listed (p. 18/new).

With respect to the security of the data transfer, it was added that any risks should be minimised by

28 05/04/2017: "...as leading practice for "receiving" data controllers, the WP29 recommends that data subjects are provided with complete information about the nature of personal data which are relevant for the performance of their services".
13/12/2016: "...as a best practice for "receiving" data controllers, the WP29 recommends that they provide data subjects with complete information about the nature of personal data which are relevant for the performance of their services."

using additional authentication information, such as a secret answer to a specific question or a one-off password (p. 19/new).

3. Effects of the Changes

The changes in the revised version from early 2017 are mostly of a clarifying and explanatory nature, but do not fundamentally change the basic meaning of the original text. For example, some reasons were added which support or substantiate the original statements. This applies for instance to statements regarding accountability, amendments to Art. 5 GDPR by listing the specific duties this includes, and additions to the authentication measures or with respect to information duties.

In detail, the following changes are important:

The Article 29 Working Party put a stronger focus on the protection of the right of data subjects to determine the use of their private data as the purpose of the right to data portability. Any statements concerning the stimulation of competition were removed.

In addition, the revised version contains a recommendation for two possible alternatives for the implementation of data portability.

One clarification concerns the differentiation of the right to data portability from other legal provisions in the individual member states. In this regard, clear criteria should be developed in the future in order to determine to what extent the requirements of the right to data portability have to be fulfilled or will not be applied, for instance within the scope of the PSD2 directive, which the Article 29 Working Party mentions as an example.

This applies to employee data, as well, which are mentioned for the first time in the revised version. In this case, too, there are still no clear criteria in which constellations the right to data portability can be exercised.

The new version also clearly specifies that processors are obligated to support the controller in the realisation of data portability by means of suitable technical and organisational measures and that this obligation must be stipulated in a contract.

With regard to the information duties of the data recipient as the new controller, it is questionable whether the modification of the wording from “best practice” to “leading practice” actually entails any qualitative changes. The same applies to the grammatical rewording of an active obligation into an impersonal passive construction.[29] Based on the wording in itself, the latter is however relevant because now, the recipient of the data as the new controller is no longer required to provide the information immediately.

29 See above: 13/12/2016: “…as a best practice for “receiving” data controllers, the WP29 recommends that they provide data subjects with complete information about the nature of personal data which are relevant for the performance of their services.” 05/04/2017: “…as leading practice for “receiving” data controllers, the WP29 recommends that data subjects are provided with complete information about the nature of personal data which are relevant for the performance of their services“ (p. 13 of the recommendations).

However, it has to be taken into account in this context that elsewhere in the text, the data recipient is obligated to inform clearly and immediately about the purpose of the new data processing (p. 7/new). [30]

4. Statements Regarding the Recommendations[31]

Most of the reactions came after the first version of the guidelines by the Article 29 Working Party from 13 December 2016 was published, also because the stakeholders had been invited during the public consultation to explain their point of view with regard to the interpretation and implementation of the new regulation. After this invitation, more than 90 statements were submitted (not all of them being publicly available).

Many stakeholders expressed concerns due to the large number of strict requirements for the data processor, while at the same time, no clear instructions were given how these requirements should be handled. One of the central points of criticism of the statements referred to the interpretation of the term "provide" because the GDPR does not give a legal definition for it. The critics claimed that it was therefore unclear whether it only included data which is relevant for the functionality of the service (and thus for a possible transmission) or if it also included traffic data such as search history, location data, etc.[32] Several stakeholders requested a detailed clarification of what exactly was meant with personal data "provided" by a person in contrast to "inferred"/"derived" data in the context of the regulation.

They also said it should be clarified that the right to data portability did not apply to sensitive company data if this would disclose trade secrets of the company and might be made available to competitors. There was also some uncertainty with respect to data which was collected within the scope of a business relationship – such as surfing behaviour of employees at their place of work, business mail traffic, video surveillance material, etc.[33] In addition, they asked for a clear specification that the regulation would only apply to such data which actually contributes to the so-called informational self-determination of the user. [34]

30 See above: "Therefore, the "new" receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14." (p. 7 of the recommendations).

31 The individual statements will be discussed in detail in Section B.

32 cf. BITKOM. Position Paper. Bitkom views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242), 31/01/2017, p. 2; https://www.nautadutilh.com/en/information-centre/news/2017/1/gdpr-series-part-4-the-right-to-data-portability-including-article-29-working-party-guidelines/; Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", p. 7.

33 cf. Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", p. 7.

34 cf. Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", p. 1-2.

With respect to the technical implementation, the most important area for further discussion were the issues of standardisation and compatibility of formats as well as the issue of ensuring the interoperability of data sets.[35]

Here, a clear differentiation between compatibility and interoperability would be welcome.[36] In this context, the stakeholders also asked for a better clarification of the concept "structured, commonly used and machine-readable format".

In conclusion, it can be noted that the provisions of Art. 20 GDPR have raised many questions, mainly with regard to their scope of application. It seems that the coordination between different stakeholders from the economy, data protection authorities and the EU commission will have to be improved and enhanced. The most important aspects will be problem-solving approaches from the economy as well as a cross-sectoral discourse between stakeholders from different industries.

III. Issues Needing Clarification

The new data protection instrument of portability has been developed to give the users better control over their personal data. However, it has not been specified yet how this theoretically plausible portability can be implemented in practice. With respect to practical implementation, the following issues will have to be resolved:

a) Objectives of the Regulation

- Is the new regulation practically suitable to actually improve the protection of data privacy ("informational self-determination") for consumers?
- Will the regulation really be able to break down network and "lock-in" effects?
- Will it result in a locational advantage for data protection in Europe or will this in the worst case only remain regulatory wishful thinking?
- Which advantages and disadvantages will the new regulation have for users and data processing companies?
- What does the regulation entail for industries and companies, where "lock-in effects" are not an issue?

35 cf. https://medium.com/mydata/comments-on-data-portability-guidelines-2102d447f73b; https://www.nautadutilh.com/en/information-centre/news/2017/1/gdpr-series-part-4-the-right-to-data-portability-including-article-29-working-party-guidelines/; BITKOM. Position Paper. Bitkom views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242), 31/01/2017, p. 3. https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwifko_95uLUAhUCmrQKHSsQAmcQFggrMAA&url=https%3A%2F%2Fetno.eu%2Fdatas%2Fpositions-papers%2F2017%2F170131%2520ETNO_Data%2520Portability_Memo%2F170131%2520ETNO_D ata%2520Portability_Memo.pdf&usg=AFQjCNHC5Cwe6fHkpMMcIYJw5Duqoy7IXw&cad=rja.

36 cf. Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", p. 12.
cf. Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", p. 12.

- Do we need clearer specifications from the legislator or other accompanying measures in order to ensure the effectiveness of the regulation and its added value for the informational self-determination of the consumer?

b) Determination of the Scope of Application

- How narrowly or broadly should the aspect of the "provision of data" in terms of Art. 20, paragraph 1 GDPR be interpreted? Can and should the types of data affected by the right to data portability be categorised?

- In which cases would it be justified to deny a transmission of data (trade secrets)?

- How should cases where data transmission is practically impossible be distinguished from cases of illegitimate hindrance with respect to the provision "where technically feasible"?

- Should an obligation to enable interoperability and compatibility be required? Where could this requirement be incorporated?

- Is it helpful to limit the aspect of provision to the respective service and thus to data which is required for the usage of a similar service?

- Should the aspect of provision be limited further and only include data which is necessary for a planned switch to another service provider?

c) Implementation Strategies

- Which strategies for the structural implementation of the right to data portability would be appropriate for individual enterprises and groups of companies? Which forms of cooperation would be helpful (associations in terms of Art. 40, para. 2 GDPR, alliances/groupings, consortia)?

- To what extent would a platform-independent/cross-sectoral solution be possible? Would sector-specific approaches be more appropriate?

- Which special requirements could emerge for the data protection management of companies (e.g. involvement of the data protection officer)?

d) Technical Realisation

- What does "commonly used format" mean precisely? Which specific requirements must be laid down for a compatible format?

- How could a cross-sectoral integration of different services be reflected in the data format (e.g. automotive industry/insurance industry: transfer of vehicle/driver data and insurance data)?

- Which technical tools could be used in order to allow for data portability?

- How should the verification of the identity of customers requesting a transfer be ensured?

B. Implementation of the Provisions in Art. 20 GDPR

I. Statements

1. Research

In answer to the Call for Papers by Stiftung Datenschutz, Armin Gerl and Dirk Pohl from the University of Passau analysed the legal requirements and technical implementation solutions regarding the right to data portability:[37]

Legal Considerations

The authors differentiate between the right to copy the data (Art. 20, para. 1) and the right to transfer the data to another controller (Art. 20, para. 2). In this context, the right to receive a copy is placed close to the right of access according to Art. 15. Both entitlements are described as negotiation processes, where Art. 20, para. 1 is called "Data Subject Negotiation" and Art. 20, para. 2 is called "Controller Negotiation".

With respect to the legal requirements, the authors emphasised that a real right to data portability must not be identical to the other rights of the General Data Protection Regulation such as the right of access according to Article 15. Therefore, the authors argue in favour of a broader scope of application of the regulation, because even non-personal data could have an economic value and thus should also be covered by the right. In addition, competition law and interoperability are not the only important aspects to be considered for the right to data portability. They argued that in fact, a consistent legislation was required in the European Union which defines the legal characteristics of data and clarifies the right of ownership over the data, in particular if more than one person is concerned. In this context, it had to be considered that each data controller would have to decide which properties are categorised as personal data and provided by the person concerned and which data would also refer to third parties.

In connection with the legal requirements, the authors also discussed whether an obligation to accept the data would be desirable. They pointed out that the person concerned initiates the data transfer, but the right would be overall significantly limited by the fact that there is no corresponding obligation for the new controller to accept the data and that this was furthermore limited to cases of technical feasibility. For a balance of interests, they suggest that the controller should be obligated to announce which formats the receiving bodies can use for the data import.

Technical Considerations

With regard to the technical feasibility of data portability, the authors believe that it is unlikely that the transmission in itself would pose any significant technical problems. The authors define the term interoperability as the ability to exchange information and to use the use the exchanged information together. However, interoperability as the minimum requirement in the General Data Protection Regulation would not ensure compatibility or guarantee a result which allows for interoperable systems. For this, competition law aspects would have to be considered, as well.

37 *See Section D.*

Therefore, the authors do not describe a concrete technical solution for a possible format in their submission, but develop different scenarios how the legal conditions should be harmonised with the technical requirements. The basis for this is their above-mentioned differentiation between Art. 20, para. 1 as "Data Subject Negotiation" and Art. 20, para. 2 as "Controller Negotiation". With respect to the process "Data Subject Negotiation", they suggest a user interface so that the person concerned can intervene in the data transfer and support, check or correct it. However, this would require the format to still be readable by humans.

The second case, "Controller Negotiation", is described as negotiation between the controllers and the authors believe that in this case, too, at least a "minimalist" user interface should be considered. Assuming that there is a commonly used format, this format should generally be used in the negotiations between the controllers. However, the authors stated with regard to a "commonly used" format that this was not a technical property but would rather depend on market conditions. What is common could rapidly change due to the fast-paced technical developments. In case there is no such format, the previous controller and the new controller will have to agree on a format and correspondingly inform the person concerned about the result of the data transfer. This information can also be given by both of them, with the requirements for the previous controller being determined by Art. 12, para. 3 GDPR and those for the new controller being determined by Art. 13 GDPR.

The authors describe these two negotiation processes based on several possible scenarios, which can occur during data synchronisation or data transmission. In order to illustrate this, they sketch out a database and describe the personal data stored there as units of attributes with individual identifiers (such as: first name/last name/date of birth) and the corresponding concrete values (accordingly for instance: Jane/Doe/12/08/1964). The attributes could then be further sub-categorised based on their format (e.g. as "text" or "cipher").

The authors pointed out that the most simple solution would be if the identifier of the attributes ("last name") and the format ("text") were the same for both source and destination, because in this case, the value of the source could be migrated without any changes. In case of differences between the identifiers of source and destination, a format for data transfer would have to offer various identifications which can be extended by the controller at any time if the identifier is unknown. This would additionally raise the question who is responsible for the maintenance and administration of such a centralised data base.

Moreover, it was essential that a format for data transmission was able to separate the different concrete values of the personal data (e.g. subdivision of an address in "street name and number") and/or to combine them (e.g. combination of "street name and number" in one address), to incorporate semantic relations between the identifiers (e.g. calculation of age based on birth date) as well as to allow for changes of the format (e.g. conversion of a text to a cipher). This would, amongst other aspects, require a granular way of description of the attribute, including different "sub-identifiers" and "sub-formats". In addition, they mentioned the possibility that the respective sources and destinations would not necessarily have to contain the same attributes, meaning that for this case, too, an appropriate handling had to be ensured.

Conclusions from the Legal and Technical Considerations

In general, the authors believe that the future of data portability is mainly driven by technical developments. For the technical realisation, it would be necessary to find a commonly used and expressly described portability format with properties which enable and support the negotiation process for the described scenarios. According to the authors, codes of conduct (pursuant to Art. 40 GDPR) are a helpful instrument in order to support the right to data portability. In general, the interfaces will have to be defined for the controllers in order to avoid proprietary solutions. Moreover, it is necessary that there are enough metadata for the realisation of the negotiation process. With regard to informational self-determination, it would also be positive to provide for readability by humans as a requirement for the portability format in order to inform the persons concerned and to support the negotiation process by manual interventions.

Nevertheless, the authors are critical with respect to the question whether the economic advantages would be strong enough to ensure a corresponding market behaviour. They also critically questioned whether it would always be possible (even) within one and the same industry to provide for mutual data portability from a technical point of view. As an example, they mentioned the services Twitter and Facebook. For instance, twitter limits its text length to 140 characters, while Facebook would allow significantly longer messages.

In one analysis submitted after the Call for Papers by Stiftung Datenschutz, the association Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) dealt with data portability in the field of medical research. They explain for example, to what extent an "empowerment" of patients could be achieved with this regulation and which problems and open questions this would entail.[38] The analysis describes that in medical research, very comprehensive and detailed data is collected and that this collection goes far beyond a mere recording and description of medical conditions. With regard to the "added value" for data sovereignty, they emphasised that the provision of their own data for research or the transfer of data from one institution to another can generally be in the interest of the persons concerned. Research results could have direct advantages for patients, in particular in case of conditions for which there was no sufficient or standardised therapy – for example in the field of oncology. However, not all application cases in research would equally benefit from data portability being facilitated and the advantages for the persons concerned could also differ very much. Oftentimes, the complexity of the health data sets alone would significantly limit their usefulness for data subjects.

Apart from that, the authors also address the data types in medical research and the issue of a differentiation between the data "provided" by the patients and "interpreted" data. They explain that there was some uncertainty about when data could no longer be considered as provided by the concerned persons themselves. Because even the observation data, which was included in the provisions of Art. 20 GDPR, was often based on a more or less comprehensive analysis. The issue of a possible infringement of third party rights is illustrated based on the example of genetic diagnostics which allow conclusions regarding the health of relatives.

With regard to compatibility, they explain that on one hand, there were a number of industry- and sector-specific formats in the healthcare sector, but on the other hand, this did not mean that there is a solution for a data exchange across these boundaries.

38 See Section D.

So this is an issue with respect to the requirement of interoperability. Interoperability itself would require the use of coordinated standards – but this coordination process was complex because many stakeholders had to be involved and the heterogeneity of the data had to be taken into account. In addition, several different levels have to be incorporated: Structural interoperability (a common data model), syntactical interoperability (a common syntax) and semantic interoperability (a common understanding of the data contents). Interoperability for different formats could only be achieved if these could be reasonably converted between each other. For this purpose, the involved formats would have to be described and documented in sufficient detail. Moreover, the classification and separation of "provided", "observed" and other data would pose a particular technical challenge for the implementation.

Finally, they emphasised that electronic medical records could be a suitable technical basis for fulfilling the requirements of data portability. Electronic medical records collect all of the medical information about the persons concerned in a structured form and can be controlled by the person concerned with regard to contents and access. However, there is still no clear concept of who would be a suitable operator of such medical records based on an appropriate business model, and according to which structure and based on which standards the data could be exchanged between treatment facilities and these electronic medical records. In addition, it would have to be taken into account that clinical and research facilities in medicine process extremely sensitive medical data and thus special measures would have to be taken in order to guarantee fulfilment of the data protection and data security requirements – for example setting up a safe web portal for the encrypted download of data following a secure authentication.

The issue of so-called "lock-in effects" in social networks is discussed in the paper "The Importance of Data Portability and Interoperability in the Social Web" which was submitted to Stiftung Datenschutz by Sebastian Göndör from TU Berlin Service-centric Networking.[39] He explained that today, social networks are a communication medium with enormous importance and reach. However, social networks are mostly designed as isolated solutions ("island solutions") and benefit from network effects through which they continuously gain new users. This means that smaller competitors are pushed out of the market or into niche solutions, which massively hinders competition and innovation within the social web. Operators of social networks and communication platforms bind users to their services. Free communication with other services is not possible. Due to this, users lose control over their data and their usage. Therefore, data portability and interoperability would be appropriate measures in order to allow for an open and free social web in which users retain control over their data and are able to communicate freely. In order to achieve this, suitable protocols and data formats would have to be created.

In his paper, the lawyer Michael Strubel dealt with the scope of application of the right to data portability.[40] In his discussion of the guidelines by the Article 29 Working Party, the development history, the very substance of the regulation as well as the analysis of its wording, he in particular analyses the concept of the "provision of data". In his analysis, he points out that regarding the interpretation of this term, there was a discrepancy between the broad interpretation by the Article 29 Working Party and the necessity to limit the scope of application of the right. He emphasises that a too broad interpretation of the aspect of "observed data" which is "provided" could result in the criterion of "provision" getting out of hand and thus becoming meaningless. As a possible solution, he suggests a compromise in which Art. 20 GDPR is not applied to all "observed data" per se but the criterion of provision is interpreted in a "service-specific" way and applied to such derived personal data which is necessary for the provision of the respective service.

39 See Section D.

40 Strubel, Michael, Anwendungsbereich des Rechts auf Datenübertragbarkeit, in: ZD 8/2017, p. 355-361.

The head of the department of tele-media at the regional Bavarian data protection authority (Landesamt für Datenschutzaufsicht), Kristin Benedikt, particularly emphasised challenges in the field of authentication with regard to the practical implementation of data portability.[41] Because the bodies disclosing the data would in any case be obligated to verify the identity of the person requesting the data transfer in cases of doubt according to Art. 12, para. 6 GDPR, it would be advisable for them to carry out a standard identity check in every case, for example by providing/transmitting the data only after successful entry of a log-in and personal password. In addition, it had to be made sure that the data to be transferred was not only transmitted to the correct recipient but that this was also taking place in a secure manner. Therefore, transport layer security by means of encryption would be a minimum requirement.

Barbara Engels from the Institute of German Economy (Institut der deutschen Wirtschaft), Cologne, submitted an analysis[42] describing that while data portability could be beneficial for the data sovereignty of the individual, it could in some cases prove detrimental to competition. In her opinion, many of the legislator's demands do not take the special characteristics of platform markets into account. On one hand, data portability would result in better control over their data for the users, lower market entry barriers and increase the chances of new businesses to establish themselves. On the other hand, the implementation costs for data portability might be detrimental to start-ups and smaller businesses because established companies were better able to increase market power with their resources, which could result in disadvantages for the users. Barbara Engels believes that because of this, the right to data portability will have to be interpreted in a finely nuanced way so that the competition and innovation activity of companies is not hindered. Data portability should be enforced in markets with complementary products. In other markets, this would – from the point of competition policy – only be necessary where there is a high risk of market power abuse, as it is the case on the search engine market.

In the "European Journal of Law and Technology", Aysem Diker Vanberg and Mehmet Bilal Ünver critically discuss the practicability of the right to data portability under the European General Data Protection Regulation.[43] They explain that the main difference between the General Data Protection Regulation and European competition regulations was that the General Data Protection Regulation only applies to individual persons so that the provisions regarding competition could be supplemented by EU competition regulations, in particular by Art. 102 TFEU. This would require that this right is analysed in detail within the scope of competition law provisions and precedents. They also pointed out that the right to data portability would require the development of new services which import data from a service in a certain format and then import it in another service. However, especially small and medium enterprises did often not have the necessary resources in order to fulfil these requirements of the General Data Protection Regulation, while the costs were not significant for large companies. Moreover, they underlined that it was still unclear whether the users would actually make use of their right to data portability. In order to make sure that the right can be effectively exercised by the persons concerned, they would have to be given more information about the importance and consequences of the right. Therefore, the national data protection authorities in particular should explain the possibilities of data portability as well as possible ways of filing complaints through their websites in simple and easily understandable language.

41 Benedikt, Kristin, Datenportabilität – das neue Recht des Betroffenen; RDV 2017,189 [190].

42 https://policyreview.info/articles/analysis/data-portability-among-online-platforms; https://www.iwkoeln.de/studien/iw-kurzberichte/beitrag/barbara-engels-nicht-immer-gut-datenportabilitaet-zwischen-online-plattformen-300089.

43 Vanberg, Aysem Diker/Ünver, Mehmet Bilal, The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?, in: European Journal of Law and Technology, Vol 8, No 1, 2017. URL: http://ejlt.org/article/view/546/726.

2. Data Protection and Consumer Protection Organisations

The report "Digitale Souveränität" ("Digital Sovereignty") by the Sachverständigenrat für Verbraucherfragen (board of experts for consumer affairs, SVRV) indicates that data portability is highly relevant for the exercise of digital sovereignty.[44] As the so-called "lock-in effects" would entail a risk of market power abuse, the SVRV recommends developing easily manageable, simple standards with respect to interoperability, which ensure compatibility between digital services and thus allow for opening the market to new and innovative service providers. At the same time, they claimed that the right to data portability – the same way as digital payment traffic – should be considered a "termination of the underlying consumer contract" under obligation law, so that the consumers can "request their data to be returned in a commonly used, machine-readable and interoperable format or their deletion free of charge".[45]

The statement from the Verbraucherzentrale Bundesverband (Federation of German Consumer Organisations, VZBV) from autumn 2016 regarding the Green Paper by the Federal Ministry of Economics and Technology expresses a favourable opinion on the introduction of the right to data portability, as it reduced consumer costs for changing platforms, avoided "lock-in effects" and therefore promoted competition.[46] The VZBV focuses in particular on an effective implementation of the right and the compliance with high standards of data protection. The Federation explained that it was still an issue how powerful companies could be persuaded to make data portability available to users. They also expressed concerns whether a mere co-regulation could be successful, because powerful platforms would not be interested in facilitating the migration of their users to competitors.[47]

The statement of the European Data Protection Supervisor (EDPS), "Opinion on Personal Information Management Systems2 from September 2016, in particular emphasises the importance of "Personal Information Management Services" (PIMS) for the implementation of the right to data portability.[48] The idea behind the PIMS solutions is to give the users a comprehensible and easy possibility to manage their data and change their transmission preferences for several service providers at the same time with a standardised and centralised data control in a one-stop solution ("One-Stop Shop").[49] PIMS would therefore be especially suitable for transmitting personal data in a targeted, complete and efficient manner and thus allow for more user control.[50] However, many of these solutions are still in a development, test or implementation stage.

44 Sachverständigenrat für Verbraucherfragen, Digitale Souveränität, June 2017, p. 26.

45 ibid., p. 27.

46 Grünbuch Digitale Plattformen, statement by Verbraucherzentrale Bundesverband, dated 26 September 2016, p. 10, 18.

47 ibid., p. 10.

48 European Data Protection Supervisor, Opinion 9/2016 "EDPS Opinion on Personal Information Management Systems", p. 9.

49 See also: Stiftung Datenschutz, „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen", p. 7 ff. URL: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

50 European Data Protection Supervisor, Opinion 9/2016 "EDPS Opinion on Personal Information Management Systems", p. 12-13.

3. Other Governmental and Non-Governmental Institutions

In December 2016, the Research Services of the German Bundestag finished their work regarding the question to what extent a market concentration or monopoly position could apply to digital platforms.[51] They analysed the so-called OTT services[52], which they defined as services which are not based on a provision of content but which enable individual or group communication using the IP protocol (internet protocol). They also limited their study to messenger services such as Skype, WhatsApp, and email services.
In general, the question is to what extent these services have to be regulated in order to create equal conditions of competition. Explanations are given with respect to Art. 6 and Art. 18 of the Telecommunications Act,[53] but also with respect to the right to data portability pursuant to Art. 20 General Data Protection Regulation. In this context, they refer to the point of view of the Federal Network Agency, according to which the prevailing opinion is that there is no national need for additional regulations regarding Art. 20 GDPR. This is complemented by citing a statement from the Federation of German Consumer Organisations saying that the federal government should rather work towards effective data portability within the scope of application of the General Data Protection Regulation. Although they indicate the general possibility of a "lock-in effect" that could affect competition, the Research Services pointed out that the Federal Network Agency considered a corresponding regulation to be unnecessary. This was justified with the possibility for users to locally save the contents of email communications as well as address books by themselves. However, this should also apply if there is no such possibility, as for example with WhatsApp. Most users would use OTT services parallel in so-called multi-homing and were able to flexibly switch from one service to another without any charges. According to the Research Services' explanations, this also corresponds to the opinion of the Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V. (German Association for Information Technology, Telecommunications and New Media, Bitkom) which also opposes a national regulation on data portability in anticipation of the General Data Protection Regulation. In their opinion, the legislator should not prescribe any formats for data portability, but the requirements should rather be developed by the industry through international cooperation.

In the USA, too, the topic of data portability is considered very important. Within the scope of a public consultation on data portability at the White House Office of Science and Technology Policy (OSTP), 22 papers were submitted.[54] Many stakeholders stated that data portability was an important instrument to promote competition and improve data control for users.[55] Most of the commentators believed that the healthcare sector could particularly benefit from data portability. At the same time, many of them emphasised that the development of data portability and the privacy of the users should not contradict each other in any way.

51 The background to this was the so-called "network effect" which could occur due to rising numbers of users and the possibility of access to large data volumes.

52 As up to now, there is no consistent definition for the various digital platforms (over-the-top (OTT) services), the Research Services use the grouping set up by the Body of European Regulators for Electronic Communications (BEREC) as a basis.

53 With regard to the general applicability of the Telecommunications Act, the question is raised whether this would even be reasonable, for example because of the differences in the data protection regulations. In addition, regarding the controversial question whether such a service could be qualified as a telecommunication service in the legal sense, the Research Services refer to the pending decision of the Federal Administrative Court or the European Court of Justice.

54 White House Office of Science and Technology Policy. Request for Information Regarding Data Portability. 10/01/2017. URL: https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/OSTP-Data%20Portability-RFI-Responses_for_humans.pdf

55 Macgillivray, A., Summary of Comments Received Regarding Data Portability, 10/01/2017. URL: https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability.

Most of the concerns expressed were related to the implementation costs and to how the portability service should be ensured, as well as to the fact that up to now, there are no format standards. They also advised against too strict regulations by government bodies. As recommendations, they suggested the development of standards in cooperation with the industry, associations and consumer organisations, supporting the government in the implementation of pilot projects and promoting best practice approaches as well as raising the awareness of the users for the topic of "data portability".

In its comments on the WP29 guidelines, the international think tank Center for Information Policy Leadership (CIPL) underlined that it had to be kept in mind that there were areas, for instance in a B2B context or in employment relationships, where the possibility of data portability would not create any added value for the informational self-determination of the user.[56] They particularly emphasised that the right to data portability should not apply to the area of employment relationships ("human resources data"). Moreover, data controllers would have to clearly differentiate and categorise the different types of personal data in order to ensure an effective data transfer. They pointed out that "observed data" would not automatically fall under the category "provided data", unless the connection to this data constituted a clear added value for the informational self-determination of the user.[57] In addition, they called for a clarification what exactly was meant by "structured, commonly-used and machine-readable format" and to what extent the "interoperability" of the data should include the "compatibility" of different commonly used formats. Finally, the CIPL argues in favour of supporting cloud-based solutions such as the "pull model", as this could allow for better user control over the transfer of data to different service providers.[58]

The Internet Economy Foundation (IE.F) answered a list of questions for an expert discussion of the Digital Agenda Committee at the German Bundestag and dealt with the questions regarding interoperability and neutrality.[59] They emphasised that the interoperability of platforms constituted an important requirement for the value creation potential and power of innovation of the digital economy because it actively prevented the creation of monopolies ("market concentration") and lowered market barriers. Closed systems, which create customer retention by means of "lock-in effects" and use this to expand and strengthen their market power, would generally have negative effects for the internet economy by closing off the market. In contrast, the definition, development and use of format standards would facilitate interoperability and prevent monopoly positions of individual service providers. Consumers, too, could benefit from open interoperable systems, as these would allow them more freedom of decision, autonomy and convenience. The IE.F stated that in order to increase the users' willingness to actively use portability services, a lot of educational work will have to be done by consumer protection organisations in order to comprehensibly explain the value of their data to them.[60] In addition, they pointed out that the planned regulations would only refer to personal data, while in many cases competition would also be hindered by a lack of portability of other data types. As a switch from one provider to another would be more worthwhile the more data could be transferred, more incentives for the development of interoperability – also for non-personal data – would have to be created within the scope of the European Commission's initiative "Free flow of data".[61]

56 Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", p. 1-2, 5.

57 ibid., p. 8.

58 Center for Information Policy Leadership, Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party´s "Guidelines on the right to data portability", p. 4.

59 German Bundestag, Ausschuss Digitale Agenda, Committee Bulletin 18(24)120, 13/12/2016.

60 German Bundestag, Ausschuss Digitale Agenda, Committee Bulletin 18(24)120, 13/12/2016., p. 11.

61 ibid., p. 14, 17.

Open Knowledge Finland (OKFI) is a non-profit non-government organisation which lobbies for a free flow of information as well as an open and transparent digital society. In their statement on the first draft of the WP29 guidelines, OKFI critically questioned the term "personal data" and asked to what extent the understanding, which data is considered personal, could change with the continuing technical development and which consequences this could have for the right to data portability. At the same time, the question was raised whether the provisions of Art. 20 would entail a requirement of identifiability for persons who use certain platforms under a pseudonym and want to exercise their right of data portability.[62] With reference to the "rainbow data approach"[63], they also underlined that the solution approaches for data portability would not require any sector-specific "island solutions" – such as "Blue Button"[64] – but would produce basic standards for the download and transfer of personal data as a result. Finally, they emphasised that the discussion regarding data portability should focus on the possibilities of improved data control for users rather than on the issue of data ownership.

4. Industry Associations and Companies

In their statement submitted following the call for papers by Stiftung Datenschutz, Deutsche Telekom AG (DTAG)[65] argued that the Article 29 Working Party's guideline exceeded the legal framework of Art. 20 GDPR. In the opinion of Deutsche Telekom, the right to data portability does only apply to such data which is useful for the person concerned.

According to this statement, the Article 29 Working Party tries to substantially extend the framework and objective of the provisions of Art. 20 GDPR. The Article 29 Working Party did not have the right nor the mandate to arbitrarily broaden the scope of application of the General Data Protection Regulation. DTAG based their argumentation on the history of the legislative process, according to which the EU legislators had deliberately decided to limit the personal data affected by Art. 20 GDPR by changing the wording. In this context, it had to be data which the person concerned "provided" to a controller rather than "processed personal data" in general.

Therefore, any interpretation of Art. 20 GDPR should closely follow its wording to avoid any conflict with the EU legislator's intention. Hence, the wording did not refer to usage data and neither to data required for the conclusion of a contract. Therefore, the data controller was not obligated to make data available which is automatically generated during the usage of the service (e.g. log files, traffic or location data). According to DTAG, the term "provided" can thus only refer to such data which is controlled and can be accessed by the person concerned during the execution of the contract (e.g. photos, emails).

The expansion of the scope of application of Art. 20 GDPR by the Article 29 Working Party would only lead to unsolvable problems for data controllers. In particular for the data from electronic communication with obligations of erasure, the right to data portability would result in a large number of legal uncertainties.

62 https://medium.com/mydata/comments-on-data-portability-guidelines-2102d447f73b.

63 See also, as below, chap. B. II.

64 For "Blue Button", see below, chap. B. II.

65 See Section D.

With respect to traffic and location data, also taking into account the ePrivacy directive, the consequences for the person concerned and the new controller were entirely unclear. In addition, the transfer of traffic data would affect third party rights and would therefore constitute an infringement of Art. 20, para. 4 GDPR. Moreover, the recipient of the transferred data would also face legal uncertainties if they were for example obliged to check whether the transmitted data are covered by consent or a contractual obligation and whether processing the data would thus be legal. This would particularly affect telecommunication data (such as traffic and location data), as their processing based on a legitimate interest would not be allowed. Furthermore they considered the practice of transmitting complete data sets in order to check whether all of the data were actually necessary, as described by the Article 29 Working Party, to be very problematic from the perspective of data protection.

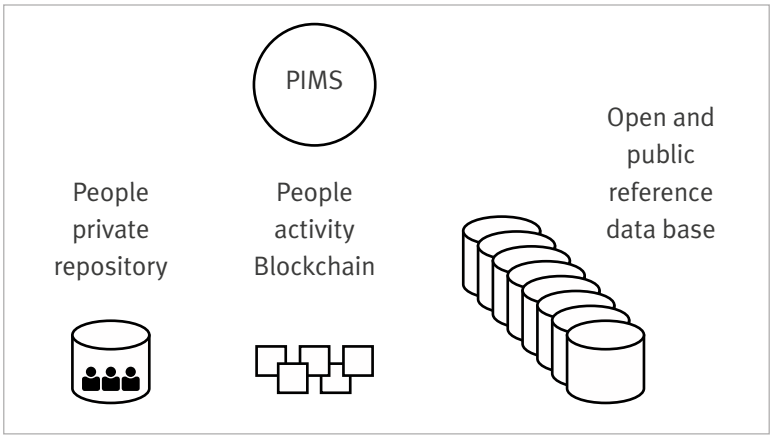
Apart from this, they also argued from a technical point of view. For instance, most service providers would not maintain separate databases for raw data which could be easily separated from the algorithms for customer analysis. As a result, a data transfer to another service provider could include detailed background information about the technical structure and the algorithms used. This would also disclose basic information about the company and affect intellectual property and trade secrets. The Article 29 Working Party did indeed have the right to support the development of general standards and interoperable systems in order to allow for simple ways for the realisation of data portability. However, this development of technical standards would take time and efforts by a large number of involved parties, including data protection authorities and institutions of the public sector.

- In a statement from Google[66] submitted to Stiftung Datenschutz, the company emphasised that data portability would allow for more user control and could also prove beneficial for innovation if it was implemented the right way. In this context, implementation should be based on four principles: User-friendly configuration, data security, reciprocal usability as well as limitation to user data rather than internal company data. In addition, they underlined that investments in the development of a portability infrastructure would pay off in the long run and that open source solutions could substantially contribute to this development. Practical implementation should however not focus on determining a universal format but rather on a search for future-oriented possibilities to create a connection between already existing, sector-specific and new formats. In this regard, Google recommends not to determine fixed standards but to support the development of open and interoperable customary standards on the part of the companies. Furthermore, the users should be strongly encouraged to security- and data protection-friendly data maintenance and should be educated about the possibilities of portability. Finally, the statement mentions the current development of a proprietary prototype, which would allow an import and export of data between two publicly accessible product interfaces and thus a direct transfer between different platforms. The company said it planned to present detailed information about this in 2018.

- The French start-up ONECUB, specialising in data portability based on PIMS since 2011, submitted a paper to Stiftung Datenschutz[67] dealing with the special significance of Personal Information Management Systems (PIMS) for the implementation of the right to data portability. At first, they identify three ways for the realisation of data portability: Direct B2C transmission, direct B2B transfer, and data transmission using an interconnected tool.

66 *See Section D.*
67 *See Section D.*

According to them, the first two solutions had the disadvantage that they were either unmanageable for users due to their complexity (for B2C) or would require (for B2B) several approvals by the user for the transfer of different data sets to a service provider (e.g. transmission of nutritional data from various services to an e-health provider), and entail high implementation expenses and efforts for the provider. An alternative would be to transfer the data using a tool with which the reuse of the data is managed by the user. The use of a so-called PIMS would allow improved access and personalised collection and reuse of the data for the user. In addition, it would also help service providers to cut costs for the implementation of data portability. However, the use of PIMS poses the problem of a concentration of a large amount of sensitive data at one central location and the security risks this entails. Therefore, the paper proposes the solution to store the data in a decentralised way on the users' devices and to connect the individual user depots by means of the blockchain method. With this approach, PIMS would be used to manage all of the technical aspects, but not to store any personal data:



- In a report submitted to Stiftung Datenschutz by the Gesamtverband der Deutschen Versicherungswirtschaft e.V. (German Insurance Association, GDV), they explain that "provided" data should primarily be defined as such data which is actively provided to the data controller by the customer, for example within the scope of an application or the processing of an insurance claim. In case any trade secrets, copyrights or rights of other persons are breached, however, a data transfer would be ruled out. Furthermore, the fulfilment of the right to data portability should ideally be integrated in existing data protection management systems. They pointed out that because in the insurance industry, highly sensitive data are processed, it is important that data portability itself did not become a risk to data protection. This could be avoided by means of an unambiguous authentication of the data recipient and by ensuring an equivalent level of data protection and data security. In this process, however, the transferring company should not be responsible for checking whether an external company needs certain data and which data they need. With respect to technical standardisation, the statement underlined that the development of general and binding standards would be very difficult given the manifold use of data in different industries and sectors. Instead, general parameters should be given – such as interoperability, platform-spanning usability, open standards and interfaces.

- In their statement submitted to Stiftung Datenschutz following their Call for Papers, the Deutsche Dialogmarketing Verband (German Association of Dialog Marketing, DDV) addresses the difference between the right of access and the right to data portability as well as the practical implementation of the regulation.[68]

68 *See Section D.*

They explain that the implementation of the right to data portability should not require considerable efforts in the area of dialogue marketing (which mainly involves data regarding invoicing and delivery addresses, order histories and information about payment processing), because it was very similar to the right of access. The data which has to be transmitted electronically would only constitute a small part of the data which a concerned person can receive in case they exercise their right of access. The special characteristic of the right to data portability was that this sub-category of data has to be transmitted in a structured, commonly used and machine-readable format. Thus, in order to meet the requirements for data portability, only a few practical adjustments were necessary in dialogue marketing – identifying the data to be transmitted, on one hand, and determining the technical method and the format, on the other hand (in the opinion of the DDV, simple formats such as ASCII as well as PDF formats would be suitable here).

- In their statement submitted to Stiftung Datenschutz following their Call for Papers, the Bundesverband Deutscher Inkasso-Unternehmen e.V. (Federal Association of German Debt Collectors, BDIU)[69] explained that the right to data portability was neither practicable nor necessary in the area of collection services. Debt collectors would communicate with the customer on behalf of another company and would on principle only receive personal data from their client. As most of this data was generated by the client, the new right to data portability would only be relevant for the collection sector if the data was directly "provided" by the person concerned within the course of the collection procedure. This could for example apply in case of address changes which are communicated via telephone. While a customer could already get an overview of the existing personal data based on their right of access pursuant to Art. 15 GDPR, the transfer of data according to Art. 20 GDPR would only concern the fragmentary information "provided" during direct customer contact. From the point of view of the industry representative, data portability would in these cases not result in any "added value" for the informational self-determination of the customer, but at the same time require considerable efforts on the part of the individual service provider (in particular for SME). Therefore, the collection sector does not consider itself a primary addressee of Art. 20 GDPR and hopes for a clarification with regard to the scope of application of the regulation.

- As a representative of the energy sector – where the issue of data portability mostly concerns energy suppliers – the managing director of regiocom GmbH, Klemens Gutmann, submitted a position paper[70] to Stiftung Datenschutz presenting the sector-specific challenges of implementing data portability. In particular the planned introductory of Smart Metering would result in extended forms of customer data collection whose transmission could on principle constitute an improvement of informational self-determination. However, there were still many unanswered questions as there were only a few examples pointing the way and Germany was still only beginning to implement a comprehensive smart meter rollout. First of all, questions regarding the contents, the amount and the format of the data to be transmitted would have to be addressed. In this context, the determination of an industry-specific format would have the advantage that it would be possible to refer to tried and tested practical examples and to transmit customer-specific data with relatively low redundancy. In addition, a practicable format for end customers would have to be determined. Apart from that, the issue of interfacing for interconnections between typical energy data and other household-relevant application areas, as it could be the case in smart homes, would have to be addressed. Considering the future situation with smart meter devices, it would also become increasingly complex to differentiate between "provided" and "processed" data.

69 *See Section D.*
70 *See Section D.*

- In another report submitted to Stiftung Datenschutz, the IT industry association Bitkom[71] underlined that the term "provided" had not been legally defined in the GDPR and therefore gave rise to a number of uncertainties. Therefore, the regulation should be interpreted based on its wording saying that the regulation only applies to such data which has been "provided" to a controller by a person. Hence, it should be sufficient only to account for those data which are controlled by the persons concerned and which they dispose of themselves. This would exclude usage data and/or data which is automatically generated during the usage of a service. With respect to technical implementation, they object to the development of cross-sectoral "one-size-fits-all" solutions because they consider it disproportionate, and call for the elaboration of industry-specific standards and formats.

- Within the scope the public consultation of the White House Office of Science and Technology Policy (OSTP) on the implementation of data portability, the industry association Software & Information Industry Association (SIIA) was one of the participants submitting a statement.[72] In their discussion regarding the implementation of data portability, SIIA argued that, depending on the service and data processing context, there had to be a stricter differentiation between different types of personal data and that colliding legal interests such as licence agreements, intellectual property and personal rights of third parties had to be accounted for. In addition, they pointed out the issues with the practical implementation of portability, for instance in the development of compatible product formats (in some cases even by competing companies), establishment of strategic partnerships as well as with regard to limited resources and capacities in small and medium-sized enterprises. According to the SIIA, political demands for data portability should therefore especially account for proportionality between the costs and efforts of implementation and the actual added value for the informational self-determination of the consumers. Data portability should first of all be facilitated in areas in which added value and benefits are evident (e.g. in the field of e-health). The SIIA believes that with respect to the implementation of data portability, the US government will mainly play the role of a mediator, supporter and moderator in the development process. The elaboration of solution approaches and development of technical standards should however be driven by the market participants.

II. Existing Solution Approaches

Up to now, there are only a few existing examples for the practical implementation of the right to data portability. These include almost no approaches which have been especially developed with regard to the fulfilment of the requirements in the General Data Protection Regulation. Indeed, many companies make an effort to prepare for the new legal situation regarding data portability.[73] However, many are still concerned about the new instrument[74]. Considering this, it is worth taking a closer look at the already existing approaches. Below, some approaches on data portability are briefly summarised.

71 See Section D.

72 White House Office of Science and Technology Policy. Request for Information Regarding Data Portability. 10/01/2017, Respondent 14, p 23-28. See also: http://www.siia.net/LinkClick.aspx?fileticket=L8dzKaK9Mx8%3d&tabid=577&portalid=0&mid=17113.

73 cf. euobserver, New EU right to data portability to cause headaches, 24/05/2017. URL: https://euobserver.com/digital/137977.

74 According to a survey by the software provider SAS, 58 of the companies surveyed saw problems with the implementation of data portability (www.pressetext.com/news/20171004025).

- Particularly with regard to the original intention of the legislator to free users from "lock-in effects" in large social networks with the help of Art. 20 GDPR, the initiative Give Me My Data (http://givememydata.com) is noteworthy. Starting from 2009, this free service from the USA has helped to retrieve user data from Facebook in a reusable format, to archive them and to reuse them accordingly. In late 2010, Facebook developed a prorietary service and demanded an update of apps which have access to the network's service, after which the company was able to determine at its sole discretion which third-party apps are granted access to the user data. These access restrictions finally resulted in the developer of "Give Me My Data" shutting the service down in 2016.[75] In a video, he still advises users on how to gain access to data stored by Facebook on their own[76]. However, as the process is very complex, it is doubtful whether the average user will make use of the suggested elaborate solution.

- Google has already in 2011 created the online service "Google Takeout"[77] for registered users, allowing them to export personal data from more than 30 online services offered by Google such as Maps, Gmail or Contacts in different formats. For this purpose, they create an archive with the selected data such as photos from Google+, videos from YouTube, mails and position data from Latitude and make it available for download. Takeout uses standard formats, which gives users additional options for handling the exported data. They can use this data for backups or other purposes or directly transfer it to services of other providers, for example Dropbox or Microsoft OneDrive. With MyAccount (www.myaccount.google.com), they also offer a central hub where users can make privacy settings and get an overview of their stored data and access rights. According to Google, this service currently registers more than one million export transactions per month.

- In Europe, as well, there are already noteworthy approaches for the implementation of data portability. For instance, the French start-up ONECUB[78] offers a data transfer service based on PIMS, the "ONECUB Connect Button".[79] This portability tool manages the exchange of personal data by allowing individual persons to collect their data and to securely transmit them between external websites or online services through an API interface. This way, ONECUB users can exchange their data with third-party providers while maintaining complete control over their privacy settings. The service has already been integrated by some companies, for example the sales platform "MyTroc", the airline passenger compensation service "Air Indemnité" and the fitness coach "Umanlife". In addition, ONECUB has been involved in the American VRM (Vendor Relationship Management) community as well as the French MesInfo community for more than seven years and discusses basic aspects of the Data Protection Regulation and data portability with French start-ups, large companies, consultancies and the French regulatory authority CNIL on a regular basis.

75 http://givememydata.com/. See also: White House Office of Science and Technology Policy. Request for Information Regarding Data Portability. 10/01/2017, Respondent 9, p. 12.

76 www.youtube.com/watch?v=WteK95AppF4&feature=youtu.be

77 See Section D, statement from Google, https://takeout.google.com/settings/takeout

78 https://www.onecub.com/

79 See Section D.

- In late 2016, the French think-tank Fondation Internet Nouvelle Génération (FING) and eight leading companies (Crédit Coopératif, Enedis, Engie, GRDF, Maif, Mgen, Orange, Société Générale) initiated the open-source project "Rainbow Button" (working title) in order to establish a common framework for the implementation of the right to data portability.[80] In the meantime, the project was also joined by the French data protection authority CNIL. The objective of the project is to reduce the complexity of the implementation of data portability by developing common specifications, guidelines and designs, allowing for manageability by the users, preventing misuse as well as creating a framework for the development of innovative services. For this purpose, the project participants developed a prototype in order to demonstrate the advantages of the portability service and to test various application scenarios. In compliance with the GDPR requirements for data portability, the project in particular develops two application scenarios: On one hand, the "download" of the data from a user account, and on the other hand, the transfer of data between different data controllers.

- In the US, several approaches on data portability have already been developed. For instance, the My Data initiative of the White House, which started in 2010, is committed to improving the access of the users to their personal data.[81] This initiative constitutes a collaborative foray to develop possible solutions supporting data portability in cooperation with public and private organisations. In cooperation with the private sector, various approaches have been worked out, such as "Green Button" for power supply data[82] or "My Student Data" for data from students. This also includes the "My Data Healthcare" initiative "Blue Button" for improved access, control and transfer of medical data.[83] The "Blue Button" is a symbol on a website, for example an online patient portal, through which patients can download their healthcare information. Depending on the implementation, users can download a large amount of infor mation in various formats, including text and PDF. In addition, "Blue Button" provides physicians with a simple way to transfer patient data. The management of the Blue Button Trust Bundle was entrusted to the non-profit organisation NATE Trust-Community.[84] Just like "Blue Button", other functional portability approaches can in particular be found in the US health sector.

One example is DirectTrust.org Inc., an organisation which was founded as a "trust community" by the US Office of the National Coordinator for Health Information Technology (ONC). As an independent non-profit association of 124 healthcare IT and healthcare service providers, they support the secure, interoperable exchange of healthcare information through direct messaging protocols. DirectTrust created a "Trust Framework" which extends the use of Direct Exchange to more than 94,000 healthcare organisations and more than 1.4 million direct addresses and accounts.[85] Recently, DirectTrust has also elaborated some suggestions regarding technical standardisation in the healthcare sector.[86] The NATE trust community mentioned above also campaigns for the improvement of data portability in the healthcare sector in a cross-sectoral collaboration with consumer protection organisations, healthcare experts, technology companies and former politicians. In conclusion, it can be noted that data portability of healthcare information within the US healthcare sector is already in an advanced stage of development which is not least due to new forms of cooperation between the government, economic operators and non-profit organisations.

80 http://mesinfos.fing.org/wp-content/uploads/2017/03/RButton_Perimetre_english.pdf

81 https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access

82 http://www.greenbuttondata.org/

83 http://www.myphr.com/Resources/blue_button.aspx

84 http://nate-trust.org/?s=Blue+button

85 https://www.directtrust.org/about-directtrust/

86 DirectTrust, Comment to ONC on Draft 2017 Interoperability Standards Advisory, p. 4-6. URL: https://www.directtrust.org/wp-content/uploads/2016/11/DirectTrusts-Comments-to-ONC-on-Draft-2017-Interoperability-Standards-Advisory.pdf

C. Assessment and Recommendations for Action

I. Assessment

1. Objectives of the Regulation

Opportunities and Risks of Data Portability

The discussion of the right to data portability with statements from relevant stakeholders and the analysis of existing solution approaches primarily raises the question to what extent the new regulation will result in an increase in the protection of data privacy ("informational self-determination") for the consumer. In this context, it has to be taken into account that the transmission of data according to the provisions of Art. 20 GDPR only concerns a copy of the data set and does not constitute a right to erasure.

On one hand, users would indeed benefit from the flexible possibility to make their data easily available to different service providers. The right to data portability would in particular be helpful in the so-called Internet of Things, if people were able to use the data from their usage of networked devices not only in the relation to the supplier of a certain product but also for other purposes, and to link data from different service providers together.

On the other hand, the duplication of personal data resulting from the data transfer could also lead to an increase of data protection risks. This would at any rate apply to possible cases in which entitled parties did not assert their right pursuant to Art. 17 GDPR (erasure) with respect to the addressee of the transfer request. Thus, the data transfer would not be carried out as an actual "data migration" but rather as a "data duplication". This would in fact mean that the use of personal data is not minimised but rather expanded – including all of the generally existing uncertainties[87] with regard to the data usage by controllers.

The objective of the regulation to support informational self-determination might in particular be reversed if consumers are incited to make excessive use of their rights pursuant to Art. 20 GDPR by means of financial incentives such as discounted contract conditions. The "right to data portability" could then de facto prove to be a hidden "obligation" to duplicate data sets. Business models could be established which deliberately exploit the portability rights of the consumers in order to accumulate personal data and create cross-sectoral customer profiles. This concern is obviously also taken up by the Swiss Federal Council in their statement that the right to data portability "rather has the objective of allowing the persons concerned to reuse their data in order to leave more space for competition than to protect their privacy".[88]

Data protection and data security risks are particularly high when very sensitive data is concerned – for example in case of insurance and healthcare data. In these cases, a definite authentication of data recipients as well as equivalent data protection and data security levels must be ensured as otherwise, fraudulent requests for data transfers could easily be possible.

87 Regarding the issue of the "informed consent", see the study by Stiftung Datenschutz "New ways of providing consent in data protection - technical, legal and economic challenges", URL: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/.

88 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, 21 December 2016, p. 22. www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.

For instance, a risk of misuse could arise if a company (e.g. a large chain of car repair shops) virtually instigates their customers to exercise their right to portability in order to impair the competitive position of their competitor by means of excessive data inquiries (e.g. from a smaller car repair shop). With regard to such constellations, it should however be pointed out that cases of excessive or fraudulent requests should be covered by Art. 12, para. 5 GDPR (possibility to refuse if requests are manifestly unfounded or excessive).

Many stakeholders also expressed concerns that the right to data portability could prove to be a competitive disadvantage. For example, some fund-raising organisations (NGOs) are concerned that in case of the application of Art. 20 GDPR, they would have to transmit the entire history of donators to competing NGOs and that this data would disclose the working methods of the respective NGO so that company secrets could be revealed. Moreover, the implementation costs for data portability might be detrimental to start-ups and smaller businesses, because established companies were better able to increase market power with their resources, which could result in disadvantages for the users.

In addition, there seem to be justified doubts that the regulation will be able to break up large market monopolies and "network effects". Indeed, data portability and interoperability could on principle be appropriate measures in order to allow for an open and free social web in which the users retain control over their data and are able to communicate freely.[89] However, it remains to be seen whether the implementation of a portability service alone could in practice lead to a removal of "lock-in effects". In particular the example of the "Google Takeout" service, which has been existing for six years and substantially corresponds to the right to data portability, does not provide any indication that the market dominating status of Google has in any way been "broken down" by the offer of "data migration". The doubts regarding the effectiveness of the regulation are especially great in regard to social networks, because the transfer of the data which would be the most relevant for users – generated user analyses, user profiles, but also data relating to third parties (e.g. Facebook "friends") – is excluded from the provisions of Art. 20 GDPR. Nevertheless, it has to be noted that the effect of the regulation on those providers who generate "network effects" from the connection between online services and the use of certain hardware products, for example in the Apple ecosystem, remains to be seen.

Promotion of Data Sovereignty

In order to ensure the promotion of informational self-determination through the right to data portability, it is important to ensure the effectiveness of the regulation. The point is that data subjects will only make use of their right to data portability if its added value is evident to them and thus the associated efforts seem proportionate to the benefits. For one thing, this means that the effectiveness of concrete solution approaches has to be tested in practice. This includes for example behavioural economic surveys examining to what extent the right to data portability is actually exercised by the users.

On the other hand, it has to be specified for the implementation of the regulation that the right to data portability only applies to such data whose portability effectively contributes to the promotion of informational self-determination. If the interpretation of the regulation is too broad, data protection risks could even increase and it could result in a disproportionately high amount of work regarding the categorisation and extraction of data sets for the data controllers. Therefore, the interpretation of Art. 20 GDPR has to focus on the original intention of the legislator which is to allow for more data control.

89 cf. Göndör, Sebastian, see section D.

Thus, the scope of application of the regulation should focus on data sets which are necessary for switching from one provider to another. The users should also have a basic understanding of the data sets they receive so that they are able to check and control them and to use them to their advantage. At least, this applies in cases where the users receive the data themselves (Art. 20, para. 1 GDPR), rather than in case of a requested direct transfer according to paragraph 2. In addition, the proportionality between the efforts and expenses for the implementation of the regulation and the practical effectiveness of individual measures for data sovereignty should be kept in mind.

The practical definition and arrangement of the regulation must be adapted to its original intention, which was brought back to the fore again by the second version of the Article 29 Working Party's recommendations: The improvement of data privacy ("informational self-determination") for the consumers. In the context of data portability, this means that users have to be given more control over the transmission of personal data.

Conclusion

In conclusion, it can be noted that, as a matter of principle, the right to data portability can give users better means of control over their personal data. However, the risks which this new regulation could entail should not be underestimated. For one thing, the duplication of data sets could lead to an increase of data risks. In particular, if consumers are incited to make excessive use of their rights pursuant to Art. 20 GDPR by means of financial incentives such as discounted contract conditions and if the portability rights of the users are deliberately exploited in order to accumulate personal data and create cross-sectoral customer profiles. On the other hand, the regulation could prove ineffective or even have an anticompetitive effect if minimal benefits for consumers from the transfer of data sets are opposed by extremely high costs and efforts for their preparation and transmission by controllers, which could then only be managed by large market operators. In addition, the analysis of previous approaches seems to raise justified doubts whether the practical implementation of a portability service would necessarily result in the removal of market monopolies and "lock-in effects". It has to be kept in mind that high implementation costs for data portability might be detrimental to start-ups and smaller businesses.

2. Determination of the Scope of Application[90]

Provided Data

The term "data provided" in Art. 20 is not legally defined in the General Data Protection Regulation. The Article 29 Data Protection Working Party uses a broad interpretation of this term in their statements (Guidelines on the right to data portability) and includes contract as well as usage data in its scope of application.[91] Hence, this interpretation also includes so-called "observed data", i.e. data which is generated based on the usage of a service.[92]

90 The following chapter is based on the statement submitted by Anne Riechert, see chap. D. III.

91 Article 29 Working Party, WP 242 "Guidelines on the right to data portability" from 13/12/2016 and Article 29 Working Party, WP 242 "Guidelines on the right to data portability" from 05/04/2017

92 Article 29 Working Party, WP 242, p. 5; Benedikt, RDV 2017, p. 190; Jülicher/Röttgen/v. Schönfeld, ZD 2016, p. 359, who are opposed to active actions as a precondition.

This extended interpretation, which includes traffic as well as location data, is rejected with reference to the wording of the regulation.[93]

In terms of such a stricter interpretation of the term "provided", only such data would be included which has actively and deliberately been provided by the person concerned and is required for the fulfilment of a contract, but no usage data.[94] In this context, it is also pointed out that this narrow interpretation was supported by the history of the legislative process as well as by the objectives of the provisions of Art. 20 GDPR.[95] Experts unanimously agree that the scope of application does not include data which is only processed and generated by the controllers themselves based on the data provided ("inferred data", such as score values).[96]

With respect to third-party data, their protection rights have to be respected according to Art. 20, para 4 GDPR. In this regard, the Article 29 Working Party explained that personal data of third parties can be transferred to a new controller for private and personal use, provided that they remain under the exclusive control of the transferring person.[97] Indeed, the General Data Protection Regulation would not apply if the data was processed "by individual persons exclusively for personal or family purposes and without any intention of making a profit". In such cases, it had however to be considered that personal data is transferred to a commercial service provider. Therefore, it is questionable how these new controllers would implement these requirements in practice. This is particularly relevant with regard to the possibility to process data based on legitimate interests according to Art. 6, para. 1f GDPR or based on a change in purpose according to Art. 6, para. 4 GDPR. Because there are no consistent interpretation criteria for these processing elements across Europe, the extent of a possible data processing would currently not be foreseeable for any concerned third parties. First of all, it has to be taken into account that these third parties could previously have consciously decided against a certain service provider so that in this situation, civil law claims could be asserted, for example claims to cease and desist. This means that it would be extremely important to ensure sufficient transparency in the entire process. The respective concerned persons should not lose track of the data controllers and the rights of erasure they are entitled to.

93 See Bitkom, statement on data portability (Stellungnahme zum Recht auf Datenübertragbarkeit nach Art. 20 Datenschutzgrundverordnung) from 14/03/2017, S. 7 as well as statement by Deutsche Telekom AG (Statement on the "Guidelines on the right to data portability" of the Article 29 Data Protection Working Party), p. 2. See also Bitkom, statement on data portability, p. 11, with the indication that telecommunication and location data were not included in the scope of application. However dissenting with Article 29 Working Party, WP 242, p. 10, who are in favour of including it.

94 See Strubel, ZD 8/2017, p. 357/358, who explains that "letting things happen" was not sufficient and this would refer to direct collection. See also statement by Deutsche Telekom AG, p. 2, who limit the characteristic to "useful" data which is controlled by the user. In addition, they suggest to interpret the aspect of provision in a service-specific way and thus only to apply the right to such data which is necessary for the usage of a similar service (see also Strubel, ZD 8/2017, p. 360, who differentiates based on whether the data is required in order to provide a similar service).

95 Strubel, ZD 8/2017, p. 357 ff., also in the legal statement submitted by Anne Riechert, in detail under section 1.1, see chap. D. III.

96 Article 29 Working Party, WP 242, p. 10.

97 Article 29 Working Party, WP 242, p. 11 ff. On one hand, the Article 29 Working Party explained that a new controller should not be allowed to use the transferred data of third parties for his own purposes (e.g. for promoting marketing products and services) On the other hand, however, they believed that such data processing was only very likely to be illegal and unfair, in particular when the concerned other persons had not been informed about this and could not exercise their right as persons concerned. Therefore, a possible further processing by a new controller would have to be subsumed under permissible processing which is based on "legitimate interests" and is at the same level with all elements of data processing according to the wording of the General Data Protection Regulation. However, until now, there are no consistent rules for interpretation across Europe in this regard.

According to the wording, the scope of application of Art. 20 GDPR also applies to employee data. As applicability in individual cases is however debatable, corresponding interpretation criteria will have to be developed for this aspect, as well.[98]

Interoperable Format

Art. 20 GDPR does not contain any definition for an interoperable format. According to the intention of data portability, however, it is important to use a format which allows for a reasonable reuse of data by the person concerned or the new controller. Such a format shall be developed in the future.[99] This means that certain formats such as PDF documents as a machine-readable format could be ruled out, even if this format is sufficient as an electronic format within the scope of the right of access.

In addition, it is debatable whether the transmission of metadata is beneficial and necessary for data portability[100] or if it actually conflicts with the interests of data protection.[101] The Article 29 Working Party believes that the personal data should be accompanied by as many metadata as possible.[102] However, they do not specify what exactly characterises metadata in contrast to personal data. Sufficient metadata is requested from a technical point of view, as well.[103] In terms of this view, metadata can on one hand be personal, but can on the other hand also concretise an attribute and for example determine restrictions (e.g. of text length). The draft of the ePrivacy Directive[104] actually even contains a legal definition for communication metadata which refers to such data, from which conclusions regarding the private life of the persons involved in an electronic communication can be drawn.[105] This metadata can for instance be traffic and location data, which are however classified as "personal data provided by the person concerned" by the Article 29 Working Party, which is in turn opposed on the part of the companies.

Therefore it is advisable to check whether there is a consistent technical and legal understanding of the term "metadata". This is particularly relevant in order to decide which metadata are required for the successful implementation of data portability as well as for the development of a format from a technical point of view, and which are permissible from a legal point of view.

98 Hennemann, PinG 01.17, p. 5; Bitkom, statement on data portability, p. 8. The Article 29 Working Party refers to individual examinations of each case and does not rule out the applicability in general (Article 29 Working Party, WP 242, p. 8/9).

99 Article 29 Working Party, WP 242, p. 18. See also Schätzle, PinG 02.16, p. 74/75; Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries, whereas these authors in their report describe the general conditions for a corresponding data transfer format based on different scenarios and do not consider portability in itself an obstacle. See also Hennemann, PinG 01.17, p. 8, who points out that, in fact, Art. 20 General Data Protection Regulation does not call for interoperability. This requirement is only mentioned in Recital 68 of the General Data Protection Regulation.

100 Article 29 Working Party, WP 242, p. 18, who suggest metadata at the highest level of granularity; Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries, see Section D.

101 See statement by Deutsche Telekom AG, in which they pointed out that the transmission of a complete data set with a subsequent check whether all of the data is actually required was highly questionable with respect to data protection.

102 Article 29 Working Party, WP 242, p. 18.

103 Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries, see Section D.

104 Suggestions for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for privacy and the protection of personal data in electronic communication and for the repeal of directive 2002/58/EC (Directive on Privacy and Electronic Communications) from 10 January 2017 (ePrivacy Directive). According to Art. 95 of the General Data Protection Regulation, no additional obligations are imposed on individual or legal persons with respect to processing in connection with the provision of publicly available electronic communication services in public communication networks within the Union, provided that they are subject to special obligations which have the same objectives and are determined in directive 2002/58/EC. The ePrivacy Directive is the follow-up regulation and defines and complements the General Data Protection Regulation by determining specific rules.

105 See definition of the term metadata in electronic communication on p. 13 as well as in Art. 4, para. 3 c of the Directive on Privacy and Electronic Communications (ePrivacy Directive). This includes for example telephone numbers called, websites visited, geographical location, time of day, date and duration of a phone call made by a person, from which precise conclusions might be drawn regarding the private life of the persons involved in the electronic communication, e.g. with regard to their social relationships, habits and daily life, their interests and tastes.

With respect to the technical feasibility of direct portability of data between the controllers, it is also important to note that this characteristic could be interpreted in a subjective as well as in an objective way.[106] This means that in this regard, criteria will have to be developed determining to what extent the individual capability of the companies could play a role.

Competition Law Aspects

The perspective of competition law is relevant for Art. 20 GDPR, because on one hand, the competition law character is always referred to[107] and on the other hand, it has to be assessed to what extent the regulation can constitute a market conduct rule. For example it might constitute a breach of §3a UWG[108] (German Act against Unfair Competition) (breach of law) and §4 no. 4 UWG[109] (deliberate hindrance of competitors) in case interoperability is not implemented and if no trouble-free transfer possibility for data is provided.[110] In the past, it has been confirmed that a breach of information duties under data protection law can constitute an infringement of competition for which a cease and desist order could be issued.[111]

In case of an accusation of a deliberate, anticompetitive hindrance, the Federal Court of Justice for instance assesses the overall circumstances of each individual case, taking into account the interests of the competitors, consumers and other market operators as well as the general public.[112] This would require that both parties supply similar goods or commercial services, however, they would not have to be in the same industrial sector.[113] In contrast to this, Art. 20 GDPR grants the right to data portability "across the board" and does not contain any restrictions or weighing of interests, for instance with regard to industrial sectors or similar services.

The law on unfair competition and the data protection law are considered equally important. Therefore, it is questionable whether different assessments and sanctioning options will be possible in the future. This is associated with the disagreement concerning the spirit and purpose of Art. 20 GDPR, which on one hand has the purpose of supporting the right of informational self-determination, but on the other hand, is construed restrictively regarding the aspect that (only) a data transfer from one service provider to another shall be facilitated and "lock-in effects" shall be avoided.[114]

106 Hennemann, PinG 01.17, p. 8.

107 See also Hennemann, PinG 01.17, p. 6, who points out the competition approach as well as the legislative process during which it was suggested not to regulate this right within the scope of the directive.

108 The breach of law is regulated by §3a UWG. According to this article, anyone is acting unfairly who acts contrary to a legal provision which has the intention to regulate market conduct in the interest of the market operators and if this breach could substantially prejudice the interests of consumers, other market operators and competitors.

109 §4 UWG regulates the protection of competitors. According to this article, anyone is acting unfairly who purposefully hinders their competitors.

110 In German jurisprudence, it is controversial to what extent data protection regulations simultaneously constitute market conduct rules in terms of the UWG. For instance denied by Higher Regional Court (OLG) Munich, decision from 12 January 2012, ref. 29 U 3926/11: The data protection right was a product of personality rights and protects this individual legal position in general while it does not concretely refer to protection in the role of a market operator. Irrespective of the fact that breaches of the provisions of the Federal Data Protection Act (BDSG) could certainly have consequences in a business environment, these provisions do not constitute market conduct rules (with reference to the exception of §28, para. 4, s. 2 BDSG). See also OLG Cologne, decision from 19 November 2010, ref. 6 U 73/10; Superior Court of Justice Berlin, decision from 29 April 2011, ref. 5 W 88/11; OLG Stuttgart, decision from 22 July 2007, ref. 2 U 132/06.

111 OLG Hamburg, decision from 27 June 2013, ref. 3 U 26/12 with the argument that §13 German Telemedia Act (TMG) (information duties) was a rule regulating market conduct in terms of §4 no. 11 UWG (now §3a UWG), and not merely as an infringement of a rule regulating only supra-individual matters of free competition.

112 BGH, decision from 22/01/2014 – I ZR 164/12.

113 BGH, decision from 24/06/2004 – I ZR 26/02.

114 See also Hennemann, PinG 01.17, p. 6 with reference to Recital 68 of the General Data Protection Regulation.

However, the latter do not necessarily occur and an obligation to implement interoperability could also have anticompetitive effects, in particular for new and innovative services, and could constitute a considerable interference with entrepreneurial freedom.[115]

Conclusion

The right to data portability has to be safeguarded. However, it is questionable whether additional decisions and assessments on individual cases would be useful in order to achieve a result doing justice to the respective interests. Regarding the issue whether the scope of application includes contract data as well as usage data, the scope of protection of the regulation could also be relevant, because usage data are in their entirety included under the electronic copy of the right of access pursuant to Art. 15, para. 3 GDPR, which means that the right to informational self-determination would be guaranteed. In any case, the question in this context is whether a direct transfer would rather have advantages for the new controller who incites persons to disclose their usage data by developing new business models.[116] Therefore, it should always be assessed for each individual case, under which circumstances a direct transfer of all usage data to another service provider would actually support the improvement of control rights for the person concerned. In this regard, a result doing justice to the respective interests could for example be achieved with the objectivity of the term "required" concerning the contractually relevant data according to Art. 20, para. 1a in connection with Art. 6, para. 1b GDPR. This way, service aspects could be considered and the creation of a customer profile (e.g. as a purchase history or records of a fitness app) could for instance be evaluated as "required for contract fulfilment" and thus also as a reasonable interest of the customer. In this context, ensuring transparency constitutes another essential requirement as the person concerned has to know all of the information relating to the processing by the old and the new data controller.

With regard to the differentiation from competition law, it will have to be decided to what extent both fields of law can influence each other and if it could therefore be advisable to develop criteria which allow for a consistent perspective on competition law and data protection law as well as for a differentiated result. In the assessment and the elaboration of rules of conduct according to Art. 40 GDPR, it could be taken into account whether the interests of the general public as well as the right to informational self-determination as interest of the persons concerned include a right to "across-the-board" data portability. Indeed, the balancing of interests is not included in the wording of Art. 20 GDPR. Nevertheless, the interpretation of the regulation could be subject to an ongoing, practice-oriented examination regarding to what extent decisions could be made in individual cases for instance based on data, industries, services or similar aspects, without interfering with the right to informational self-determination of the persons concerned. In addition, the competition law aspect of the comparability of services likewise corresponds to the original intention of the law and the protection purpose of Art. 20 GDPR, as this was focused on social networks and was intended to facilitate a switch from one provider to another.[117]

It should also be kept in mind that the sanctioning options of the data protection authorities could now result in severe consequences due to an increase of the level of fines.

115 Paper of the Research Services of the German Bundestag on the topic of "Regulierung von Messengerdiensten, Datenportabilität und Interoperabilität" ("Regulation of messenger services, data portability and interoperability"), p. 18, also with reference to the opinion of the Federal Cartel Office. See also Hennemann, PinG 01.17, p. 6, who underlines the competition approach.

116 See above, C. I. 1, as well as Gutmann, Beispiele aus der Energiewirtschaft, who is generally critical in his assessment of the demand for more informational self-determination for the persons concerned.

117 See Hennemann, PinG 01.17., p. 6 with reference to the competition approach as well as to the statement by Jan Albrecht (Rapporteur of the European Parliament on the General Data Protection Regulation) who considers Article 20 a catalyst for a competition for data protection-friendly technologies.

3. Implementation Strategies

Structural Implementation

The definition and arrangement of the data portability regulation reflects a fundamental dilemma regarding network regulation: On one hand, the regulation has the objective to determine the framework for legal data processing in as concrete terms as possible, while on the other hand, such a regulation would "ex ante" have to remain vague enough for newly developing technologies and possible innovative approaches to solutions.[118] For example, the data portability regulation calls for keeping the data in a "structured, commonly used and machine-readable format" (Art. 20, para. 1 GDPR) but does not specify what this format should look like in detail, which requirements it has to fulfil and how interoperability between different "commonly used formats" shall be achieved. Thus, the individual addressees of the regulation face the challenge to fulfil the requirements of the regulation without being given a precise guideline, general standards or even tried and tested practical examples. This makes a fundamental problem blatantly obvious: The lack of suitable implementation strategies for data protection regulations.

In particular, the implementation of data portability in the US healthcare sector and the "Rainbow Button" project of the Fondation Internet Nouvelle Génération (FING)[119] show that new forms of public-private partnerships can be considered a suitable concept for the practical realisation of requirements for data portability and the development of standards. The management of the cooperation between technology companies, experts, consumer protection organisations, NGOs, public bodies and political decision-makers by independent non-profit institutions ("trust communities") following the example of the US healthcare sector[120] has the necessary potential to respond to the government's protective duties on one hand and to support the flexible development of innovations on the other hand in the implementation of the right to data portability.

For this purpose, corresponding approaches for "regulated self-regulation" have to be developed, establishing a framework under state supervision within which government and non-government institutions as well as companies develop implementation strategies and standards for data portability. For an effective definition and arrangement of data portability and realisation of legal compliance, it is absolutely necessary to involve companies and industries which will presumably be particularly affected in formal consultation processes of the regulatory authorities from an early stage in order to ensure an implementation of Art. 20 in accordance with the law.

Approaches for Practical Implementation

The focus in the practical implementation of the right to data portability lies above all on the development of procedures for the data transfer. As it has already been explained in the second version of the Article 29 Working Party's recommendations (page 16/new), there are basically two possible solutions to enable data portability: A direct transfer to the user (para. 1) or rather to the third-party provider (para. 2), or a transfer via an interconnected centralised application.

118 See also: Horn, Aus Sicht der Stiftung Datenschutz – wie die Regulierung im Datenrecht Schritt halten kann, in PinG 05/17.
119 See above, B. II.
120 Cf. above, B. II.

In particular in cases in which, due to specific business models, the right to data portability only applies to a small number of data sets which are easy to collect and to transmit, a direct transfer of data can be realised in a relatively simple and efficient way which is also easily manageable for the user. In addition, it is currently still unclear how many users will actually exercise their right to data portability. For the respective industries and companies, the actual demand for data transfers will be relevant because this could influence their decision to undertake great efforts and to carry out fundamental adjustments to their systems. In case of a low demand for data transfers, they could however react based on each individual case and by means of manual compilation and direct transfers of data sets. Currently, it cannot be predicted to what extent the interest in data portability will be increased by new business models and how many users will as a result actually exercise their rights.

In cases in which portability concerns several heterogeneous personal data sets, which are transmitted to different third-party providers for different processing purposes, a tool-based approach might be preferable. In this case, a distinction would have to be made between group-specific, sector-specific and universal procedures.

For market-dominating groups such as Apple, Facebook or Google, a group-specific technical implementation based on the model of the above-mentioned "Takeout" service (chapter B. II) would be possible. By bringing together individual online services and with the possibility of extracting personal data, users are in a simple way given the opportunity to manage the use and transfer of their data in a centralised manner. In the example of "Takeout", it is particularly relevant that this portability service is integrated in a global data protection dashboard (here "MyAccount") where the portability functionality can be easily found next to the other privacy settings. However, the question remains whether and how interoperability, compatibility and real integration possibilities for data sets extracted from the services of individual "big players" can be guaranteed in practice. In any case, the will of individual market-dominating groups to cooperate will be an important requirement for the effective implementation of the right to data portability which is also practicable for users. In this regard, it has to be taken into account that in case market-dominating groups agree on one or more certain standards, a "standard monopoly" could result which could prove detrimental to the development and the competition of alternative portability models.

Industry-specific solutions following the example of "Blue Button" services[121] in the US healthcare sector seem promising. The main advantage of industry-specific initiatives is that data types and formats as well as special data protection aspects can be adjusted to industry-specific requirements. In addition, the development of and agreement on specific tools and formats within individual industry sectors can be realised in a more efficient and targeted way than it would be for more complex cross-sectoral agreement processes. Furthermore, there are already existing overriding portability regulations under European law in certain sectors, as for example in the credit industry with regard to account information, the switch to another credit institute and the records of securities transactions. Industry-specific adjustments are also facilitated by the possibility of referring to already existing internal portability practices within the sector (such as the transfer of master and supply data of customers in the power supply sector[122]).

121 *See above, B. II.*

122 *See Section D., Klemens Gutmann.*

In many cases (in particular with respect to the switch to another provider), in which the transfer of customer data is useful for consumers as well as companies, there are already existing arrangements – for example mail forwarding orders, telephone number porting, account switching services or the transfer of no claims bonuses .Moreover, it is becoming evident that the efforts and expenses for the implementation of the regulation can be relatively low in certain economic sectors if it only applies to a limited amount of data[123] or if only a small number of portability requests is to be expected.

Universal solution approaches are mainly recommendable for application to cross-sectoral and complementary services. For services which use cross-sectoral data sets (e.g. location data, insurance data, healthcare data, purchase profiles, etc.) or for markets with complementary products (e.g. in the Smart Home area), the added value can be increased[124] and a framework for new and innovative business models can be created. In particular, universal, tool-based and user-oriented solutions based on Personal Information Management Systems (PIMS) can prove to be promising implementation strategies for the right to data portability.[125] With a standardised and centralised data control in one stop ("One-Stop Shop"), users are given a comprehensible and easy possibility to manage their data and to share it with several service providers at the same time.[126] PIMS would therefore be especially suitable for transmitting personal data in a targeted and efficient manner and thus allow for more user control.[127] Additionally, the development of PIMS solutions such as the "Rainbow Button" project or the "ONECUB-Connect Button" described above (chapter B. II), could also provide a suitable platform for the cooperation between different service providers and industries.

Conclusion

In conclusion, it can be said that for the implementation of the right to data portability, approaches of "regulated self-regulation" should be used, establishing a framework under state supervision within which regulatory authorities, NGOs as well as companies develop implementation strategies and standards for data portability. For an effective definition and arrangement of data portability and realisation of legal compliance, it is above all desirable to involve companies and industries which will presumably be particularly affected in formal consultation processes of the regulatory authorities from an early stage.

For the practical implementation of data portability, industry-specific as well as universal approaches can be taken into account. The application of industry-specific methods is advisable for the use of sector-specific data sets (e.g. healthcare and power consumption data) as well as in cases in which there are already tried and tested internal portability solutions within the industry. Universal solution approaches based on PIMS are mainly recommendable for application in cross-sectoral and complementary services such as in the networked home or for networked driving. In cases in which the right to data portability only applies to a small number of data sets which are easy to collect and to transmit and/or in case a low demand for data transfers is to be expected, a direct transfer of data based on individual cases could however be preferable.

123 cf. statement by Deutschen Datenmarketing Verbands (DDV), see Section D.

124 cf. statement by Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV), See Section D.

125 See also statement by the European Data Protection Supervisor (EDPS) "EDPS: European Data Protection Supervisor, Opinion 9/2016 "EDPS Opinion on Personal Information Management Systems", p. 9.

126 See also: Stiftung Datenschutz, „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen", p. 7 ff. URL: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

127 European Data Protection Supervisor, Opinion 9/2016 "EDPS Opinion on Personal Information Management Systems", p. 12-13.

4. Technical Realisation[128]

Current Situation

Due to the right to data portability, service providers are faced with the challenge to adjust and complement existing IT systems in such ways that precisely defined data sets with personal data can be transmitted to the individual persons concerned or to another service provider indicated by these persons. In the future, this data has to be made available in a structured, commonly used and machine-readable format.

The question, in which format the data shall be transmitted, concerns technical, legal and economic as well as acceptance-oriented aspects. The legislator does not define or specify precise requirements regarding the technical realisation. The General Data Protection Regulation only calls for the creation of organisational and technical measures and processes in order to efficiently achieve the objectives of the provisions. At the same time, the act remains neutral with respect to technology. It does not prescribe a certain format or a standard. The wording of the regulation only provides for the use of a "structured, commonly used and machine-readable" format. In addition, it calls for the development of interoperable formats (Recital 68) which allow for the further processing of the data in other systems.

Architecture of the Data Format

The original version of the Guideline by the Article 29 Working Party, according to which as much metadata as possible shall be made available at the highest level of granularity, was in a revised version clarified to include the specification that commonly used and open formats shall be used, unless another or no format was customary in a certain industry or a certain context. As examples, the formats XML, JSON, CSV were listed.

More important than the selection of the precise format is however the architecture or rather the general characteristics of a "commonly used" format. Here, different levels have to be incorporated: Structural interoperability (a common data model), syntactical interoperability (a common syntax) and semantic interoperability (a common understanding of the data contents). Interoperability for different formats could only be achieved if these could be reasonably converted between each other. For this purpose, the involved formats would have to be described and documented in sufficient detail. As a result, the data shall be arranged within a file following a comprehensible pattern or rather a certain blueprint. The architecture has to indicate syntax and semantics of the data within the file. While syntactical information defines how the data is structured and composed (metadata), the actual contents are consistently determined on the semantic level. From this structure, it can be deduced how the file itself (identify and handle) and also how the data within the file have to be interpreted. Thus, the efficient machine-readability of the personal data contained therein is ensured.[129] This would also allow for the functional realisation of interoperability.

128 This chapter is based on the expert opinion by Gunnar Hempel/Karl Schmid, SCRC e.V. Leipzig, University of Leipzig, Chair of Business Informatics, Prof. Dr. Rainer Alt., commissioned by Stiftung Datenschutz, see chap. D. II.

129 cf.: Hempel/Schmid, SCRC e.V. Leipzig, University of Leipzig, Chair of Business Informatics, Prof. Dr. Rainer Alt., see chap. D. II.; Drepper/Schlünder/Buckow, Praktische Umsetzbarkeit der Datenportabilität im Bereich der medizinischen Forschung, see Section D.

A suitable solution in this context would for example be the XML-based standard for the structuring of personal data. XML allows for different granularity levels without any problems. In addition, the information contained in the XML schema is not only machine-readable but it can also be read by the persons concerned themselves using standard software. Apart from the right to data portability, this property could also support the exercise of access rights by the persons concerned.[130]

The minimum requirement for data portability and/or interoperability is to write the data into a basic CSV format and to add a simple description of how the data is arranged in the file. This description has to indicate which data contents can be found at which position inside the file (surname, first name, date of birth, etc.) and, if applicable, what certain codings mean.

For the transmission via information technology, appropriate security measures must be guaranteed, such as end-to-end encryption of the data during transport using to the latest technology. In addition, secure identification and authentication of the person concerned has to be ensured in any case (log-in procedure, double opt-in).[131] The requirement to process the data in a way which guarantees sufficient security is indispensable and a general principle in data protection law (e.g. Art. 5, para. 1f GDPR). This also includes the integrity and confidentiality of the data, which has to be ensured by means of suitable technical and organisational measures. For this purpose, it will be advisable to transmit the data in a tamper-proof and signed format. This way, it could in case of doubt be verified that the controller has exported correct and unaltered data. Otherwise, there would be a general risk of data manipulations within the scope of the transmission. In order to be effectively covered against liability risks, appropriate measures have to be taken.

Industry Standards

Over time, a large number of industry standards for the exchange of data has been developed. One of the best known examples for the specific exchange of data is EDIFact. This standard communication is used to realise a large part of the data exchanges in the industrial, service and commercial sectors. Standard systems such as ERP by SAP, but also less commonly used commercial applications provide an EDIFact interface for export and import. The implementation of new EDIFact interfaces requires relatively sophisticated expert knowledge as well as some effort. Also, EDIFact is hardly readable on the part of the user. EDIFact is for example used to exchange personal data in case of a switch from one power supplier to another.[132]

The same applies in the case of DATANORM. This format is used to transmit article information. DATANORM is highly generic and thus flexible, and it offers a broad range of functionalities. However, this standard, too, is hardly suitable for the extensive requirements of data portability.

In the field of medical informatics, the standard HL7 has become the established solution. However, this standard, as well, is subject to the above-mentioned limitations in terms of a cross-sectoral portability.

These three examples show how application- and/or industry-specific exchange standards have developed.

130 ibid.

131 See also WP 242 Guidelines on the right to data portability. Adopted on 13 December 2016. As last revised and adopted on 5 April 2017. 2017. Article 29 Data Protection Working Party, WP 242, rev.01, http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (access: 2017-07-31).

132 See also statement by Klemens Gutmann., see Section D.

The XML standard (Extensible Mark-up Language) has a more general relevance. The advantages of this standard are:

- Widely spread industrial standard
- Used by many IT solutions, platform-spanning, flexible and easily expandable
- Basis for modern transmission technologies such as web services
- Allows for quick reactions to legal requirements
- Standardisation avoids individual solutions
- Even deeply nested layers can be read with relative ease
- XSLT is available for conversion into different formats.

XML has the advantage that this technology can deliver data as well as the corresponding metadata for the description of the data, for plausibilities and further processing. This way, the data description is automatically included in the delivered exchange format. Moreover, data in XML format can easily be displayed in a readable way, e.g. by means of MS EXCEL or any editor. In connection with web services, XML is extremely well-suited for the communication between different systems. Of course, this technology does not eliminate the need for a definition which data shall be transmitted at all – this applies to all exchange formats.

Lately, JSON (JavaScript Object Notation) is being used more and more. It offers relatively easy readability for humans

- Simple, minimalist syntax
- Low data volume
- More suitable for AJAX applications
- Supports a large number of programming languages
- Less suitable for documents and media data

Generally speaking, both XML and JSON are open interface technologies which fulfil the requirements for interoperability.

Conclusion

The minimum requirement for data portability and/or interoperability is to write the data in the CSV format and to add a simple description of how the data is arranged in the file. This description has to indicate which data contents can be found at which position inside the file (surname, first name, date of birth, etc.) and, if applicable, what certain codings mean. For more complex solutions, XML or JSON would be suitable. Both standards fulfil the requirements regarding machine-readability as well as interoperability. They contain the data as well as descriptive metadata and have sufficient depth due to their structure so that they are able to represent even complex data structures. Finally, the necessity to encrypt data is essential, as well. This also includes the integrity and confidentiality of the data, which have to be ensured by means of suitable technical and organisational measures.

II. Recommendations for Action

1. Objectives of the Regulation

- The regulation should be implemented in line with its original intention – the improvement of data privacy ("informational self-determination") for the consumers. This refers primarily to possibilities of control over the transmission of personal data.

- The right to data portability has to include at least such data whose portability actually supports informational self-determination and which can correspondingly be utilised by the users. The efforts and expenses required for the implementation of the regulation have to be proportionate, also with regard to the consumers' data sovereignty.

- The effectiveness of the regulation has to be tested in practice. This includes for example behavioural economic surveys examining the actual willingness of the users to make use of data portability options. The results should be taken into account in the evaluation of the EU General Data Protection Regulation.

- The introduction of the right to data portability should be accompanied by information campaigns regarding its scope and possibilities (e.g. by national data protection authorities or through information platforms).

2. Determination of the Scope of Application

- The determination of the scope of application should focus on the consumer benefits in order to increase acceptance and success of the new right.

- The definition of "data provided" should be based on the spirit and purpose of the regulation.

- Apart from the statement of the Article 29 Working Party, the regulatory authorities should specify what “data provided” means exactly and give examples for the data categories included under this term.

- The question whether the scope of application could include inventory data as well as usage data should be answered based on each individual case and on the respective service. It has to be examined, in which cases the transfer of “provided” usage data to another service provider would actually support the control rights of the person concerned.

- With respect to the data format and the requested interoperability, issues of competition law have to be taken into account. It has to be examined, to what extent criteria have to be developed in order to achieve a consistent perspective across Europe as well as a differentiated result with respect to competition law and data protection law. Antitrust issues with respect to agreements on methods for data transfer have to be avoided. The protective purpose of the regulation, i.e. to facilitate a switch from one provider to another, has to be realised in an effective way.

- In case of data processing by an individual person exclusively for personal or family purposes, it has to be taken into account with regard to third-party protection rights whether personal data are transmitted to a commercial provider or if they are processed on their own private devices. In this regard, rules of conduct have to be elaborated indicating to what extent further processing by commercial providers due to legitimate interests or a change of purpose would be actually ruled out in the future.

- It is advisable to check whether there is a consistent technical and legal understanding of the term “metadata”. This is particularly relevant in order to decide which metadata are required for the successful implementation of data portability as well as for the development of a format from a technical point of view and which are permissible from a legal point of view.

- All of the involved parties should always ensure transparency when the right to data portability is exercised. The respective concerned persons should not lose track of the data controllers and the rights of erasure they are entitled to. They have to know all of the information relating to the processing by the old and the new controller.

- With regard to the request “where technically feasible”, it has to be decided whether objective criteria can be developed or if the individual capacities of the respective data controller (subjective standard) are taken as a basis.

- It is also important to strive for a harmonisation and consistent interpretation across all of Europe in construing Art. 20 GDPR as well as in the elaboration of rules of conduct according to Art. 40 GDPR.

3. Implementation Strategies

- It is advisable to develop approaches of "regulated self-regulation" establishing a framework under state supervision within which regulatory authorities, NGOs as well as companies develop implementation strategies and standards for data portability.

- For an effective definition and arrangement of data portability and realisation of legal compliance, companies and industries which will be particularly affected should be involved in formal consultation processes of the regulatory authorities.

- In case of the transfer of sector-specific data sets within one category of controllers and in cases where there are already existing internal portability solutions within the industry, an industry-specific procedure is recommended.

- Solution approaches based on Personal Information Management Systems (PIMS) seem very promising for cross-sectoral application cases.

- In cases in which a low demand for data transfers is to be expected, individual solutions for the direct transfer of data sets could be applied.

- In order to allow for better orientation, the responsible bodies should work towards rules of conduct for the practical implementation of portability (Art. 40 GDPR).

4. Technical Realisation

- The minimum requirement for data portability and interoperability should be the use of the CSV format. To this, a simple description of how the data is arranged in the file has to be added.

- For more complex solutions, the formats XML or JSON should be used. These formats allow for finer granularity levels, contain content data as well as describing metadata and have sufficient depth due to their structure so that they are able to represent even complex data structures. The information contained in these files is not only machine-readable but it can also be read by the persons concerned themselves using standard software, which at the same time supports the users' exercise of their information rights.

- The data protection authorities should define which specific requirements are imposed with regard to authentication in order to avoid legal uncertainties for the controllers as well as risks for the persons concerned.

- It has to be made sure for individual solutions as well as for industry-specific or cross-sectoral and universal approaches that the technical solutions are as a matter of principle made interoperable with each other by means of open interfaces.

- With regard to the efficient reuse of the transferred data, the PDF format should not be used as a standard in the field of data portability, even if it is sufficient as an electronic format within the scope of the right of access with respect to transparent information.

D. Anlagen / Annexes

Haftungsausschluss
Beiträge und Stellungnahmen in diesem Abschnitt sind eigenständige Werke der einreichenden Person/ Institution und geben alleine deren Auffassung wieder.

Disclaimer
Any papers and statements cited in this section are independent works of the submitting person(s)/ institution and only reflect their own opinions.

D. Anlagen / Annexes

bitkom

Umsetzung Datenportabilität

Call for Papers – Stiftung Datenschutz

04.10.2017

Seite 1

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon gut 1.700 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Ab 25. Mai 2018 wird mit der neuen Datenschutzgrundverordnung ein neues Rechtsinstrument eingeführt: Das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO). Die DS-GVO führt damit ein Recht ein, welches es jeder Person ermöglicht, „die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten".

Die Stiftung Datenschutz untersucht die Möglichkeiten zur praktischen Umsetzung des Rechts zur Datenportabilität. Ziel ist es, Empfehlungen für eine Standardisierung in der Praxis zu geben. Die Stiftung Datenschutz bat im Rahmen dieser Untersuchung um Vorschläge in Form von Konzepten, Stellungnahmen, Gutachten oder Forderungskatalogen. Bitkom bedankt sich für diese Möglichkeit und nimmt zu den Fragestellungen wie folgt Stellung:

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Rebekka Weiß
Referentin Datenschutz & Verbraucherrecht
T +49 30 27576-161
r.weiss@bitkom.org

Martina Krauss
Referentin Europäische Wirtschaftspolitik
P +32 2 60953-16
m.krauss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

www.bitkom.org

bitkom

Stellungnahme
Umsetzung Datenportabilität

Inhalt

Seite

bitkom

Stellungnahme
Umsetzung Datenportabilität

I. Allgemeine Fragen

1. Wie eng oder weit ist das Merkmal des „Bereitstellens von Daten“ zu verstehen?

Bei den Daten, die durch die Nutzung eines Dienstes oder Produkts entstehen, stellt sich die Frage, ob hiermit nur die Daten gemeint sind, die auch für die Funktionalität des Dienstes relevant sind und daher eben auch für einen möglichen Anbieterwechsel eine Rolle spielen oder ob ebenfalls z.B. als Nebenprodukt entstehende Daten (wie z.B. Log Files und Verkehrsdaten) umfasst sein sollen. Da der Begriff des Bereitstellens in der DS-GVO nicht legal definiert ist, lässt sich der Begriff nur interpretieren:

Der Wortlaut von Art. 20 DS-GVO sollte die Grundlage für die Auslegung des Rechts auf Datenübertragbarkeit sein. Darüber hinaus darf das Recht auf Datenübertragbarkeit nicht isoliert von anderen Vorschriften der DS-GVO betrachtet werden, sondern ist systematisch im Zusammenhang mit und in Abgrenzung zu anderen Rechten zu interpretieren: Datenübertragbarkeit tritt in der DS-GVO neben andere Betroffenenrechte auf Information, Auskunft, Berichtigung und Löschung. In diesem Zusammenhang hat der Gesetzgeber sich ganz bewusst für einen anderen Wortlaut in Art. 20 entschieden und den Umfang des Rechts auf Datenübertragbarkeit auf Daten begrenzt, die eine betroffene Person einem Verantwortlichen „bereitgestellt hat”. Im Gegensatz dazu sind andere Betroffenenrechte wie beispielsweise das Auskunftsrecht nach Art. 15 weiter formuliert und umfassen alle personenbezogenen Daten, die vom Verantwortlichen über die betroffene Person „verarbeitet werden”. Jede weitergehende Interpretation widerspricht dieser Einschränkung und berührt das ausgewogene Verhältnis der DS-GVO zwischen den Rechten betroffener Personen, Verantwortlicher und Dritter.

Darüber hinaus sollten auch Sinn und Zweck der gesetzlichen Vorschrift bei der Interpretation miteinbezogen werden: Wenn man das Portabilitätsrecht wie es die EU-Kommission beschrieben hat als „Recht [des Betroffenen versteht], seine Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System zu übertragen, ohne dass der für die Verarbeitung Verantwortliche ihn daran hindern kann“ , reicht es aus, dass der Betroffene **nur diejenigen Daten transportiert bekommt, die er benötigt, um einen neuen Dienst sinnvoll weiternutzen zu können**. Der Schwerpunkt sollte also auf Daten liegen, die eng mit der Dienstleistung (vom Verantwortlichen A) verknüpft sind und notwendig sind, um den Service (von Verantwortlichen B) nützlich zu machen. Alle anderen Daten werden bereits durch andere Betroffenenrechte adressiert. Die WP29 benennt in ihren „Guidelines on the right to data portability“ z.B. die Playlist beim Streaming Service und die Leistungsaufzeichnung beim Fitnessarmband – beides gehört wohl unzweifelhaft zum Service. Da Art. 20 DS-GVO verschiedene Branchen und

Stellungnahme
Umsetzung Datenportabilität

Geschäftsmodelle betrifft, wird dies von Fall zu Fall unterschiedlich sein und die Abgrenzung mal leichter und mal schwerer fallen. Sachfremde Erwägungen wie „die Stärkung des Wettbewerbs" oder die „Förderung der Entwicklung neuer Dienstleistungen" aus dem Arbeitspapier der WP29 finden sich dagegen weder in den Erwägungsgründen wieder noch lassen sie sich datenschutzrechtlich begründen. Zwar stützt sich die DS-GVO im Grundsatz neben dem Schutz natürlicher Personen (Erw.9 DS-GVO) auch auf den „freien Verkehr von personenbezogenen Daten". Allerdings soll dieser gemäß Erw.13 DS-GVO durch die EU-weite Harmonisierung der Datenschutzvorschriften erfolgen, die wiederum zu mehr Rechtssicherheit und Transparenz für Wirtschaftsteilnehmer führen soll. Dies soll zur Stärkung des digitalen Binnenmarktes führen.

Das Recht auf Datenübertragbarkeit ist nicht schrankenlos. Eine enge Auslegung würde verhindern, dass geistiges Eigentum und Geschäftsgeheimnisse sowie die Rechte und Freiheiten Dritter tangiert werden. Dies entspricht dem Rechtsgedanken des Art. 20 Abs. 4 DS-GVO, der vorschreibt, dass durch die Rechteausübung nach Art. 20 Abs. 1 DS-GVO die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden dürfen. [1]

Ergebnis: Wenn man miteinbezieht, dass der Gesetzgeber sich ganz bewusst für den Wortlaut „bereitgestellt" entschieden hat in Abgrenzung zum Wortlaut „verarbeitet", sollte es ausreichend sein 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 schließt Nutzungsdaten aus. Insbesondere sollten keine Daten unter das Recht fallen, die bei Nutzung des Dienstes automatisch generiert werden (z.B. Logfiles, Verkehrsdaten).

2. Ist die neue Norm geeignet, für die Verbraucherinnen und Verbraucher ein echtes Mehr an informationeller Selbstbestimmung zu schaffen?

Wenn man Art. 20 DS-GVO so interpretiert, dass dessen Ziel darin sieht, dass es einer natürlichen Person erleichtert werden soll, durch einen elektronischen Datentransfer den

[1] Der Art. 20 Abs. 4 DS-GVO nimmt dem Wortlaut nach in der deutschen Fassung der DS-GVO lediglich den Abs. 2, die direkte Übertragung der Betroffenen-Daten von einem Verantwortlichen zum anderen, in Bezug. Es handelt sich dabei, wie auch ein Vergleich mit anderssprachigen Fassungen der DS-GVO zeigt, um ein Redaktionsversehen. So heißt es beispielsweise in der englischen General Data Protection Regulation in Article 20(4): „The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others." Und auch in der französischen Règlement Général sur la Protection des Données: „Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés de tiers." Artikel 20 Abs. 4 DS-GVO bezieht sich daher also auf das Recht zur Datenübertragung aus Art. 20 Abs. 1 DS-GVO, sodass auch bei der Datenübertragung an den Betroffenen die Einschränkung des Absatz 4 beachtet werden muss und die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden dürfen. Diese Interpretation wird auch gestützt von Erwägungsgrund 68, der „das Recht auf Empfang" der Daten, und damit das Recht nach Absatz 1, in Bezug nimmt und klarstellt, dass dieses Recht die Grundrechte und Grundfreiheiten anderer betroffener Personen unberührt lässt.

Anbieter zu wechseln, sieht der Bitkom ein Mehr an informationeller Selbstbestimmung.

II. Technikbezogene Fragen

1. Inwieweit bestehen Vorteile branchenspezifischer Formate gegenüber sektorübergreifenden Formaten?

Das Recht auf Datenübertragbarkeit bringt nicht nur eine Reihe von Fragen bezüglich der Auslegung mit sich, sondern stellt die datenverarbeitende Wirtschaft auch vor praktische Herausforderungen. So müssen gemeinsame Standards und interoperable Systeme erst noch geschaffen werden, die eine leichte Ausübung des Rechts für den Betroffenen ermöglichen. Dabei wird man durch die unterschiedlichen Branchen, die betroffen sind, nicht auf eine Einheitslösung wie APIs abstellen können. Die Entwicklung technischer Standards ist ein komplexer Prozess, der von vielen Beteiligten, einschließlich Aufsichtsbehörden und öffentlichen Stellen, viel Zeit und Arbeit erfordert. Zum Zeitpunkt des Inkrafttretens der Verordnung werden diese Standards noch nicht vorliegen.

Im Allgemeinen werden Standards innerhalb bestimmter Bereiche wie Banken, Telekommunikation, Gesundheitswesen, Transport oder Einzelhandel entwickelt werden müssen. Der Vorteil des Datenportabilitätsrechts liegt nicht nur in der einfachen Datenübertragung, sondern darin, die Daten, die übertragen werden, tatsächlich in einem neuen Dienst nutzen zu können. Sinn und Zweck der Vorschrift sollten hier daher Beachtung finden. Die gezwungene Entwicklung sektorübergreifender Standards würde dem Grundsatz der Verhältnismäßigkeit widersprechen, da sie sowohl eine übermäßige Belastung für Unternehmen darstellt als auch in den meisten Fällen technisch nicht realisierbar ist. Es ist auch nicht notwendig, um der betroffenen Person einen Anbieterwechsel zu ermöglichen.

2. Ergebnis

Die Branchen sollten dazu ermutigt werden (z.B. von der WP29), Standards und Formate zu entwickeln, die es dem Betroffenen ermöglichen seine einmal bereitgestellten Daten mittels des Rechts auf Datenübertragbarkeit zu einem anderen Anbieter „mitzunehmen" und „wiederzuverwenden", um den Anbieterwechsel innerhalb eines Sektors zu erleichtern.

III. Abgrenzung zwischen bereitgestellten und verarbeiteten Daten

1. Einführung

Kundendaten werden in den meisten Unternehmen einer Anreicherung und/oder Weiterverarbeitung unterzogen. Dies umfasst unter anderem eine Vervollständigung (fehlende Daten, Rechtschreibüberprüfung, Verifizierung Kontodaten, o.ä.), Verbindung mit Infrastruktur-, Netz- und Geodaten (z.B. bei TK, Energie, Logistik), eine Weiterverarbeitung in aggregierte Berechnungen (Ressourcenplanung, Erwartungswertes etc.), ein Verbuchen und „Wegspeichern" (z.B. für Abrechnungszwecke, Vorratsdatenspeicherungspflichten etc.) und u.U. Kommunikation von Daten an relevante Branchen-/Marktpartner.

2. (Wo) Sollte eine Grenze zwischen bereitgestellten Kundendaten und weiterverarbeiteten Daten zu ziehen sein? Ist diese Grenze scharf oder eher diffus? Wie würden Sie diese Grenze beschreiben?

Die Abgrenzung von bereitgestellten Daten zu sonstigen Daten ist schwierig, da sich in der Verordnung keine Legaldefinition des Bereitstellens findet. Die WP29 unterscheidet hier zunächst zwischen wissentlich und aktiv bereitgestellten Daten wie z.B. Bestandsdaten (Account Data wie E-Mail Adresse, Nutzername, Alter), die durch Online-Formulare eingegeben werden und zwischen Daten, die durch den Nutzer z.B. durch Nutzung eines Dienstes oder Produkts erzeugt und vom Verantwortlichen gesammelt werden wie z.B. die Rohdaten, die ein Smart Meter erfasst. Beides fällt laut WP29 unter den Begriff „bereit gestellt". Nicht bereit gestellt sind laut WP29 jedoch solche Daten, die vom Verantwortlichen selbst erzeugt werden wie z.B. ein Nutzerprofil, das durch die Analyse der von einem Smart Meter gesammelten Rohdaten gewonnen wurde.

Die WP29 nennt als weiteres Beispiel für „bereit gestellte" Daten die Suchhistorie einer Person, Verkehrs- und Standortdaten („observed data").

Nicht bereitgestellt, sondern „abgeleitete" („inferred" or „derived") Daten sind solche, die vom Verantwortlichen aus bereitgestellten Daten abgeleitet wurden z.B. ein Credit Score oder das Ergebnis einer Gesundheitsprüfung. Solche Daten sollen nicht unter das neue Datenportabilitätsrecht fallen.

Bei den Daten, die durch die Nutzung eines Dienstes oder Produkts entstehen, stellt sich die Frage, ob hiermit nur die Daten gemeint sind, die auch für die Funktionalität des

Dienstes relevant sind und daher eben auch für einen möglichen Anbieterwechsel eine Rolle spielen oder ob ebenfalls z.B. als Nebenprodukt entstehende Daten (wie z.B. Log Files und Verkehrsdaten) umfasst sein sollen.

Da der Begriff des Bereitstellens in der DS-GVO nicht legal definiert ist, lässt sich der Begriff nur interpretieren. Dabei sollten die in 1. gemachten Überlegungen berücksichtigt werden. Wenn man miteinbezieht, dass der Gesetzgeber sich ganz bewusst für den Wortlaut „bereitgestellt" entschieden hat in Abgrenzung zum Wortlaut „verarbeitet", sollte es ausreichend sein 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 schließt Nutzungsdaten aus. Insbesondere sollten keine Daten unter das Recht fallen, die bei Nutzung des Dienstes automatisch generiert werden (z.B. Logfiles, Verkehrsdaten).

3. Veranschaulichung am Beispiel zu Verkehrs- und Standortdaten

Sinn und Zweck der Norm

- Nicht erforderlich, um den Dienst auch für die Zukunft bei einem Dritten zu beziehen
- Wenn überhaupt, kann nur die Nummer des B-Teilnehmers als vom A-Teilnehmer „bereitgestellt" angesehen werden, der er diese „gewählt" hat;

Bereitgestellt durch den Betroffenen

- Verkehrs- und Standortdaten werden nicht von Nutzer bereitgestellt; dieser initiiert allein den Kommunikationsvorgang
- Verkehrs- und Standortdaten fallen erst im Rahmen der Signalisierung innerhalb des TK-Netzes an; insbesondere Standortdaten beziehen sich auch nur auf Standorte von TK-Anlagen/-Linien (Mobilfunk-Antennen)
- Verkehrs- und Standortdaten fallen als Folge standardisierter Protokolle an und hängen nicht am Willen der Beteiligten

Verarbeitung auf der Grundlage einer Einwilligung/des Vertrages

- Erhebung von Verkehrs- und Standortdaten erfolgt – auch unter hypothetischer Geltung der e-Privacy-Verordnung – allein auf der Grundlage spezifischer Erlaubnistatbestände und nicht auf der Grundlage eines Vertrages oder gar einer Einwilligung; das mag dort anders sein, wo erhobene Daten auf Grundlage einer Einwilligung für weitere Zwecke verarbeitet werden dürfen. Aber auch in diesen Fällen beruht die Erhebung der Daten auf gesetzlichen Erlaubnistatbeständen und fällt daher nicht in den Anwendungsbereich der Norm.

Betriebs- und Geschäftsgeheimnisse sowie Rechte Dritter

- Wenn überhaupt, dann wird nur die Nummer des B-Teilnehmers vom A-Teilnehmer „bereitgestellt"; und gerade im Hinblick auf diese gelten kollidierende Interessen des B-Teilnehmers; somit wären diese Informationen gemäß Art. 20 Abs. 4 DS-GVO von der Datenübertragung ausgeschlossen.

Entgegenstehende Rechtsnormen

- Kollision mit den (abschließenden) Erlaubnisnormen des TKG/ePR-V

- Konterkariert z.B. die engen Voraussetzungen, unter denen ein EVN erstellt werden muss und darf

Ergebnis:

Der Bitkom vertritt daher die Auffassung, dass Verkehrs- und Standortdaten aus dem Anwendungsbereich des Art. 20 DS-GVO fallen.

4. Veranschaulichung am Beispiel zu Daten von Arbeitnehmern

Sinn und Zweck der Norm

- In vielen Fällen nicht erforderlich, um den Dienst auch für die Zukunft bei einem Dritten zu beziehen

Verarbeitung auf der Grundlage einer Einwilligung/des Vertrages

- Auf Basis der Einwilligung werden nur die Daten verarbeitet, die nicht für die Durchführung des Arbeitsverhältnisses erforderlich sind (z.B. freiwilliges

Stellungnahme
Umsetzung Datenportabilität

Bonusprogramm? Private Handynutzung?), da die Daten vor allem in Bezug auf die Abwicklung und Administration des Arbeitsverhältnisses anfallen und in diesem Zusammenhang verarbeitet werden (Personalakte, HR-Systeme). Da der Anwendungsbereich für Einwilligungen im Arbeitsverhältnis sehr eng ist, wird der Großteil der im Arbeitsverhältnis verarbeiteten Daten auf Basis des Art. 6 Abs.1 lit. b) oder c) DS-GVO erfolgen.

Ausnahme öffentlich-rechtlicher Vorschriften nach Art. 20 Abs. 3 S.2 DS-GVO

• Art. 20 Abs. 3 Satz 2 DSGVO ist geeignet, die Anwendbarkeit bei Arbeitnehmern um die Daten zu reduzieren, die der Arbeitgeber zwar in der Regel direkt vom Arbeitnehmer erhält, aber die er in Umsetzung öffentlich-rechtlicher Vorschriften, die im öffentlichen Interesse liegen, verarbeitet.

Ergebnis:

Der Bitkom vertritt daher die Auffassung, dass Daten von Arbeitnehmern daher aus dem Anwendungsbereich des Art. 20 DS-GVO fallen.

Recht auf Datenübertragbarkeit nach Art. 20 Datenschutz-Grundverordnung (DS-GVO) aus Sicht der Inkassobranche

BDIU – Bundesverband Deutscher Inkasso-Unternehmen e.V.[1]

I. Allgemeines zum intendierten Anwendungsbereich des Art. 20 DS-GVO

Gemäß Art. 20 der Europäischen Datenschutz-Grundverordnung (DS-GVO)[2] kann die betroffene Person verlangen, dass ihre personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format erhält. Weiter hat sie das Recht, dass der Verantwortliche diese Daten einem anderen Verantwortlichen übermittelt. Dies gilt auch, wenn die Verarbeitung auf einem Vertrag gemäß Art. 6 Abs. 1 Buchstabe b DS-GVO beruht.

Sinn und Zweck sowie Hintergrund der Vorschrift ist, dass mit diesem Recht der betroffenen Person ein leichterer Wechsel zwischen sozialen Netzwerken, E-Mail- und anderen Cloud-Diensten ermöglicht werden soll. Die Vorschrift soll in diesem Bereich zu einer Stärkung des Wettbewerbs führen und die Betroffenen dadurch veranlassen, öfter datenschutzfreundliche Dienste zu wählen.[3]

Das Augenmerk lag im Gesetzgebungsverfahren bei Schaffung der Vorschrift auf Facebook & Co. – nicht auf allen europäischen Unternehmen, die ebenfalls Verantwortliche im Sinne der DS-GVO sind und nunmehr bei Vorliegen der gesetzlichen Voraussetzungen die Anforderungen beachten müssen. Der Europäische Rat hatte eine Begrenzung des Anwendungsbereichs auf Plattformanbieter im Internet oder von Apps vorgesehen, um das Recht nach Art. 20 DS-GVO auf Internet-bezogene Sachverhalte einzuschränken. Einige Delegationen im Rat wollten dazu sogar noch einschränkend das Recht auf Datenübertragbarkeit allein auf Angebote sozialer Medien im Internet begrenzen.[4] Die Europäische Kommission nannte als Beispiele, für die das Recht auf Datenübertragbarkeit gelten soll, Freundeslisten oder Fotos.[5]

II. Tätigkeiten von Inkassodienstleistern im Bereich des Forderungsmanagements und deren Betroffenheit bzgl. Art. 20 DS-GVO

1. Begriff der Inkassodienstleistung

Die Inkassodienstleistung ist eine Rechtsdienstleistung und ist gemäß der Legaldefinition in § 2 Abs. 2 des Rechtsdienstleistungsgesetzes (RDG)[6] „die Einziehung fremder oder zum Zweck der Einziehung auf fremde Rechnung abgetretener Forderungen, wenn die Forderungseinziehung als eigenständiges Geschäft betrieben wird“.

---

[1] Seit 1956 vertritt der Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU) die Interessen der Inkassobranche gegenüber der Öffentlichkeit und der Politik. Der BDIU ist mit rund 560 Mitgliedern der größte Inkassoverband in Europa und der zweitgrößte weltweit. Mehr Informationen unter: www.inkasso.de.

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1.

[3] Vgl. Albrecht / Jotzo, Das neue Datenschutzrecht der EU, 2017, S. 87.

[4] *Piltz* in Gola, DS-GVO – Datenschutz-Grundverordnung VO (EU) 2016/679, 2017, Art. 20, Rn. 6.

[5] *Piltz* aaO, Rn. 18.

[6] Rechtsdienstleistungsgesetz vom 12. Dezember 2007 (BGBl. I S. 2840), das zuletzt durch Artikel 6 des Gesetzes vom 12. Mai 2017 (BGBl. I S. 1121) geändert worden ist.

Inkassodienstleister[7] machen im Rahmen des Forderungsmanagements für Ihre Mandanten, die Forderungsgläubiger, Forderungen gegenüber säumigen Schuldnern geltend. Sie sind dabei sowohl vorgerichtlich tätig, indem sie z.B. Zahlungsaufforderungen versenden oder Telefonate mit den Forderungsschuldnern führen, ggf. Ratenzahlungsvereinbarungen mit diesen treffen, als auch zur Titulierung im Rahmen des gerichtlichen Mahnverfahrens berechtigt, ebenso zu Maßnahmen im Rahmen der Zwangsvollstreckung in das bewegliche Vermögen wegen Geldforderungen.[8] Weitergehende Vertretungsberechtigungen ergeben sich zudem aus der Insolvenzordnung (InsO).[9]

Inkassodienstleister werden dabei als „Verantwortliche" im Sinne der DS-GVO bei der Datenverarbeitung tätig, da sie nach wie vor (wie nach jetzigem deutschen Recht) über die Zwecke und Mittel der Verarbeitung personenbezogener Daten selbstständig entscheiden (Art. 4 Nr. 7 DS-GVO).

2. Datenverarbeitungen bei Inkassodienstleistungen

Zwecks Vertragsabwicklung bzw. Rechtsverfolgung erhalten die Inkassodienstleister von den Forderungsgläubigern die (personenbezogenen) Daten, die diese zuvor von deren Kunden/Schuldnern zu gleichen Zwecken erhalten haben. Dazu zählen Kommunikations-, Vertrags- und Forderungsdaten sowie ggf. weitere Zahlungsinformationen, die zur weiteren Geltendmachung der Forderung durch das Inkassounternehmen erforderlich sind.

Diese Daten erhalten die Inkassodienstleister von ihren Auftraggebern, den Forderungsgläubigern, auf ganz unterschiedlichen Wegen. Kommt es zu regelmäßigen Forderungsübergaben, z.B. von einem großen Mobilfunkanbieter bzgl. ausstehender Forderungen aus einzelnen Monatsabrechnungen, dann werden die zum Forderungseinzug durch den Inkassodienstleister erforderlichen Daten über extra dafür eingerichtete Schnittstellen vom Forderungsgläubiger an den Inkassodienstleister übermittelt. Im umgekehrten Extremfall kann es – wenn z.B. eine einzelne Forderung eines Handwerkers nicht beglichen wurde und diese Forderung von einem auch kleinen Inkassodienstleister eingezogen werden soll – zur „händischen" Übergabe vom Auftrag gebenden Handwerker an den Inkassodienstleister kommen.

Der Unterschied zu vielen anderen Branchen, z.B. zum Versandhandel oder Energieversorgern, besteht demnach darin, dass Inkassodienstleister grundsätzlich von ihrem Auftraggeber Daten mit Bezug zu dessen Kunden/Schuldner übermittelt bekommen, um die weitere Forderungseinziehung gegen diesen zu betreiben.

Die zum Zweck der Vertragsabwicklung bzw. Rechtsverfolgung sowie zum Zweck des Forderungsmanagements beim Inkassodienstleister in der Folge gespeicherten Daten werden zur Erfüllung der Inkassodienstleistungen im Weiteren verarbeitet.[10]

Einen Großteil der von den Inkassodienstleistern einzuziehenden Forderungen bilden solche aus Vertragsverhältnissen zwischen dem Forderungsgläubiger und dem Forderungsschuldner. Rechtsgrundlage für die diesbezüglichen Datenverarbeitungen

---

[7] Das sind nur solche Unternehmen, die gemäß §§ 10, 12, 13 RDG als Inkassodienstleister im Rechtsdienstleistungsregister registriert sind (www.rechtsdienstleistungsregister.de).

[8] Die erwähnten Vertretungsbefugnisse ergeben sich aus § 79 Abs. 2, Nr. 4 der Zivilprozessordnung (ZPO).

[9] Z.B. aus § 174 Abs. 1, S. 3 InsO.

[10] Weitere Ausführungen zu den Datenverarbeitungen der Inkassodienstleister liefert *Plath*, White Paper zu den Anforderungen der DSGVO an die Tätigkeit von Inkassodienstleistern, Juli 2017 (http://inkasso.de/sites/default/files/downloads/BDIU%20DSGVO-WHITE%20PAPER.pdf).

personenbezogener Daten beim Inkassodienstleister ist Art. 6 Abs. 1 Buchstabe b DS-GVO. Für den Einzug von gesetzlich entstandenen Forderungen, z.B. von Schadensersatzansprüchen aus Delikt, bildet künftig Art. 6 Abs. 1 Buchstabe f DS-GVO die Rechtsgrundlage.[11]

Insoweit besteht – nicht nur, weil Rechtsdienstleistungen erbracht werden, sondern auch bzgl. der Art und Weise der Verarbeitung von personenbezogenen Daten – eine Vergleichbarkeit mit der Tätigkeit von Rechtsanwälten, die ebenfalls zur Mandatsbearbeitung, somit auch teilweise auch zur Forderungseinziehung, die dafür erforderlichen Daten von ihren Mandanten übermittelt bekommen und im Weiteren verarbeiten.

3. Betroffenheit der Inkassobranche bzgl. Art. 20 DS-GVO und Umfang des Merkmals „Bereitstellen von Daten“

3.1. Betroffenheit der Inkassobranche

Im Folgenden wird aufgezeigt, inwiefern Art. 20 DS-GVO für die Inkassobranche von Relevanz wäre.

Im Regelfall ist die Inkassobranche in den Fällen, in denen es sich bei den betroffenen Personen um Forderungsschuldner handelt, nicht von Art. 20 DS-GVO betroffen, da die Daten zur Erfüllung der Inkassodienstleistungen zum Großteil vom Auftraggeber stammen.

Eine Betroffenheit wird aber in den Fällen vorliegen, bei denen nach Übergabe der – vertraglich entstandenen und damit der Rechtsgrundlage des Art. 6 Abs. 1 Buchstabe b DS-GVO unterfallenden – Forderungen (nebst entsprechend erforderlicher Daten) vom Forderungsgläubiger der Inkassodienstleister im weiteren Inkassoverfahren weitere personenbezogene Daten direkt von der betroffenen Person, dem Forderungsschuldner, erhält.

Das ist zum Beispiel dann gegeben, wenn der Schuldner im Rahmen eines Telefonats dem Inkassodienstleister z.B. eine Adress- oder Namensänderung mitteilt. In diesem letzten Fall könnte – folgt man dem Wortlaut der Vorschrift – ein „Bereitstellen“ im Sinne des Art 20 Abs. 1 DS-GVO angenommen werden, so dass diesbezüglich eigentlich eine branchenspezifische Betroffenheit vorläge.

Grundsätzlich ist es zu begrüßen, dass die betroffene Person Transparenz und Mitwirkungsmöglichkeit bei sie betreffenden Datenverarbeitungen erlangen kann. Das Recht auf Datenübertragbarkeit aus Art. 20 DS-GVO bringt allerdings – bezogen auf den Bereich der Inkassodienstleistungen – keinen dahingehenden Mehrwert für die betroffene Person, auch kein Mehr an informationeller Selbstbestimmung für diese, hingegen nicht abschätzbaren und erheblichen Aufwand für die einzelnen Inkassodienstleister:

Eine nur teilweise Übermittlung der personenbezogenen Daten, nämlich solcher, die der Forderungsschuldner als betroffene Person direkt dem Inkassodienstleister mitgeteilt und damit „bereitgestellt“ hat, ist nicht für den Forderungsschuldner sinnvoll. Er würde gemäß Art. 20 DS-GVO nur Bruchstücke der personenbezogenen Daten erhalten, die der Inkassodienstleister von ihm verarbeitet, so – um auf die erwähnten Beispiele zurückzugreifen – die aktualisierte Adresse oder der aktualisierte Name, die der

[11] Weitere Ausführungen bzgl. der Umsetzung der DS-GVO-Vorgaben bei Inkassodienstleistern sind hier zu finden: *Plath*, White Paper zu den Anforderungen der DSGVO an die Tätigkeit von Inkassodienstleistern, Juli 2017 (http://inkasso.de/sites/default/files/downloads/BDIU%20DSGVO-WHITE%20PAPER.pdf); BDIU, Die Europäische Datenschutz-Grundverordnung – Best Practice Guide 1.0 – Leitfaden für den Bereich Forderungsmanagement, Februar 2017 (http://inkasso.de/sites/default/files/downloads/DS-GVO-Leitfaden.pdf).

Forderungsschuldner dem Inkassodienstleister bei vorheriger Kommunikation selbst mitgeteilt hat.

Diese bruchstückhaften Informationen dem Forderungsschuldner als betroffener Person oder einem anderen Verantwortlichen (theoretisch kämen nach dem Wortlaut alle Verantwortliche gemäß der DS-GVO in Betracht) in einem „strukturierten, gängigen und maschinenlesbaren Format“ zu übermitteln, brächte weder einen Transparenz- noch einen Kontrollgewinn[12] für die betroffene Person. Zudem ist bislang keine Konstellation ersichtlich, in der es einen Sinn hätte, diese Daten in das Verarbeitungssystem eines anderen Verantwortlichen zu übertragen.

Möchte der Forderungsschuldner als betroffene Person einen Gesamtüberblick über die Datenverarbeitungen beim Inkassodienstleister erhalten, kann er sein Auskunftsrecht nach Art. 15 DS-GVO nutzen. Die Auskunft muss dann im Regelfall auf den bislang gängigen Kommunikationswegen vom Inkassodienstleister als Verantwortlichen erteilt werden.

Dies ist für ihn viel effektiver als der „Ausschnitt“ der personenbezogenen Daten, die ihm über Art. 20 DS-GVO zur Verfügung gestellt werden müsste.

3.2. Umfang des Merkmals „Bereitstellen von Daten“

Das Merkmal „Bereitstellen von Daten“ ist gemäß seinem Wortlaut und in der Zusammenschau mit Art. 15 DS-GVO so zu verstehen, dass es sich dabei nur um die Daten handeln kann, die die betroffene Person selbst dem Verantwortlichen zur Verfügung gestellt hat.[13]

Würde der Begriff des „Bereitstellens“ ausgeweitet werden bzw. angenommen, dass im Fall dass der betroffenen Person ein Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO bzgl. aller sie betreffenden, beim Verantwortlichen verarbeiteten personenbezogener Daten zusteht, wenn sie ggf. auch nur ein personenbezogenes Datum selbst direkt übermittelt hat, würde es zu einer Überschneidung mit Art. 15 DS-GVO, dem Auskunftsrecht der betroffenen Person, kommen.

Art. 15 DS-GVO sieht hingegen keine Übermittlung der Auskunft in einem „strukturierten, gängigen und maschinenlesbaren Format“ vor. Aus diesem Grund kann ein wie eben beschriebener weit verstandener Begriff des „Bereitstellens von Daten“ nicht tragen.

Damit, dass der Forderungsschuldner als betroffene Person seine dem Verantwortlichen selbst zur Verfügung gestellten Daten nur über die Auskunft nach Art. 15 DS-GVO und nicht über Art. 20 DS-GVO erhalten könnte, wäre auch keine Senkung des Schutzes der betroffenen Person verbunden.

---

[12] Zum Ziel der Regelung des Art. 20 DS-GVO: *Piltz* in Gola, DS-GVO – Datenschutz-Grundverordnung VO (EU) 2016/679, 2017, Art. 20, Rn. 3.

[13] Vgl. auch *Piltz,* aaO, Rn. 14.

III. Struktur der Inkassobranche

Derzeit sind 2105 Registrierungen[14] von Personen und Unternehmen, die Inkassodienstleistungen erbringen, im Rechtsdienstleistungsregister zu finden. Nicht alle davon sind aktiv am Markt tätig.

Unabhängig von den Inkassodienstleistungen bieten viele Inkassodienstleister aber heute auch noch weitere Services an: Gemäß der „Branchenstudie Inkasso 2016“[15] gehören zum Service-Angebot bei einem Großteil der Inkassodienstleister auch Adressermittlungen, Inbound- und Outbound-Calls, Bonitätsprüfungen, das Debitoren-Management sowie der Ankauf notleidender Forderungen oder Factoring.

Die diesbezüglichen Betroffenheiten in Bezug auf Art. 20 DS-GVO werden in dem vorliegenden Beitrag nicht thematisiert, lediglich die gemäß dem Vorschriftswortlaut vorliegende Betroffenheit in Bezug auf Inkassodienstleistungen im Sinne des RDG.

Etwa 70 Prozent der aktiven Inkassodienstleister sind Mitglied im Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU), die rund 90 Prozent des Marktvolumens repräsentieren und mit insgesamt ungefähr 19.000 Mitarbeitern für über eine halbe Million Auftraggeber aus allen Wirtschaftsbereichen arbeiten.

Zwischen fünf und zehn Milliarden Euro führen sie pro Jahr dem Wirtschaftskreislauf wieder zu und sichern so die Liquidität nicht zuletzt der kleinen und mittleren Unternehmen.

Die Inkassodienstleister halten Ende 2015 ein Forderungsvolumen von fast 60 Milliarden Euro. Hierbei handelt es sich zu knapp 90 % um Forderungen gegenüber privaten Schuldnern (b2c) und nur zu gut 10 % gegenüber Geschäftskunden (b2b). Drei Viertel aller bearbeiteten Forderungen haben einen Wert von mehr als 500 Euro.[16]

Die Inkassobranche ist eine sehr heterogene Branche: Es gibt Einzelunternehmen, sehr viele mittelständische Inkassodienstleister sowie auch Großunternehmen, die teilweise Konzernen angehören. Aufgrund der unterschiedlichen Unternehmensgrößen und deren Kapazitäten gibt es in der Folge auch bei der Anzahl der Forderungsschuldner, gegenüber denen die Inkassodienstleister aufgrund des Inkassovertrags mit dem Forderungsgläubiger tätig werden, erhebliche Unterschiede.

IV. Auswirkungen bzgl. des Rechts auf Datenübertragbarkeit – Informationen zur verwendeten Software

Unterschiede gäbe es auch bei den Marktteilnehmern bzgl. des Aufbaus einer ggf. geforderten Schnittstelle zur Bedienung des Rechts auf Datenübertragbarkeit. Insbesondere kleine und kleinere der mittelständischen Inkassodienstleister könnten mit dieser technischen Einführung überfordert sein. Eine mögliche Lösung – auch wenn aus erwähnten Gründen die betroffene Person kein Mehrwert dadurch erfahren würde – wäre allenfalls eine entsprechende Vorgabe durch die Softwares, mit denen die Inkassodienstleister arbeiten. Eine Standardsoftware gibt es nicht. Es gibt allerdings mehrere Anbieter auf dem Markt, die speziell auf die Inkassobranche ausgerichtete Software anbieten und mit denen auch viele Inkassodienstleister arbeiten. Selbst wenn alle Inkasso-Software-Hersteller Lösungen in ihren Softwares etablieren würden, wäre dennoch nicht der gesamten Branche geholfen.

---

[14] Zu finden unter www.rechtsdienstleistungsregister.de für den Bereich „Inkassodienstleistungen“ (Stand: 22. August 2017).

[15] *Bülow*, Update Branchenstudie Inkasso, zfm 2016, 223.

[16] Alle Angaben ergeben sich aus der „Branchenstudie Inkasso 2016“, siehe Fußnote 15.

Einige Inkassodienstleister, darunter auch v.a. kleine Unternehmen, arbeiten z.B. mit Softwares für Rechtsanwälte. Große Inkassodienstleister hingegen verwenden oftmals eine selbst programmierte Software. Um das Recht auf Datenübertragbarkeit einheitlich auszugestalten – sofern es verbindlich für alle Verantwortlichen zu erfüllen wäre – bedürfte es somit einheitlicher Vorgaben zur technischen Umsetzung.

V. Fazit

Für den Bereich der Inkassodienstleistungen erweist sich das Recht auf Datenübertragbarkeit weder als praxistauglich noch erforderlich.

Forderungsschuldner als betroffene Personen könnten – im Fall, dass es sich um eine Einziehung einer vertraglich entstandenen Forderung handelt – nur selten das Recht auf Datenübertragbarkeit geltend machen, da sie selbst nur selten personenbezogene Daten dem Inkassodienstleister mitteilen. Die über Art. 20 DS-GVO herausverlangten Daten hätten zudem keinen Mehrwert, da sich das Recht auf Datenübertragbarkeit nur auf die von ihnen direkt bereitgestellten Daten erstrecken würde und nicht auf alle beim Inkassodienstleister als Verantwortlichen verarbeiteten Daten.

Das Recht auf Datenübertragbarkeit kann sich nicht auf all diese Daten erstrecken, da ansonsten Art. 15 DS-GVO eine Herausgabe in einem „strukturierten, gängigen und maschinenlesbaren Format“ hätte vorsehen müssen. Dies ist aber gerade nicht der Fall.

Die ursprünglichen Intentionen von Europäischem Rat und Europäischer Kommission, das Recht auf Datenübertragbarkeit allein auf Angebote sozialer Medien im Internet bzw. auf Freundeslisten oder Fotos zu begrenzen, sollte nicht außer Acht gelassen werden.

(Gelb markierte) Schlagwörter:

- Auskunftsrecht
- Forderungsmanagement
- Inkassodienstleister
- Intendierter Anwendungsbereich von Art. 20 DS-GVO
- Rechtsverfolgung

Deutscher Dialogmarketing Verband e.V.

18. August 2017

Stellungnahme

Das Recht auf Datenportabilität im Dialogmarketing

Als eine der zentralen Innovationen der Europäischen Datenschutz-Grundverordnung (DS-GVO) gilt das Recht auf Datenübertragung. Es findet sich in Artikel 20 der DS-GVO und ergänzt den allgemeinen Auskunftsanspruch nach Artikel 15. Die Anwendung des Rechts auf Datenübertragung im Bereich des Dialogmarketings lässt sich gegebenenfalls dadurch umsetzen, dass die bestehenden Verfahren zur Beauskunftung von betroffenen Personen um eine elektronische Datenübermittlung ergänzt werden. Deshalb ist für die Umsetzung des Rechts auf Datenportabilität die Frage zu stellen, welchen Umfang der allgemeine Auskunftsanspruch hat (1.) und wie er sich vom Recht auf Datenportabilität unterscheidet (2.). Auf der Basis dieses Vergleichs lässt sich ermitteln, welche Anpassungen am bisherigen Auskunftsverfahren vorzunehmen sind, um es für Anfragen auf Datenportabilität verwenden zu können (3.).

Die Artikel 29 Datenschutzgruppe hat "Guidelines on the right to data portability" beschlossen (letzte Fassung vom 5. April 2017). Diese enthalten teilweise eine Darstellung der in der DS-GVO verankerten rechtlichen Pflichten und teilweise Empfehlungen der Datenschutzgruppe hinsichtlich der Umsetzung, die jedoch nicht rechtlich verpflichtend sind. Beide Bereiche sind nicht klar voneinander abgegrenzt. Dies wird vor allem dadurch deutlich, dass Beispiele verwendet werden, die nicht vom rechtlichen Anspruch auf Datenportabilität gedeckt sind.

Es ist deshalb wichtig, die datenschutzrechtliche Diskussion zum Recht auf Datenportabilität im ersten Schritt auf die gesetzlichen Anforderungen zurückzuführen. Ob in bestimmten Branchen freiwillig darüber hinausgegangen wird, ist eine andere Frage. Im Bereich des Dialogmarketings besteht hierfür kein Anlass, da nur mit vergleichsweise wenigen Anfragen zu rechnen ist.

1. Welchen Umfang hat der Auskunftsanspruch?

Nach Artikel 15 haben betroffene Personen einen Anspruch auf Auskunft über die personenbezogenen Daten, die ein Unternehmen über sie gespeichert hat. In einem typischen Customer Relationship Management (CRM) System wären dies insbesondere die Rechnungs- und Lieferanschriften, Bestellhistorie und Informationen zur Zahlungsabwicklung. Diese Daten sind der betroffenen Person nach Artikel 15 (3) in Kopie zur Verfügung zu stellen, soweit es sich um personenbezogene Daten der anfragenden Person hält. Dazu sind noch weitere Angaben zu machen, die weitgehend den allgemeinen Transparenzpflichten nach Artikel 13 und 14 entsprechen.

Soweit Analysen zum Kunden gespeichert werden, handelt es sich nach der Rechtsprechung des Gerichtshofs der Europäischen Union nicht um personenbezogene Daten (EuGH, Urteil vom 17. Juli 2014 – C-141/12 und C-372/12). Nach der Rechtsprechung des Bundesgerichtshofes sind Meinungsäußerungen keine personenbezogenen Daten (BGH, Urteil vom 22. Februar 2011 – VI ZR 120/10 und Urteil vom 28. Januar 2014 – Az. VI ZR 156/13). Soweit Analysen oder Meinungsäußerungen zum Kunden gespeichert werden, besteht kein Anspruch auf Auskunft. Wenn beispielsweise eine Analyse des Kaufpotentials erfolgt, ist das Ergebnis nicht auskunftspflichtig.

Weiterhin sind Daten über andere Personen als den Auskunftsersuchenden nicht bereitzustellen. Dies betrifft beispielsweise die Namen von Call-Center Mitarbeitern, die von einem Kunden eine Bestellung aufgenommen haben.

In einem CRM-System befinden sich außerdem Daten über Bestellungen, die nicht gleichzeitig personenbezogene Daten über den Kunden sind. Dies gilt beispielsweise für organisatorische Informationen zur Abwicklung der Bestellung.

2. Wie unterscheiden sich Auskunft und Datenportabilität?

Der Anspruch auf Datenportabilität nach Artikel 20 ist im Vergleich zum Auskunftsanspruch teils erweitert und teils eingeschränkt. Die Erweiterung besteht einmal darin, dass die Kopie der Daten in einem strukturierten, gängigen und maschinenlesba-

ren Format bereitzustellen ist. Außerdem kann die betroffene Person verlangen, dass die Daten direkt an einen anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

Im Vergleich zum Auskunftsanspruch ist der Umfang der im Rahmen der Datenportabilität zu übermittelnden Daten eingeschränkt. Erfasst werden ausschließlich personenbezogene Daten zur betroffenen Person, die von dieser selbst bereitgestellt wurden. Wenn beispielsweise in einem CRM System Daten aus öffentlich zugänglichen Quellen hinzugefügt wurden, sind diese zwar vom Auskunftsanspruch umfasst, jedoch nicht vom Anspruch auf Datenportabilität. Außerdem gilt der Anspruch nur für Daten, die auf Grund einer Einwilligung oder zum Zwecke der Durchführung eines Vertrages verarbeitet werden. Wenn jedoch Daten zu Zwecken des Dialogmarketings auf Grund der Interessenabwägungsklausel verarbeitet werden, greift der Anspruch auf Datenportabilität nicht.

Damit stellen die Daten, die in elektronischer Form zu übermitteln sind, nur eine Untergruppe der Daten dar, die eine betroffene Person im Rahmen eines Auskunftsanspruches erhalten kann. Diese Untergruppe von Daten muss in einem strukturierten, gängigen und maschinenlesbaren Format übertragen werden. Die Entscheidung darüber, welches Format verwendet wird, ist dem Unternehmen überlassen, das die Daten übermitteln muss. Konkrete technische Vorgaben enthält Artikel 20 nicht. Eine direkte Übermittlung an ein anderes Unternehmen ist technisch nur "machbar", wenn dieses Unternehmen die Daten auf die Weise empfangen kann, wie sie bereitgestellt werden.

Ein weiterer Unterschied zwischen dem Auskunftsanspruch und dem Anspruch auf Datenportabilität besteht darin, dass beim Auskunftsanspruch für weitere Kopien Kosten verlangt werden können. Artikel 20 enthält zur Frage der Kosten keine Regelung. Es gilt nur die Regelung für exzessive Anträge nach Artikel 12 (5).

In der Praxis ist für beide Ansprüche von Bedeutung, wie die Identität der betroffenen Person festzustellen ist. Zwischen Auskunftsanspruch und Anspruch auf Datenportabilität bestehen dabei keine Unterschiede. Allenfalls bei der Datenportabilität direkt zu anderen Unternehmen müssten wohl höhere Anforderungen gestellt werden, als bei einer Beauskunftung oder Übermittlung direkt an die betroffene Person.

Im Dialogmarketing lässt sich die Adresse der betroffenen Person leicht identifizieren. Ob ein anderes Unternehmen aber zum Empfang der Daten berechtigt ist, kann nur die betroffene Person selbst bestätigen.

3. Anpassungsbedarf für den Anspruch auf Datenportabilität

Unter Berücksichtigung der Unterschiede zwischen Auskunftsanspruch und Anspruch auf Datenportabilität sind in der Praxis des Dialogmarketings nur wenige Anpassungen erforderlich, um dem Anspruch auf Datenportabilität zu genügen.

In einem ersten Schritt ist zu ermitteln, welche Daten zu übermitteln sind. Da es sich um eine Untergruppe der im Rahmen eines Auskunftsanspruchs zu übermittelnden Daten handelt, kann auf der Basis der bei einer Auskunft bereitzustellenden Daten entschieden werden, welche dieser Daten für den Anspruch auf Datenportabilität gestrichen werden können.

In der Praxis werden einige Unternehmen dieser Fragestellung entgehen, in dem sie schlicht alle Daten übermitteln, die auch im Rahmen einer Auskunft übermittelt werden. Es schadet datenschutzrechtlich nicht, wenn im Rahmen der Datenportabilität alle Daten übermittelt werden, die auch dem Auskunftsanspruch unterliegen.

Bei einer direkten Übermittlung an ein anderes Unternehmen ist jedoch Vorsicht geboten. Wenn Datendienstleister dem übermittelnden Unternehmen die Daten zur Verfügung gestellt haben, könnten lizenzrechtliche Beschränkungen einer Übermittlung entgegenstehen. Artikel 20 (4) weist ausdrücklich darauf hin, dass Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden dürfen. Dazu gehören auch Rechte Dritter am geistigen Eigentum.

Im zweiten Schritt ist ein technisches Verfahren auszuwählen. Hier sollten keine Formate verwendet werden, die erst nach kostenpflichtiger Anschaffung einer bestimmten Software lesbar sind. Insofern bieten sich einfache Formate (wie ASCII) an. Im Bereich des Dialogmarketings sind auch pfd-Formate denkbar. Nur in Einzelfällen ist zu erwarten, dass Ansprüche auf Datenportabilität geltend gemacht wer-

den. Vollautomatische Verfahren zur Erfüllung des Anspruchs sind für die meisten Unternehmen deshalb nicht geboten.

Für die Übermittlung der Daten sind verschiedene Verfahren denkbar. Aus Sicherheitsgründen bietet es sich an, die Daten für die betroffene Person elektronisch zum Abruf zur Verfügung zu stellen. Die Zugangsdaten für den Abruf können per Post oder E-Mail zugesendet werden. Wenn die betroffene Personen die Daten einem anderen Unternehmen überlassen will, kann sie die Nachricht mit den Zugangsdaten entsprechend an dieses Unternehmen weiterleiten.

4. Fazit

Im Ergebnis zeigt sich, dass die Umsetzung des Anspruches auf Datenportabilität schon deshalb keinen erheblichen Aufwand im Bereich des Dialogmarketings verursachen sollte, weil er dem Auskunftsanspruch weitgehend gleicht. Die Einführung automatischer und branchenweit abgestimmter Verfahren ist im Bereich des Dialogmarketings nicht angezeigt.

Kontakt bei weiteren Fragen:

Daniela Henze, Leiterin Public Affairs und des Hauptstadtbüros
Pariser Platz 6 a, 10117 Berlin, d.henze@ddv.de, 030/3001493054

Hans Jürgen Schäfer, Justiziar
Hahnstr. 70, 60528 Frankfurt, hj.schaefer@ddv.de, 069/401276531

www.ddv.de

Frankfurt/Main, 18. August 2017

gez. Patrick Tapp, Präsident

Über den DDV:

Der Deutsche Dialogmarketing Verband ist der größte nationale Zusammenschluss von Dialogmarketing-Unternehmen in Europa und gehört zu den Spitzenverbänden der Kommunikationswirtschaft in Deutschland. Im DDV sind Auftraggeber von Dialogmarketing und ihre Dienstleister vertreten, u. a. Agenturen, Adress- und Informationsdienstleister, E-Mail-Dienstleister, Customer Services- und Contact-Center, Direct-Mail-Unternehmen sowie Werbungtreibende aus verschiedenen Wirtschaftszweigen. Der Verband sorgt für den Interessenausgleich zwischen Wirtschaft, Politik, Wissenschaft und Verbraucher - für die Freiheit der Kommunikation und die Möglichkeiten, Dialogmarketing in seiner Vielfalt gestalten und einsetzen zu können. Schwerpunkte des Verbandsengagements sind politische Arbeit, Informationsaustausch, Qualitätssicherung und Nachwuchsförderung.

LIFE IS FOR SHARING.

Statement on the Guidelines on the right to data portability of the Article 29 Data Protection Working Party

In order to clarify the interpretation of the new right to data portability, the Article 29 Data Protection Working Party (WP29) has published an opinion on the respective provision laid down in Article 20 of the GDPR. The draft opinion contains highly problematic statements, due to the fact that the WP 29 tries to significantly extent the scope and aim of the given regulation. This contradicts the extensive process and the political discussions around the creation of the GDPR, while also creating new levels of legal uncertainty for companies and data subjects alike.

In detail:

1) The GDPR purposefully has narrowed down the personal data affected by the right to data portability to data „provided by" the data subject. This wording was chosen deliberately over "processed" personal data. The EU legislators have chosen this angle to avoid conflicts regarding the different rights of data controllers, data subjects an third parties while also creating an easy to execute right for the data subject. Any further interpretation contradicts this limitation. The WP 29 has neither the right nor mandate to arbitrarily broaden the scope of the GDPR.

2) The broadening of the scope to data ""provided" by the data subject by virtue of the use of the service or the device" would lead to insolvable problems for the data controller. From a technical point of view, most service providers do not have a separate data base containing only the raw data that can easily be separated from the algorithms to create profiles for customer analytics. Transferring this data to another service provider would in almost all cases give detailed background information about the technical setup of the original controller and the used algorithms. Therefore the very base of the controllers business would be revealed, essentially always tackling intellectual properties and trade secrets. Therefore, most data controllers can only provide data that is not affected by these concerns, linking back to the original language of Article 20 of the GDPR (data provided by the data subject, not data by virtue of usage).

3) The burden on the new data controller to analyze the data provided by the data subject in terms of whether it contains information that goes beyond the consent or contractual obligations is overly cumbersome and creates legal uncertainties. If the data is not covered by the consent given by the data subject or contractual obligations, the controller has no right to process such data. Since processing starts with the saving of data, the inspection of the data by the controller would already be illegal. Especially with regard to telecommunications data such as traffic and location data where a processing based on legitimate interests is not allowed. In addition, the

described practice to hand over full sets of data to further investigate whether all the data points are actually needed is very alarming from a data privacy perspective.

4) Especially for electronic communication data with legal deletion obligations, the right to data portability creates a myriad of legal uncertainties. In case of traffic and location data, it is totally unclear what the implications for the data subject and the new data controller are, given the obligation to delete respective data according to the ePrivacy directive. In addition, the porting of traffic data always tackles the right of third parties. This would be a clear violation of section 4 of Article 20.

5) The WP 29 has the right to encourage the development of common standards and interoperable systems creating easy ways to enforce the right to data portability. However, it must be made clear that this cannot mean an establishment of open API layers until the GDPR will enter into force. Technical standards are surely challenging to achieve and their development will take time and effort from many parties involved, including supervisory authorities and public entities.

In conclusion:

Any interpretation of Article 20 should stick closely to its wording, in order to not contradict the intention of the European legislator:

"data provided to a controller":

- → means only the data which the data subject controls and accesses on its own (e.g. photos, emails) during the performance of the contract.
- → does not mean usage data and necessary data for the conclusion of the contract.

the controller is not obliged to provide any data, which has been generated automatically by the service while the data subject is using the service (e.g. logfiles, traffic or location data).

Stiftung Datenschutz - Call for Papers zur Datenportabilität

Thesen der Deutschen Versicherungswirtschaft zum Recht auf Datenportabilität

- Das Recht auf Datenportabilität umfasst Daten, die der verarbeitenden Stelle aktiv zur Verfügung gestellt wurden. Dazu können auch Daten aus vernetzten Geräten gehören. Im Einzelnen bedarf der Umfang des Rechts noch rechtlicher Klärung.
- Eine Datenportabilität kommt nicht in Betracht, wenn dadurch Geschäftsgeheimnisse oder Urheberrechte des übertragenden Unternehmens sowie Rechte und Freiheiten anderer Personen verletzt würden.
- Das Recht auf Datenportabilität darf nicht zum Risiko für den Datenschutz werden. Insbesondere muss sichergestellt sein, dass die Daten nicht an einen Unberechtigten herausgegeben werden. Die Übermittlung zum Teil hochsensibler Daten, wie sie die Versicherungswirtschaft verarbeitet, an dritte Stellen, kann ebenfalls ein Risiko für den Datenschutz darstellen, wenn bei diesen Unternehmen kein gleichwertiges Datenschutzniveau und – in der Personenversicherung – kein strafrechtlicher Geheimnisschutz besteht. Auch muss sichergestellt sein, dass der Übertragungsweg ausreichend abgesichert ist.
- Es kann nicht in der Verantwortlichkeit des übertragenden Unternehmens liegen, prüfen zu müssen, ob und welche Daten ein drittes Unternehmen benötigt.
- Die Erfüllung des Rechts auf Datenportabilität sollte in bestehende Datenschutzmanagementsysteme integriert werden.
- Ein Anspruch auf ein bestimmtes Format lässt sich aus der DSGVO nicht herleiten.
- Die Anforderungen an ein Format müssen sich daran orientieren, dass die Daten auf dem Empfängersystem, insbesondere bei Privatpersonen sowie auch durch branchenfremde Verantwortliche, verarbeitet werden können.
- Das Recht auf Datenportabilität begründet nicht die Pflicht des Verantwortlichen, Datenverarbeitungssysteme zu übernehmen oder beizubehalten, die mit den Systemen anderer Datenverarbeiter technisch kompatibel sind.
- Einen für alle Sektoren und Branchen verbindlichen Standard zu entwickeln, ist jedoch aufgrund der vielfältigen Datennutzung nur schwer leistbar. Hilfreich sein dürften allgemeine Eckdaten – wie Interoperabilität, plattform-übergreifende Nutzbarkeit, offene Standards und Schnittstellen.

Vorbemerkung

Für bestimmte Datenübermittlungen zur Übertragung ausgewählter Kundendaten zwischen Beteiligten im Versicherungsgeschäft bestehen zum Teil bereits heute innerhalb der Branche datenschutzrechtskonforme und standardisierte technische Lösungen. Dies betrifft etwa die Datenübermittlung zwischen Vermittlern und Versicherungsunternehmen oder Versicherungsunternehmen untereinander im Rahmen von Vorversicherungsanfragen oder Übertragung von Schadenfreiheitsrabatten. Die nach der EU-Datenschutz-Grundverordnung als Be-

troffenenrecht ausgestaltete Datenportabilität steht sowohl rechtlich als auch in Bezug auf prozessuale und technische Anforderungen als eigenständiges Rechtsinstrument daneben.

Zu den Leitfragen

a) Allgemeine Fragen

1. Wie eng oder weit ist das Merkmal des „Bereitstellens von Daten“ zu verstehen?

a) Begriff des Bereitstellens

Bereitstellen ist nach dem allgemeinen Sprachgebrauch jedenfalls ein aktives „zur Verfügung stellen“ oder ein Bereithalten zum Abruf. Jedenfalls **bei einer aktiven, zweckgerichteten Übermittlung** der Daten sind diese also bereitgestellt. Bei Versicherungsunternehmen wird es sich in erster Line um Daten handeln, die Kunden bei der Stellung eines Antrags auf Versicherungsschutz oder im Rahmen der Abrechnung eines Leistungsfalles für die Risiko- bzw. Leistungsprüfung des Unternehmens zur Verfügung stellen.

Ob sich das Recht auf die bei Vertragsschluss zur Verfügung gestellten Stammdaten beschränken lässt (so Kamlah in Plath, Art. 20 Rn. 6), ist fraglich. Jedoch wird sich bei Auslegung des Begehrens des Betroffenen häufig ergeben, dass nur dies gewollt ist.

Nach den Leitlinien der **Artikel-29-Datenschutzgruppe** zum Recht auf Datenportabilität (WP 242 rev. 01, S. 9 f.) soll sich der Herausgabeanspruch auch auf solche Daten erstrecken, die vom Betroffenen mittels technischer Einrichtungen (z. B. mittels Fitnesstracker oder eines Kfz) generiert und vom Verantwortlichen gespeichert werden. Ob und in welchen Konstellationen dem zu folgen ist, bedarf noch einer vertieften rechtlichen Diskussion. Für die Einbeziehung dieser Daten spricht, dass die Daten durch das Verhalten der Nutzer erzeugt wurden. Es kann auch z. B. im Interesse des Betroffenen liegen, dass er Daten aus Fahrzeugen, Kfz-Werkstätten oder Versicherungsunternehmen zur Verfügung stellt, damit diese die Daten für die vom Kunden gewünschten Angebote weiterverarbeiten können.

Darüber hinaus sollen nach Ansicht der Artikel-29-Datenschutzgruppe auch Daten erfasst sein, die aus der **Überwachung der Aktivitäten des Betroffenen** resultieren und nicht auf einer aktiven Bereitstellung beruhen, wie Daten aus Logfiles und Suchhistorien (WP 242 rev. 01, S. 9 f.). Im Gegensatz zur Ansicht der Artikel-29-Datenschutzgruppe wird man diese Daten nur schwerlich unter den Begriff des „Bereitstellens“ subsumieren können. Ungeachtet dessen gehört die Erhebung derartiger Daten auch nicht zur Hauptleistung von Versicherungsunternehmen. Während derartige Daten bei Suchmaschinen eine Rolle spielen können, ist es wenig wahrscheinlich, dass ein Kunde eines Versicherungsunternehmens diese Daten sinnvoll weiterverwenden kann. Eine Auslegung des Kundebegehrens wird häufig ergeben, dass eine Übermittlung dieser Daten nicht gewünscht ist. Auch hierzu ist **noch eine vertiefte rechtliche Diskussion** erforderlich.

Bewertet der Verantwortliche die vom Betroffenen bereitgestellten Daten und erlangt **eigene Erkenntnisse** (z. B. im Rahmen der Risikoeinschätzung oder Leistungsprüfung), handelt es sich nicht mehr um Daten, die der Betroffene bereitgestellt hat, sondern um **Verarbeitungsergebnisse**. Spätestens hier findet der Anspruch auf Datenportabilität auch aus Sicht der Artikel-29-Datenschutzgruppe (WP 242 rev. 01, S. 10) seine Grenze.

Ebenso handelt es sich nicht mehr um vom Betroffenen bereitgestellte Daten, wenn der Erstversicherer die ihm vom Betroffenen bereitgestellten Daten im Rahmen der vertraglichen Beziehung zwischen Erst- und Rückversicherer an den Rückversicherer weitergibt. Der Anspruch des Betroffenen kann hier nur gegenüber dem Erst-, nicht aber gegenüber dem Rückversicherer bestehen.

b) Grenzen des Rechts auf Datenportabilität

Ungeachtet der Auslegung des Begriffs des Bereitstellens von Daten, ist zu bedenken, dass das Recht auf Datenportabilität nicht grenzenlos gilt.

Das Recht auf Datenportabilität kann insbesondere in **Konflikt mit dem Schutz von Geschäftsgeheimnissen** oder den Rechten Dritter geraten, wenn z. B. durch die Datenübertragung Wettbewerber zugleich Erkenntnisse über geschäftsrelevante Verarbeitungsformen gewinnen können. Das ist in der Versicherungswirtschaft z. B. der Fall, wenn durch die Datenübertragung Wettbewerbern unternehmensindividuelle Kriterien für die Risikobewertung oder Interna zur Prämienbemessung offenbart werden könnten. Einschränkungen könnten sich hier aus Art. 20 Abs. 4 DSGVO herleiten lassen. Danach darf die Geltendmachung des Rechts aus Art. 20 Abs. 2 DSGVO die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Darunter lassen sich nicht nur die Rechte anderer Betroffener, sondern auch die Rechte des für die Datenverarbeitung Verantwortlichen subsumieren. In diese Richtung geht im Grundsatz auch die Argumentation der Artikel-29-Datenschutzgruppe (WP 242 rev. 01, S. 12). Denkbar könnte auch sein, dass allein durch die Zusammensetzung der herauszugebenden Daten auf die Ausgestaltung bestimmter Geschäftsprozesse geschlossen werden kann. Fraglich ist, ob hier dem Anspruch auf Herausgabe der Schutz von Urheberrechten entgegengehalten werden kann.

2. Ist die neue Norm geeignet, für die Verbraucherinnen und Verbraucher ein echtes Mehr an informationeller Selbstbestimmung zu schaffen?

Ein Mehr an informationeller Selbstbestimmung ist z. B. zu erwarten, wenn durch das Recht auf Datenportabilität sog. **Lock-in-Effekte vermieden** werden. Das ist z. B. der Fall, wenn es erst ermöglicht oder leichter wird, Daten auf andere Anbieter zu übertragen. So ist es mittels des Rechts auf Datenportabilität leichter, z. B. Daten aus sozialen Netzwerken auf andere soziale Netzwerke zu übertragen oder Cloud-Anbieter zu wechseln. Auch könnte das Recht auf Datenportabilität eine Hilfe sein, wenn Menschen Daten aus der Nutzung vernetzter Geräte nicht nur im Verhältnis zum Anbieter des Geräts, sondern auch für andere Zwecke nutzen möchten. Die Versicherungswirtschaft hat hier bereits in der Vergangenheit bestimmte Datenaustauschverfahren entwickelt, um Lock-in-Effekte zu vermeiden. Zu denken ist beispielsweise an die Mitnahme eines Schadensfreiheitsrabattes in der Kfz-Haftpflichtversicherung, der einen entsprechenden Austausch der relevanten Daten zwischen dem alten und dem neuen Versicherer voraussetzt.

Das Recht auf Datenportabilität darf aber nicht zum Risiko für den Datenschutz werden.

Die **Versicherungswirtschaft verarbeitet zum Teil hoch sensible Daten**. So werden in der Lebens-, Kranken- und Unfallversicherung Gesundheitsdaten zur Überprüfung des zu versichernden Risikos und zur Erbringung der Leistung, z. B. bei Krankheit oder Berufsunfähigkeit, benötigt. In der Haftpflichtversicherung werden Gesundheitsdaten geschädigter Menschen zur Prüfung des Schadensersatzanspruchs und zur Regulierung des Schadens verarbeitet.

Eine Herausgabe dieser Daten setzt voraus, dass sich der Kunde oder Geschädigte, der die Daten zur Verfügung gestellt hat, **eindeutig identifizieren** kann und dass es möglich ist, die **Daten auf sicherem Wege zu übermitteln**. Anderenfalls kann das Bestreben, dem Recht aus Art. 20 DSGVO zu entsprechen, schnell zu einer Datenpanne werden, die für den Betroffenen verheerende Folgen haben kann. Darüber hinaus kann in der Lebens-, Kranken- und Unfallversicherung die Herausgabe der Daten an einen unberechtigten Empfänger für den Versicherer ein nach § 203 StGB strafbewährtes Offenbaren von Geheimnissen darstellen. Fraglich ist daher, ob hier allein die Geltendmachung des Anspruchs aus Art. 20 DSGVO durch den Betroffenen genügt oder zusätzlich die Einholung einer Schweigepflichtentbindungserklärung erforderlich ist.

Der Forderung der Artikel-29-Datenschutzgruppe nach einem Authentifizierungsprozess (WP 242 rev. 01, S. 14) ist grundsätzlich zuzustimmen. Die Datenschutzbehörden sollten EU-weit definieren, welche konkreten **Anforderungen an die Authentifizierung** gestellt werden, damit keine Rechtsunsicherheit für die Verantwortlichen und keine Risiken für die Betroffenen bestehen. Das Gleiche gilt für eine Übermittlung der Daten, die den Anforderungen an die Datensicherheit genügt.

Wenn Dritte, insbesondere die neuen Verantwortlichen, als **Vertreter oder Bote** des Kunden oder der geschädigten Personen eine Herausgabe von deren Daten nach Art. 20 Abs. 2 DSGVO verlangen, bestehen ebenfalls erhebliche Risiken. Es muss sichergestellt sein, dass der Kunde oder Geschädigte wirklich die Übermittlung seiner Daten an den Dritten möchte und in welchem Umfang dies geschehen soll. Es muss zudem sichergestellt sein, dass keine Daten an einen Unberechtigten herausgegeben werden. Daher stellen die Datenschutzbehörden zu Recht sehr hohe Anforderungen an die Erteilung der Auskunft an Bevollmächtigte (dazu z. B. https://www.datenschutz.hessen.de/tb45k04.htm#entry4860 Ziffer 4.4.2.1.5). Entsprechend hohe Hürden werden auch für die Datenportabilität gestellt werden müssen.

Weiterhin ist zu bedenken, dass bei Geltendmachung des Rechts auf Datenportabilität die verlangten Daten herausgegeben bzw. an den neuen Verantwortlichen übertragen werden müssen. Es kann **nicht in der Verantwortlichkeit des Übertragenden liegen, zu prüfen, welche Daten für den neuen Dienst bei dem Dritten benötigt werden**. Das verlangt das Gesetz nicht und eine solche Prüfung wäre oft auch tatsächlich gar nicht möglich, weil der Verantwortliche die Verarbeitungszwecke des neuen Verantwortlichen nicht kennt. Die Artikel-29-Datenschutzgruppe stellt zutreffend fest, dass der herausgebende Verantwortliche nicht für die Datenverarbeitung durch den Betroffenen oder die empfangenden Dritten verantwortlich ist (WP 242 rev. 01, S. 6). Dies ist Angelegenheit des Betroffenen bzw. des neuen Verantwortlichen. Das bedeutet aber zugleich, dass der neue Verantwortliche möglicherweise mehr Daten erhält, als er für seine Verarbeitung benötigt. Auch dies stellt ein Risiko für den Betroffenen dar. Unklar ist auch, was mit „überschüssigen Daten“ zu geschehen hat. Die Artikel-29-Datenschutzgruppe vertritt, dass der verantwortliche Dritte die Datenannahme verweigern kann (WP 242 rev.01, S. 6). Hier können sich Risiken im Hinblick auf die Sicherheit ergeben. Die Verantwortung muss bei dem Betroffenen oder dem empfangenden Dritten liegen. Er muss die Daten daher löschen, wenn es keine Rechtsgrundlage für die Verarbeitung gibt.

Es besteht auch das Risiko, dass die Daten bei dem neuen Verantwortlichen schlechter geschützt sind. Das ist z. B. der Fall, wenn Gesundheitsdaten aus einem Lebens-, Unfall- oder Krankenversicherungsverhältnis zunächst beim Versicherer dem **Geheimnisschutz des § 203 StGB** unterliegen und an einen neuen Verantwortlichen weitergegeben werden, der nicht unter die Geheimnisschutznorm fällt.

3. Welche Aspekte müssen im Datenschutzmanagementsystem berücksichtigt werden?

Verfügt ein Verantwortlicher über ein Datenschutzmanagementsystem, muss er die ordnungsgemäße Erfüllung des Rechts auf Datenportabilität implementieren. Es muss gewährleistet sein, dass die notwendigen Maßnahmen zur Datenportabilität geplant, sicher umgesetzt und dokumentiert werden sowie prüfbar sind. Dazu gehören insbesondere

- die Identifizierung des anfragenden Betroffenen,
- Vermeidung der Übertragung an Unberechtigte, z.B. durch Identifizierung und Authentifizierung des Empfängers,
- die Eingrenzung, welche Daten übertragen werden sollen,
- die Prüfung, ob es sich um „bereitgestellte" Daten handelt
- die Feststellung, dass die Verarbeitung der Daten aufgrund einer Einwilligung oder eines Vertrages erfolgt,
- die Feststellung, dass kein Ausschlussgrund für die Datenportabilität besteht.

Daneben kann bei Gesundheitsdaten ggf. noch eine Schweigepflichtentbindungserklärung des Betroffenen einzuholen sein. Die technische Lösung für die Übertragung und die Auswahl eines sicheren Übertagungswegs müssen im Einklang mit Art. 32 DSGVO gewährleistet sein. Dabei müssen zunächst auch prozessuale Überlegungen angestellt werden, etwa hinsichtlich des Umgangs mit Übermittlungsfehlern oder der Prüfung der Legitimation des Empfängers.

b) Technikbezogene Fragen

1. Welche konkreten Anforderungen sollen an ein kompatibles Format gestellt werden?

Kompatibilität muss so verstanden werden, dass das Format unter Zugrundelegung des vernünftigerweise Erwartbaren auf dem Empfängersystem verarbeitet werden kann, d. h. Maßstab muss sein, dass die Daten in einem Format übergeben werden, welches von typischerweise erwartbaren Anwendungen verarbeitet werden kann. Dies kann auf PDF-Dateien, aber auch, wie von der Artikel-29-Datenschutzgruppe festgestellt, auf das XML-Format zutreffen (WP 242 rev.01, S. 18).

2. Wie sollten angesichts der Vorgabe „soweit es technisch machbar ist" Fälle faktischer Unmöglichkeit von Fällen ungerechtfertigter Behinderung einer Datenübertragung abgegrenzt werden?

Erwägungsgrund 68 Satz 2 der DSGVO wirkt zwar darauf hin, dass interoperable Formate entwickelt werden sollten, die die Datenübertragbarkeit aus Art. 20 DSGVO ermöglichen. Erwägungsgrund 68 Satz 6 stellt jedoch auch klar, dass das Recht der betroffenen Personen auf Datenportabilität nicht die Pflicht des Verantwortlichen begründet, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten. Vor diesem Hintergrund darf die genannte Formulierung in Art. 20 Abs. 2 DSGVO also nicht dahingehend missverstanden werden, dass die Verantwortlichen neue technische Lösungen suchen müssen. Eine

Datenportabilität ist nicht erst bei einer faktischen Unmöglichkeit in dem Sinne ausgeschlossen, dass niemand in der Lage sein darf, die Informationen zu übertragen.

3. **Was ist für den Fall vorzusehen, in dem ein Hersteller ein „gängiges Format“ zur Verfügung bereitstellt, die Übertragung jedoch daran scheitert, weil der Empfänger ein anderes, ebenfalls „gängiges“ Format verwendet?**

   - **Soll ein Anspruch des Betroffenen auf ein bestimmtes Format bestehen?**
   - **Wie kann Interoperabilität zwischen unterschiedlichen „gängigen Formaten“ hergestellt werden?**

Ein Anspruch auf ein bestimmtes Format lässt sich aus der DSGVO nicht herleiten. Auch muss der Bereitstellende mögliche Vorgaben des Empfängers nicht erfüllen.

4. **Inwiefern bestehen Vorteile branchenspezifischer Formate gegenüber sektorübergreifenden Formaten?**

Vor dem Hintergrund, dass die betroffene Person die Übertragung der im Wege des Betroffenenrechts auf Datenportabilität übermittelten Daten an einen „anderen Verantwortlichen“ verlangen kann, ohne dass der „andere Verantwortliche“ notwendigerweise Teil derselben Branche ist, und insbesondere vor dem Hintergrund der datengetriebenen Wirtschaft, in der Wertschöpfung gerade durch sektorübergreifende Datennutzung an jedweder Stelle der Wertschöpfungskette beflügelt wird, spricht viel für Formate, die gerade sektorübergreifend nutzbar sind. Damit würde auch dem Ziel der Datenschutzgrundverordnung, den freien Datenverkehr zu fördern, genüge getan.

Zudem muss bedacht werden, dass es sich zuvörderst um ein Betroffenenrecht handelt, bei dem also das Format zunächst aus Sicht der betroffenen Person zu betrachten ist. Diese hat regelmäßig Beziehungen zu datenverarbeitenden Stellen der unterschiedlichsten Branchen und kann gegenüber jedem Verantwortlichen das Betroffenenrecht ausüben. Dabei dürfte zwar die vernünftige Erwartungshaltung der betroffenen Person bestehen, dass je nach Art, Umfang und Zweck der Datenverarbeitung eines bestimmten Verantwortlichen die Gestaltung von Datensätzen (Datenfelder, Umfang, etc.) unterschiedlich ist, zugleich aber auch, dass die – auch sektorübergreifende – Übertragung auf einen anderen Verantwortlichen technisch reibungslos funktioniert.

Einen für alle Sektoren und Branchen verbindlichen Standard zu entwickeln, ist aufgrund der vielfältigen Datennutzung nur schwer leistbar. Sinnvoll sein dürften Rahmenbedingungen in Bezug auf bestimmte allgemeine Eckdaten – wie Interoperabilität, plattformübergreifende Nutzbarkeit, offene Standards und Schnittstellen.

Sofern es sich bei der Verarbeitung von typischerweise von einer bestimmten Branche an eine anderen Branche übermittelten Daten (z. B. Fahrzeugdaten an Versicherungsunternehmen) handelt, wird es jedoch regelmäßig nicht allein auf das datenschutzrechtliche Betroffenenrecht auf Datenportabilität ankommen. Hier bedarf es – jenseits des Rechts auf Datenportabilität und nicht (allein) bezogen auf das Datenschutzrecht – eines Rechtsrahmens oder jedenfalls einer Standardisierung, die den freien Datenverkehr ermöglicht und zugleich berechtigte Interessen der am Wirtschaftsleben beteiligten Stellen wahrt.

Eine Standardisierung, die in einem so beschriebenen Kontext erfolgt – z. B. für eine offene Schnittstelle vernetzter Kraftfahrzeuge – wird jedoch regelmäßig Daten enthalten, die nicht vom Recht auf Datenportabilität erfasst sind, so dass zwar zur Vermeidung von Doppelnormierung und Effizienzverlusten ein Rekurrieren auf bestehende Standards angezeigt sein kann, jedoch nicht davon entbindet, für die Datenportabilität eine gesonderte Betrachtung anzustellen.

5. Wie könnte eine sektorenübergreifende Verschränkung bestimmter Dienste im Format abgebildet werden (z. B. Automobilwirtschaft/Versicherungswirtschaft: Portierung von Fahr(zeug)daten und Versicherungsdaten)?

In der datengetriebenen Wirtschaft ist die (Weiter-)Nutzung von Daten über Branchen und Sektoren hinweg unerlässliche Voraussetzung für neue Wertschöpfung aus digitalen Daten. Gerade im Hinblick auf das Internet of Things, z. B. vernetzte Fahrzeuge, Smart Home oder Industrie 4.0, liegt der Schwerpunkt der Fragestellung aus wirtschaftlicher Sicht jenseits der Datenportabilität. Richtigerweise setzt sich auch die EU-Kommission dafür ein, dass zur Ermöglichung des freien Datenverkehrs und der digitalen Wertschöpfungskette unter Einbeziehung aller Stakeholder interoperable Formate und Schnittstellen geschaffen werden, um Daten (weiter)nutzen zu können.

Insofern erscheint die Fragestellung zu eng, wenn sie nur auf die Berücksichtigung der im Wege der Datenportabilität zu übermittelnden Daten abzielt.

c) Branchenspezifische Fragen

1. Durchführbarkeit:

A) Ist die Erfüllung der Anforderungen zur Datenportabilität in Ihrer Branche und aus Ihrer Sicht automatisierbar und mit deterministischen Prozessen durchführbar?

Grundsätzlich ja.

B) In welchen Bereichen ist dies aus Ihrer Sicht schwierig oder ggf. sogar unmöglich?

Daten, die vom Kunden telefonisch, in nicht automatisiert auslesbarer Papierform (z. B. handschriftlich) oder sonst unstrukturiert übermittelt wurden.

C) Wie wichtig ist es für Ihr Unternehmen bzw. Ihre Branche, eine standardisierte, verlässliche und automatisierbare Format- und Inhaltevorgabe zur Erfüllung der Portabilität zu haben?

Die Notwendigkeit einer Formatvorgabe wird von der praktischen Bedeutung abhängen, die das Recht auf Datenportabilität nach dem Anwendungsbeginn der DSGVO erfahren wird.

D) Mit welcher Wahrscheinlichkeit wird der nachfolgende Dienstleister die Daten in Form eines weitgehend automatisierten Importes nutzen können?

Innerhalb der Branche wie auch in den meisten anderen Fällen einer branchenfremden Datenportabilität ist zu erwarten, dass die Daten in jedem Falle automatisiert weitergenutzt werden sollen. Allerdings ist zu erwarten, dass ein Erhebungsaufwand beim Betroffenen trotz der Übertragung von Daten im Rahmen des Art. 20 DSGVO nicht völlig entfallen wird, etwa,

wenn aufgrund der internen Prozesse beim neuen Anbieter weitere oder andere Informationen erforderlich sind.

2. Branche:

E) Wie scharf ist Ihre Branche gegenüber anderen/benachbarten Branchen abgrenzbar? Wo überlappt sie mit anderen Branchen? Inwieweit ist es eine „Meta"-Branche, die meist als Dienstleister auf klassischen Branchen aufsetzt?

Die Versicherungswirtschaft unterhält Geschäftsbeziehungen zu fast jedem Privathaushalt und jedem Unternehmen in Deutschland und ist mithin fester Teil der Wertschöpfungskette aller Branchen. Zudem hat die Branche durch ihre Funktion als Risikoträger eine zentrale volkswirtschaftliche Rolle zur Ermöglichung wirtschaftlicher Betätigung und privater Entfaltung inne. Auch die Anreiz-Wirkung risikoadäquater Tarifierung durch die private Versicherungswirtschaft hat im Hinblick auf Risikovermeidung eine große volkswirtschaftliche und gesellschaftliche Bedeutung. Die Versicherung von Risiken ist ein Alleinstellungsmerkmal der Branche, die Versicherungsprodukte und Versicherungsleistungen sind nicht durch Produkte und Dienstleistungen anderer Branchen ersetzbar oder austauschbar.

Insofern ist die Versicherungswirtschaft auch von technischen Entwicklungen, insbesondere der Digitalisierung, anderer Branchen betroffen, etwa durch neue Risiken aufgrund der Digitalisierung (Cyber-Risk), aber auch in dem Sinne, dass die zunehmende Menge an Daten, die von Versicherungsnehmern und durch von diesen genutzte vernetzte Gegenständen generiert wird, neue Möglichkeiten und Chancen für die Risikobewertung, Schadenregulierung und Prävention oder für innovative Produkte bieten.

Die Versicherungswirtschaft ist traditionell zur Erfüllung ihres Kerngeschäfts auf Daten zu den versicherten Risiken angewiesen. Sie ist dabei zum Teil auch Datennutzer von Daten anderer Branchen, z. B. Abrechnungsdaten von Werkstätten oder Mietwagenfirmen. Zudem gibt es einen Datenaustausch innerhalb der Branche, z. B. bei einem Vermittlerwechsel oder bei einem Wechsel des Versicherers (z. B. Mitnahme des Schadenfreiheitsrabatts bei Wechsel der Kfz-Versicherung). Insofern bestehen jedoch andere Rechtsgrundlagen für die Übermittlung der Daten, sodass es nicht auf den Anspruch auf Datenportabilität ankommt. Die Versicherungswirtschaft ist regelmäßig nicht Datenlieferant für andere Branchen.

F) Wie viele Anbieter gibt es in der Branche (formlose Beschreibung der Branchenstruktur (typischer großer/mittlerer/kleiner Branchenteilnehmer)? Wieviel Kunden hat ein typischer großer/mittlerer/ kleiner Branchenteilnehmer?

Die deutsche Versicherungswirtschaft ist durch eine Anbietervielfalt gekennzeichnet. Vom regionalen Versicherer bis zum globalen Konzern, vom Versicherungsverein über öffentliche Versicherer bis zur Aktiengesellschaft finden sich viele Rechts- und Organisationsformen und Unternehmensgrößen. Unter Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) stehen derzeit 360 Lebens-, Kranken-, Schaden-/Unfall- und Rückversicherer, die etwa 90 Prozent des deutschen Versicherungsmarktes ausmachen. Hinzu kommen 139 Pensionskassen und 29 Pensionsfonds zur betrieblichen Altersversorgung sowie 35 Sterbekassen und zahlreiche ausländische Anbieter, die die Möglichkeiten des EU-Binnenmarkts (Passporting) für ein Versicherungsangebot in Deutschland nutzen. Darüber hinaus werden einige hundert kleine Versicherer direkt von den Bundesländern beaufsichtigt. Viele Unternehmen sind in Gruppen organisiert und bieten spartenübergreifend Versicherungsschutz aus einer Hand.

Verweis auf Branchenkennzahlen (http://www.gdv.de/zahlen-fakten/branchendaten/)

G) Gibt es eine Dominanz in der Branche (Monopol/Oligopol)?

Nein, die Branche ist durch eine Vielzahl und Vielfalt der Anbieter gekennzeichnet (s. oben). Derzeit lässt sich auch keine Tendenz zur Erhöhung des Konzentrationsgrads am Markt beobachten, s. http://www.gdv.de/wp-content/uploads/2016/09/GDV_Makro_und_Maerkte_-kompakt_05-2016.pdf

3. Informationstechnische Abbildung eines Kunden:

H) Gibt es in der Branche eine Art „Basisdatensatz", der bei allen Marktteilnehmern weitgehend einheitlich oder zumindest ähnlich ist? (inkl. Skizzierung der Merkmale des „Basisdatensatz")

In der Versicherungswirtschaft werden für verschiedene Kommunikationsprozesse standardisierte Datensätze verwendet, so z. B. BIPRO-Normen für die Kommunikation mit Maklern oder der GDV-Datensatz. Branchenweit standardisierte Datenformate kommen beispielsweise zum Einsatz für den Austausch von – spartenübergreifenden – Bestands-, Inkasso-, Schaden- und Antragsinformationen zwischen Versicherungsunternehmen und Vermittlern (insb. Makler und Mehrfachvermittlern).

Datensatzbeschreibungen und weiterführende Informationen zu BIPRO-Normen finden Sie unter https://www.bipro.net/normen, nähere Informationen zum GDV-Datensatz unter http://www.gdv-online.de/vuvm/bestand/Broschuere_gdv-datensatz_vu-vermittler.pdf.

Die Normen und standardisierten Datensätze erfassen allerdings nicht alle Daten, die dem Recht auf Datenportabilität unterliegen.

I) Gibt es bereits einen Datenaustauschstandard bezüglich Kundendaten? (Skizzierung von Art und Anwendung sowie ggf. der Standardbezeichnungen)

s.o. zu H)

J) Wo liegen die individuellen Ausprägungen? Was unterscheidet Marktteilnehmer?

Jedes Versicherungsunternehmen ist grundsätzlich in der Lage, branchenweit eingesetzte Datensätze (z. B. BIPRO-Normen, GDV-Datensatz) zu generieren, zu übermitteln oder entgegenzunehmen. Die Datenverarbeitung in den Versicherungsunternehmen und die Einbindung der mittels entsprechend standardisierter Datensätze erhaltenen oder übermittelten Daten in eigene Datenverarbeitungssysteme ist jedoch unternehmensindividuell, so auch die Zufügung eigener, unternehmens- und produktspezifischer weiterer Datenfelder, die Verarbeitung im Rahmen der Risikobewertung und Anreicherung mit eigenen Berechnungen sowie insbesondere Schadenbearbeitung. Beispielsweise wird ein Versicherungsunternehmen, das einen Telematik-Tarif in der Kfz-Versicherung anbietet, zum jeweiligen Kunden die Telematik-Daten speichern und diese verarbeiten, die jedoch nicht notwendigerweise Bestandteil der standardisierten – und nach ihrem jeweiligen Zweck ausgestalteten – branchenüblichen Datensätze sind. Hinzu kommt, dass Daten oft auch von Dienstleistern erfasst und ausgewertet werden. Das Versicherungsunternehmen erhält dann nur die Ergebnisse. Die Verantwortlichkeit für die Daten hängt dann von der zugrundeliegenden Vertragsgestaltung in der Zusammenarbeit mit Dienstleistern ab, die von VU zu VU unterschiedlich sein kann.

K) In welchem Branchenteil/Marktabschnitt sind Kundendaten in Format, Semantik oder Inhalt sehr individuell bzw. unterschiedlich?

Schadenregulierung, Customer Relations Management, künftig im Bereich der Echtzeitdatenerhebung (z. B. Telematik, Smart Home, etc.). Auch im Bereich der Lebensversicherung unterscheiden sich die tarifrelevanten Daten zwischen den einzelnen Versicherern.

L) Sind Sie selbständig in der Gestaltung der Datenstruktur und -ausprägung oder folgen Sie einem technischen Standard oder einem (de facto-) Branchenstandard oder Prozessen und Vorgaben der Auftraggeber?

N/A (Frage richtet sich nur an Unternehmen)

4. Vereinheitlichung der Datenübergabe

M) Welche Datenbereiche könnte aus Ihrer Sicht und Branchenerfahrung ein möglicher Branchenstandard für die Portabilitätsanforderung umfassen?

Bestimmte Daten, die dem Portabilitätsanspruch unterliegen, können in Teilen auch Bestandteil von branchenüblichen Datensätzen (z. B. BIPRO-Normen für die Kommunikation mit Maklern, GDV-Datensatz) sein. Siehe dazu 3. H).

N) In welchen Datenbereichen wäre eine solche Vereinheitlichung aus Ihrer Sicht eher schwierig oder unmöglich?

Kundendaten, die von den Unternehmen im Rahmen der Schadenregulierung, des Customer Relations Managements oder der produktspezifischen Datenerhebung verarbeitet werden.

O) Gibt es in Ihrer Branche eine / typische Systemarchitekturen? (kurze Skizze)

Nein.

P) Gibt es explizite Branchenstandards für Systemarchitekturen oder hierfür implizite/ de-facto-Branchenstandards?

Nein.

Q) Gibt es in vorhandenen Architekturen bereits Schnittstellen für strukturierten Datenexport oder Portierung?

Die oben aufgezeigten Beispiele stellen keine Schnittstellen für den strukturierten Datenexport oder die Portieren dar.

R) Erleichtern oder erschweren die ggf. vorhandenen Architekturen den Aufbau einer Portabilitätsanforderung?

N/A

S) Sind bestimmte Marktteilnehmer beim Aufbau einer solchen Schnittstelle benachteiligt oder ggf. sogar überfordert?

Versicherungsunternehmen verfügen traditionell über komplexe IT-Systeme, die in der Lage sind, verschiedene Schnittstellen und Datenformate zu bedienen und hierbei auch unterschiedliche Anforderungen (z. B. Schnittstellen, die von Behörden im Bereich des Reporting

vorgegeben werden, Schnittstellen zu Branchenservices, Schnittstellen zu Vermittlern, Sachverständigen, Kreditwirtschaft, etc.) zu implementieren. Auf der anderen Seite sind kleinere Unternehmen häufig nicht in der Lage, eigene Schnittstellen zu entwickeln.

Submission from Google to Stiftung Datenschutz re: Data Portability
August 31, 2017

Google is pleased to provide comments as part of the Foundation for Data Protection's (Stiftung Datenschutz) project to examine practical methods and implications of data portability, as described in Article 20 of the General Data Protection Regulation.

Subject Matters of Data Portability:

Google's mission is to organize the world's information and make it universally accessible and useful. User trust is paramount to our mission, and we strive to earn and maintain it. Consumers have competing online services that they can and do use, so we take special care to ensure that users have control over their data and can trust Google to provide their data to them upon request. Google's approach to data portability is simple: the user comes first. We make continual efforts to keep users' information private and secure, are clear with users on how their data are collected and used, and provide best in class tools so users can view, delete, download, and transfer the content they store in their Google account.

Data portability and interoperability are also central to innovation. Google has always believed robust and reciprocal portability offerings will reduce switching costs, resulting in more innovative and user-focused products. Making it easier for consumers to choose among services facilitates competition, giving users the power to try new services and choose the offering that best suits their individual needs. Data portability can also provide a security benefit for users. For example, allowing users to backup or archive important information, organize between accounts, and recover from account hijacking and deprecated services are practical tools that improve user security.

We believe the following principles around interoperability and portability of data promote user choice and encourage responsible product development, maximizing the benefits to users and mitigating the potential drawbacks.

- **User Driven:** Data portability tools should be easy to find, intuitive, and readily available to consumers. They should also be open and interoperable with standard industry formats, where applicable, so that users can easily transfer data between providers or download it for their own purposes.

- **Privacy and Security:** Providers on each side of the portability transaction should have strong privacy and security measures---such as encryption in transit---to guard against unauthorized access, diversion of data, or other types of fraud.

- **Reciprocity:** While portability offers more choice and flexibility for users, it will be important to guard against incentives that are misaligned with user interests. A user's decision to move data to another service should not result in any loss of transparency or control over that data. Users will expect that data ported into a provider can likewise be exported again, if they so choose. Data should only be transferrable between reciprocal services to incentivize provider participation and guard against the possibility of companies with limited consumer relationships requesting and gaining control over data that does not fit the purpose of their business or benefit the consumer.

- **Focus On Users' Data, Not Company Data:** Data portability is not, and should not be, without reasonable limits. Portability efforts should be limited to data that has utility for a user, e.g. the content a user creates, imports, approves for collection, or has control over. This reduces the friction for users who want to switch among products or services because the data they export is meaningful to them. Portability should not extend to data collected to make a service operate, including data generated to improve system performance or train models that may be commercially sensitive or proprietary. This approach also encourages companies to continue to create, knowing that their proprietary technologies are not threatened by data portability requirements.

Concerned Sectors:

Data portability is aligned with general industry trends to increase user engagement by making it easier to try new, innovative services. Companies are building increasingly sophisticated features and need to ensure that a wide variety of users can enjoy the experiences they are offering. One solution to increasing the audience is to reduce the infrastructure burdens that products place on users. This requires companies to build products that minimize the bandwidth, storage space, and technical expertise required to participate. These solutions result in better experiences for all users, but particularly for those who reside in areas that lack robust digital infrastructure or where data can be prohibitively expensive. Portability aligns with this trend and is an obvious step toward the larger goal of expanding the digital economy.

That said, porting data between entities raises challenging policy and engineering questions that industry will need to address collectively. We can look to existing infrastructure and industry trends for guidance on possible solutions.

First, companies must simultaneously advance their understanding of the importance users place on controlling their digital lives as they build products that assume responsibility for data storage. Although individual companies may have policies or principles that give users control, the industry at large must respond to some user expectations as a community. Users rely on

data to engage in everyday life. They need to be able to manage both the content they create, like a drawing or document, and content about them like their medical records, banking information, or records of the songs they listened to. Because of this users expect to have control over all of this data, including the right to relocate it freely. At the same time, the combination of an increasing amount of digital data and the shift to mobile devices with lower storage capacities results in much of users' personal data being stored with third-parties. Users understand that their control over their data requires the participation of the technology companies they are entrusting with their digital life, and portability is a pillar of meeting their expectations.

Additionally, industry should not assume that successful portability requires building entirely new products. Lightweight approaches to solving the engineering challenge might rely on existing infrastructure, creating minimal burden on companies. For many data types, it is already industry standard to offer platforms that support importing and exporting user data. Building a solution that leverages this existing infrastructure to allow users to send data directly between companies enables a robust data portability ecosystem without the long delays that might be caused by starting at a nascent state.

Data portability aligns with an industry-wide shift. While it may require some investment to develop platforms that are minimally burdensome on users, the increased engagement and user empowerment will benefit the technology sector at large. We believe open source solutions will foster a robust data portability ecosystem, while requiring relatively little investment from the majority of the industry. Companies and sectors that align their portability efforts with larger goals to improve user experiences globally will see long-term gains in their ability to innovate.

Practical Implementation:

Industry has an important role to play in fostering the right framework to encourage more robust and meaningful data portability and interoperability for users. When done right, data portability enables user control, and promotes user choice through improved competition between providers.

Developing one universal format should not be a prerequisite for a portability solution. For some types of data, a recognized industry standard exists (jpeg), for some there are defacto portability standards (mbox and PST for mail), and for others there isn't a clear format of choice (IMs). Additionally, different products offer unique features and encouraging this uniqueness is paramount to encouraging innovation. New features and use cases may be developed at any time and may be incompatible with current formats. Enforcing static, standard formats may reduce the opportunity for portability of these new features because they are not represented in the standard. Decisions about standardization must account for technological innovation.

For data types where there is a standard, these standards should continue to be used. We believe that compatibility can be achieved by providing an open source repository of ways to

translate from proprietary formats into one or more common formats. If a service provider feels existing interfaces don't suit their needs, they are free to define a new one and also write the interface for one or more competitor importers for that data type.

While we support maximizing the role of existing standards and protocols, there still must be a mechanism to encourage reciprocity among data providers. We believe companies have a strong interest in being able to import data from a wide variety of sources. Maintaining parity allows a given provider to choose any format that works for its purposes, and encourages portability by enabling export in any format a different service can import. We believe companies' desire to be able to import data from the most common formats will provide a strong business incentive for them to also export data in the most common format.

To that end, we recommend policymakers consider the following points:

- **Portability should be flexible:** Locking in rigid data portability requirements or standards is an ineffective approach. Inflexible "one size fits all" requirements may promote consistency, but they often result in a focus on compliance over innovation. Portability solutions must work for services of all sizes and sectors, and should not create artificial barriers to new services entering the marketplace.

- **Encourage open, consistent, interoperable standards:** Industry should encourage more providers to voluntarily offer robust data portability mechanisms that are open and interoperable with industry-standard formats. Increasing portability and interoperability incentivizes providers to improve their product offerings and improves user engagement.

- **Increase consumer awareness:** Encouraging users to practice good data hygiene empowers them to make smart choices about their data. More effort should be made to educate users about data portability and what factors they should consider, such as security and data protection when choosing services.

Google's Takeout:

In 2011, Google launched a portability product called "Google Takeout." This straightforward tool enables users to download a copy of the data they store or create in a variety of industry-standard formats. Takeout (available at https://takeout.google.com/settings/takeout) has become a staple of our user control offerings and we continue to make improvements.

Allowing users to download data in multiple formats maximizes flexibility, creating many options for how users can utilize their downloaded data. Users most commonly download their data to create a copy as a backup, but Google also enables exports directly to certain competing services, including Dropbox and Microsoft OneDrive. We expect to add additional services for direct portability in the near future.

Takeout currently facilitates the export of data for more than 30 products (see appendix for details). Since launching, users have exported more than one exabyte of data and there are currently more than one million exports per month. We continue to refine the user experience and add additional functionality and products to expand the types of data users can download.

The Future-- Service-to-Service Portability:

At Google, we believe users should be able to seamlessly and securely transfer their data directly from one provider to another. To help make this possible, we are developing a prototype that can connect any two public-facing product interfaces for the purpose of importing and exporting data. This allows for a direct transfer between the corresponding platforms. This is especially important for users in developing markets as it does not require a user to upload and download the data over what may be low bandwidth connections and at potentially significant personal expense.

Our proposed approach envisions an ecosystem of adapters to convert proprietary interfaces and formats into a small number of canonical formats useful for porting data. This makes it possible to transfer data between any two arbitrary providers using existing authorization mechanisms. The sustainability of this ecosystem is supported by the inherent benefits of reciprocity; the easiest way for companies to attract new users to share their existing data is to support and maintain an interface that allows for data portability.

This approach does not address all challenges. For example, restrictions on formatting and a loss of access to specific features are not mitigated through our open source solution. However, our approach proves the concept that a substantial amount of industry-wide data portability can be achieved without changes to existing products or authorization mechanisms by most companies. In 2018 we plan to publish more detailed information about this proposal, as well as make it available in an open-source format, to demonstrate our commitment toward universal data portability.

Conclusion:

Thank you for this opportunity to share our views on the practical methods and implications of data portability. The implementation of data portability requirements, described in Article 20 of the General Data Protection Regulation, provides an opportunity to advance user control over data and, if done correctly, can achieve this without reducing incentives for continued innovation. We look forward to continuing dialogue on this and other topics.

APPENDIX:
Takeout, accessible through MyAccount, is a simple tool that enables users to download a copy of their data at anytime. Many Google products enable download from Takeout including:

- 3D Warehouse
  - 3D Models the user created
- Android Pay
  - Loyalty and gift card info
- Blogger
  - Blog data in Atom format
- Bookmarks
  - Bookmarks in structured html format that are importable into other browsers
- Calendar
  - Calendar data in iCal format
- Chrome data
  - Chrome Sync data including: autofill, bookmarks, browser history, custom dictionary, metadata about extension, and search engine settings
- Contacts
  - Contacts data in either vCard, CSV, or HTML format
- Drive (Documents, Drawings, Forms, Presentations, and Spreadsheets)
  - All drive content that you own
- Fit
  - Fitness data
- Gmail
  - Mail content in MBOX format
- Google Photos
  - Original photos, edited photos, as well as metadata and comments
- Google Play Books
  - Books you've uploaded as well as bookmarks and notes
- Google+ (+1's, Circles, Pages, Stream)
  - HTML formated data on your various social data
- Groups
  - Membership lists of all the groups you manage
- Handsfree
  - Transaction data made with the platform
- Hangouts
  - JSON formatted chat data
- Hangouts on Air
  - Q&As from events you've hosted
- Keep
  - HTML formatted data from keep, including uploaded photos
- Location history
  - JSON of KML formatted list reported location data

- Maps (Your Places, My Maps)
    - Places you have rated or stored on Maps
- Moderator
    - HTML formated Questions or Answers you have contributed to
- Panoramio
    - Photos you have uploaded
- Profile
    - Profile data you have entered
- Search history
    - HTML formatted listing of search queries
- Tasks
    - JSON formatted list of all your task data
- Voice
    - Text messages, voicemails, greetings, call and billing history
- Wallet
    - CSV Transaction History
- YouTube
    - Videos, comments, playlists, watch history, search history

June 2017

Call for Papers

Stiftung Datenschutz

Practical Implementation

of the Right to Data Portability

Concepts for Standards

for the Implementation of Art. 20 GDPR

Olvier Dion
Onecub proposal

" The PIMS approach "

onecub

Tags : PIMS, decentralization, blockchain

Abstract

Onecub is a French startup that created a PIMS (Personal Information Management System) and is a Data Portability tool for individuals.

Onecub helps companies to apply GDPR Art.20 for a limited cost and allows individuals to benefit from it through a very simple user experience.

In this paper we present our views, based on 7 years of experience in the field, of the real purposes, barriers and implications of Data Portability.

We also propose a general architecture for Data Portability based on PIMS. We extend it by presenting a decentralized solution based on the blockchain technology.

In the end we explain why we think that PIMS should be at the center of the Data Portability standards debate.

Contents

I. Who is Onecub?

In the era of Big Data, organizations have truly learned to seize the opportunities given by this revolution. Every day the costs of collecting, storing, analyzing and distributing data decrease, and the value of data goes up. However, where companies knew how to ride this wave, individuals haven't benefited from it yet. This observation is all the more absurd when we know that 75% of all data used by companies is "personal data" concerning the individuals themselves.

ONECUB, a French startup created in 2011, aims at giving individuals back the control of their data through an innovative service: a data portability tool that manages personal data exchange between users and service providers in a homogenous manner.

1. Proposed service

ONECUB is a data portability tool that allows an individual to easily gather his personal data and securely exchange it with external websites or online services via an API, ONECUB Connect. Thus, ONECUB users will be able to share their data with third party services while remaining in full control of their privacy settings, in a transparent way and to discover new ways to benefit from that data.

Companies and organizations in general will be able to provide their users more personalized services and a simplified end-user experience. Furthermore, ONECUB is an ideal solution for data controllers as it can help them respond to the new right to data portability introduced by the GDPR framework.

2. Current realizations and partnerships

Mytroc is the first online service which had integrated a ONECUB Connect Button. Currently, discussions are advanced with many online services in order to integrate a ONECUB Connect button.

2.1 Mytroc

Mytroc is a digital platform which allows its users to trade every kind of stuff. Concretely, Mytroc users have to publish an ad on the website with a picture and a description of the product that they want to exchange.

Thanks to the ONECUB Connect Button, a user can offer something to trade more easily by clicking on the ONECUB Connect button to share his online purchases history with Mytroc. In this way, he will only have to select the product that he wants to sell among all of his online purchases to publish a new ad.

2.2 Air Indemnité

Air Indemnité is an online compensation service for air passengers which takes care of the entire claim procedure in cases of delays, cancellations or overbooking. An air passenger

can claim for cancelled and overbooked flights over the past five years! To file a claim, an Air Indemnité user has to send the electronic ticket issued by the air carrier.

A ONECUB Connect button could enable the user to share directly with Air Indemnité all of his airline tickets that he purchased in the past and that he will purchase in the future.. Therefore, Air Indemnité will be able to notify the user when a compensation opportunity is identified.

2.3 Umanlife

Umanlife is a personal wellness coach which aims at influencing healthy behaviors through innovation and disruptive user experience. Umanlife suggests personalized goals as well as relevant advice and recommendations thanks to data collected. Umanlife provides, among others, a nutritional follow-up service. Such a service requires a large amount of data which is difficult to collect at the present time.

A ONECUB Connect button could enable the user to share directly with Umanlife all of the data relating to their diet thanks to the food online orders. Thus, Umanlife will be able to offer the user a simplified user experience and at the same time, give him nutritional advice tailored to his needs.

3. ONECUB engagement in the PIMS community

Onecub has been involved for 7 years in the American VRM (Vendor Relationship Management) community and in the French MesInfo community.

In 2017 Onecub has been selected by Facebook to be a part of Startup Garage Paris, a program that helps startups dealing with personal data in the context of GDPR grow.

Onecub regularly discusses GDPR key aspects and Data Portability with French startups, big companies, consulting firms and the French data protection authority.

Onecub is a member of the newly born French PrivacyTech community which aims at promoting privacy friendly technologies.

We regularly participate in GDPR related events and have already organized our own events.

II. Why do we need Data Portability?

1. Purposes and benefits

GDPR Art.20 enforces the new right for Data Portability. It will allow individuals to get their personal data back from their service providers, in order to reuse it anywhere they want. Service providers (companies, administrations, etc.) on their side are required not to oppose any kind of obstruction to the process.

This new ability given to EU citizens does not come with an obvious purpose: as mentioned in recital 68 of the GDPR, the right for data portability aims at strengthening data subjects' control over their own data. That is interesting but what are practical implications?

We can guess that almost no one will claim for his data portability rights without any direct benefit and that no business will deploy any data portability technical solution if there is no constraint or benefit related to it. So we can ask ourselves what each kind of actor is looking for within Data Portability.

1.1. For individuals

Market freedom and "the Switch"

In many occasions individuals want to switch operators for a specific service (telecommunication, utilities, bank, insurance, etc.). Each operator often tries to retain its customers by making the unsubscribing process overly complicated on the user experience point of view (unsubscription postal mail required for instance).

The other main barrier for switching is the fact that when opening a new account with a new service provider, the individual has to start from scratch, there is no continuity throughout its different operators although services are very similar form one to another.

Service provider's retention strategies and service discontinuity largely participate in the lock-in effect that traps a customer with a service provider even when the customer is not satisfied. On a market point of view, lock-in effect creates or maintain de facto monopolies and oligopolies which can be detrimental to the customer (high prices, poor service quality, etc.).

Data Portability adds fluidity to markets: it is way easier to change your telecommunication operator when you know that your phone number will stay the same. In the same time if people in general change their telecommunication operator easily, it increases competition and can lead to lower prices and better service quality. The same goes for many industries.

Task efficiency

Online services make our lives easier. We spend a smaller amount of time than before on our administrative tasks since we can fill online forms home instead of waiting in line at the service provider's office.

But at the digital era, task management is still a frustrating endeavor. We continuously fill up online forms containing the same information within various service providers and it still requires an organization effort since there does not exist any consolidated online view of our situation over our different service providers.

Data Portability would save us a lot of time and pain by allowing us to reuse the same data throughout our different services. We could reuse provided data (ex: identification data) as well as processed data (when processed data is not covered by rights of any kind: intellectual property, etc.) from one service to another in a fluid manner. Instead of giving data to a service provider we would just have to grant access to it. User experience as well as data quality online would be greatly improved by this kind of processes.

We would also benefit from a consolidated view of our general situation over our multiple service providers which would help us to stay organize and to make informed decisions (ex: consolidated view of our financial situation).

Cross domain innovation

With the boom of artificial intelligence and social networks many new online services that require a lot of personal data are reaching a wider audience:

- Digital agents (pre-sale and after-sale services)
- Virtual assistants (health coach, finance planners, travel advisors,…)
- Sharing economy marketplaces (travel housing, goods exchange, jobbing,…)
- Etc.

Many services are technically easy to build today but they cannot take off due to an overly complex user experience (ex: a health assistant that would have to ask users what they eat for each meal in order to give advice). Data Portability is finally a great opportunity to foster online innovation for these services as it will allow individuals to make use of their data through a fast and simple user experience.

Data Portability will make a multitude of new services possible and will allow service personalization like never before. Cross domain use cases can be build (ex: food and sport data reuse for a health service, travel and energy data reused for a carbon footprint calculators,…) and may unleash tremendous as well as unexpected opportunities.

1.2. For services providers

User experience

Today competition makes it essential for service providers to create a fast and simple user experience for their users. If online forms are too long, if there are too many screens or too many clicks, users can switch to the next service in a matter of seconds.

Data Portability will greatly decrease the need for online forms. If a certain data has already been provided for a certain service, it can be reused for other services which will result in reducing redundancy for the user and augment data quality at the same time.

Reaching people at the right time

Cheap modern prospection techniques like mailing have made online marketing a burden for Web users. Most of the time marketing emails are just missing their target as companies sending. They based their communication on a very limited amount of data, they just lack context (ex: gardening tools ads sent to someone living in an apartment).

Data Portability will allow businesses to gather more personal data – within user consent - in order to better understand context and propose relevant offers at the right time, to the right person.

Trust and relationship

Personal data stored by a specific company can prove useful for many use cases (ex: food purchase data can be reuse within health services, carbon footprint calculators, personal finance management services, etc.). This is why a company that would make its data easily accessible for reutilization would be really helpful for its users.

It would also be a way to build trust on the long term with users as the company would show that it firmly rejects lock-in effect.

2. Concerns and limitations

2.1. For individuals

Use cases

So far Data Portability is still expert subject matter. It does not ring a bell with the general audience as it is still an abstract concept with almost no visible practical application.

Online, people generally want to do exactly what they were doing offline before:

- Socialize
- Buy/sell goods and services
- Find a home, a job, a mate
- Play
- Etc.

The benefits they generally look for in a service are:

- Saving time
- Saving money
- Having fun
- Etc.

People will not make use of their new right for Data Portability if use cases related to it do no help them with their daily life concerns.

Privacy

The last few years have seen the accumulation of scandals, trials and media coverage that changed public opinion for good on the privacy topic. People are asking for more privacy and GDPR is the perfect example of the regulator's answer to the problem.

Data Portability is distinct from other GDPR articles as it protects users by allowing them to be freer. Unlike other articles it does not limit data circulation, on the contrary it fosters it under the strict control of the individual itself. Data Portability means more data on the marketplace and it could raise major privacy concerns in the general audience.

2.2. For companies

Companies are not supposed to make obstruction to Data Portability. So far most of them were either indifferent to the subject matter or clearly reluctant to participate in the process or even to let it happen.

Purpose

Most of the companies are focused on their everyday activities. They want to find new clients and keep the ones they already have satisfied. New use cases made possible via Data Portability are too theoretical for them so far. Short term as well as long terms benefits are hard to estimate for them, as the online world does not revolve around this principle today, they have a hard time imagining it.

Business model

Most companies highly value their customer relationship. If Data Portability becomes mainstream they clearly fear the "switch" and they fear disintermediation in general. Sometimes they can understand cross domain innovation use cases benefits but if the cost is to open the door for the switch they do not want it and will make everything they can to ignore Art. 20, diminish it or postpone its application.

Cost

GDPR in general and Art. 20 in particular raise a major concern among companies concerning costs. Who will pay for it? As Art. 20 risks are considered high and benefits are considered low, some companies do not want to invest time and money in looking for practical solutions yet. They rather wait that solutions show up on the market concerning a topic they do not fully master or even understand.

3. Scope

3.1. Industries

All the companies and administrations that offer a B2C service are concerned, when the data subject provides personal data on the basis of his or her consent or when processing is necessary for the performance of a contract.

If we limit Data Portability to the switch it gets easy to think about big companies telecommunication, banks and insurances, utilities, etc.. If we add to Data Portability task efficiency and cross domain innovation, it opens up to every domain of the economy from startups to worldwide firms and administrations.

From what we have experienced, the opinion of a company does not really depend on the industry. It is more a matter of key manager's opinion, company culture, company size, position regarding competition. In a monopoly or quasi-monopoly the company generally thinks Data Portability would help competitors to arise. In an oligopoly they fear the Switch.

3.2. Concerned data

The GDPR states that portability only applies to personal data concerning an individual that he or she has "provided to" a data controller. According to the WP29, "provided by" includes data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. On the other hand, inferred data and derived data are created by the data controller does not fall within the scope of the article 20. However, the reuse of processed data which is not covered by rights of any kind could be interesting to foster the development of innovative services. Therefore, the data processor should not be legally forced to release processed data but should be encourage to.

4. Use cases

Data	Service provider	Value proposal
Food orders	Drive and online shopping	Automatized wish lists (switch)
Utilities bills	Energy provider	Energy consumption history (switch)
Telecom bills	Telecom company	Telecom consumption history (switch
Food orders	Personal wellness coach	Personalized nutritional tips
Fashion orders	Personal shopper	Personalized fashion tips
Receipts	Administration	Proof of address
Travels	Mobile luggage storage service	A luggage storage service at the right place, at the right moment
Travels	Crowd-shipping service	Connecting individuals who want to have something delivered to others who are traveling
Trips & Energy use	Personal environmental coach	Personalized green tips
Books orders	Readings social network	Comments sharing
Job and education history	Jobbing platforms	Finding personalized job offers
Global Purchase history	Financial advisors	Personalized financial tips
Bills	Utilities/Telecom	Automatized relocation administrative tasks
Global Purchase history	Personal accountant	Automatized accountability
Etc.		

III. A general architecture for Data Portability

1. Architectural options for Data Portability

We identified 3 possible architectures for Data Portability:

Direct B2C restitution

Service providers could give data back to their users directly via a restitution button. Users could for instance get their data back in an Excel/CSV. They could decide to reuse it by importing it manually onto other services.

On the service provider side this solution is easy to implement but it is minimalist, we can barely consider this solution as Data Portability.

On the user side this solution is very manual with a poor user experience. Many people who use online services will not know how to export and import their data.

B2B transfer

Service providers could organize direct data transfer solutions with APIs. The user could ask a utility service provider to transfer his consumption data from one service to another in one click.

Considering user experience this solution is better than the previous one for a simple transfer from a service to another. Problems would arise for use cases requiring multiple data transfers at once (ex: transferring food data coming from multiple service providers to a health service that will analyze it); the user would then be asked to give his consent multiple times.

On the business side this solution would be complicated and expensive from a technical point of view. Every service provider would have to build and maintain an incredible number of APIs. They would also have to maintain relationships with many other service providers which has a non-negligible cost.

The PIMS approach

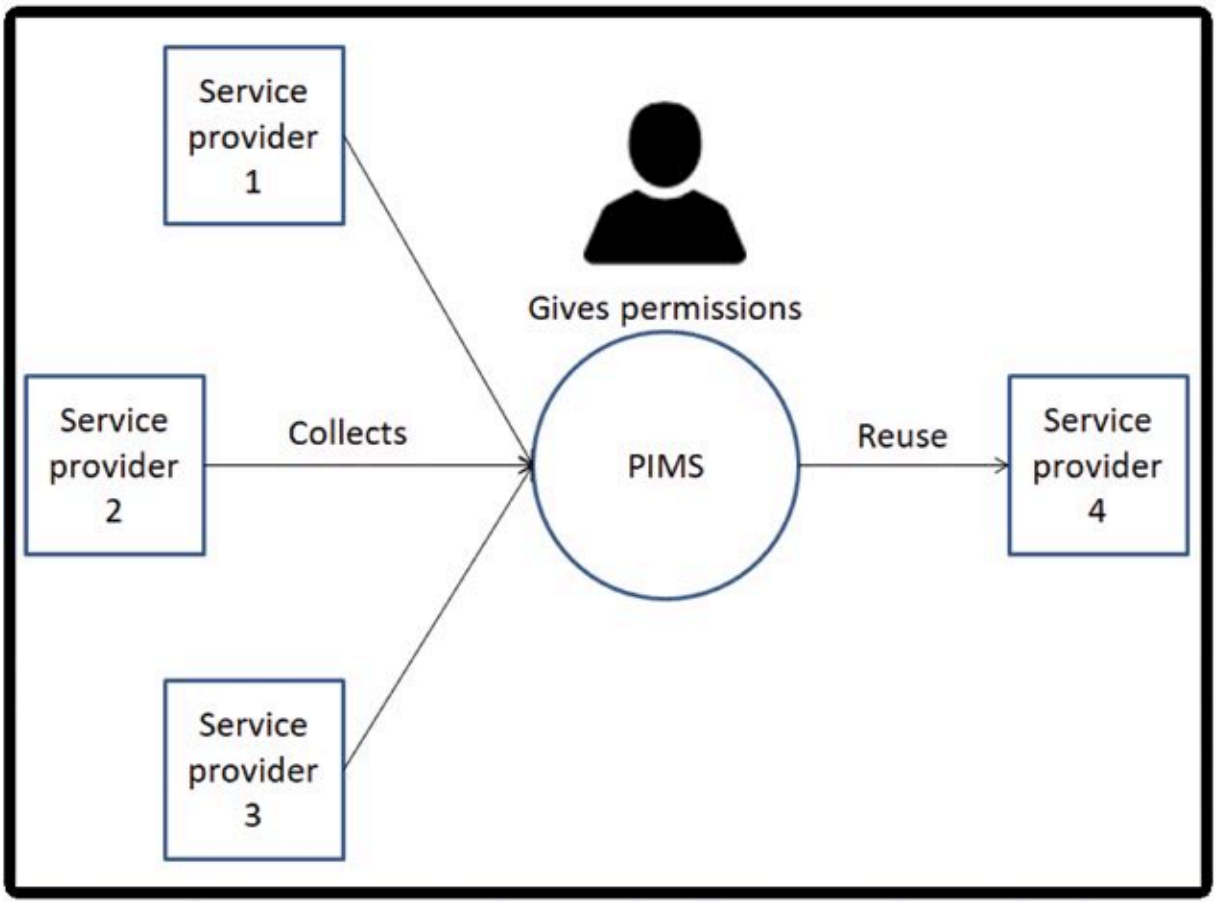
Service providers could allow their users to export their data into a tool dedicated to data portability. This kind of tool already exists under different names:

- PDS (Personal Data Store)
- VRM (Vendor Relationship Management)
- PIMS (Personal Information Management System)

From their PIMS users could reuse their data in a single click onto other services.

This solution offers a great user experience on the individual side and has a very limited cost on the companies' side. The European Data Protection Supervisor recently gave a public and very positive opinion about the PIMS solution.

2. The PIMS architecture



3. Technical solution for data collection and reutilization

The PIMS solution can mostly be based on APIs for Data collection and reutilization. APIs connect the PIMS to service providers that have to export data and other APIs connect the PIMS to other service providers that have to import.

PIMS can be standalone or web based, they can also appear as pop-ups or pop-ins directly inside service providers in order to facilitate user experience.

When individuals make use of their PIMS users have to be able to grant access to their data for collection or reutilization.

4. The PIMS data centralization problem

There exists a major concern with the PIMS architecture though. In order to allow Data Portability, PIMS have to centralize a huge quantity of data that can be highly sensitive.

Personal cloud solution

A proposed solution to this problem is to allow users to download their data in a personal cloud hosted directly on the individual's device and not in the cloud. This solution answers privacy concerns and some security concerns but can be detrimental to user experience with hard to install tools.

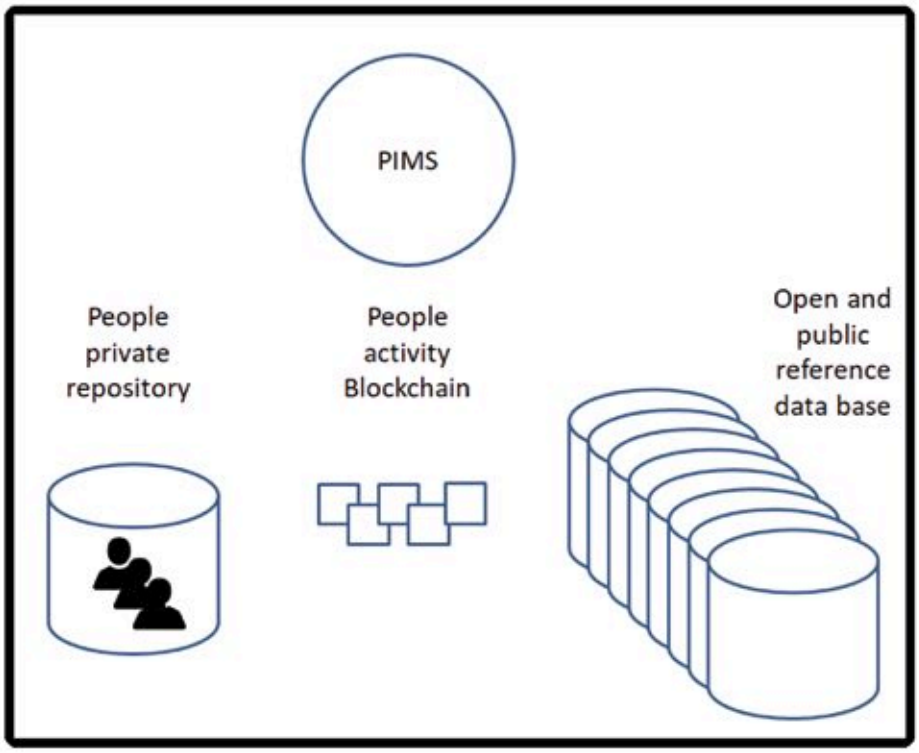
Blockchain solution

If we want to keep the system in the cloud for a simple user experience but still want to decentralize data storage we can build a data storage system based on the blockchain.

Such an architecture would be composed of:

- *A standard users' repository* managed by one or plural PIMS that keep information strictly private
- *Open and Public reference databases* containing everything a user can do online (a public E-commerce products database, a public music and movies database, a public services database, etc.). For an even more decentralized approach these public reference databases could be built on top of a P2P file system like IPFS.
- *An activity blockchain* that makes the link between a user and an item in the reference databases (ex: " Oliver bought Harry Potter on Amazon "). This blockchain would be semi-private and people could share their data through smart contracts.

In this architecture PIMS manage all the technical aspects and the user interface of the transfert but they do no store data on their servers anymore.



5. PIMS specific status

In order to build trust with PIMS which would become very central, the regulator should grant a specific status for PIMS with rights and obligations. For instance PIMS themselves would have to be compatible from one to another and they would also have to respect neutrality, they would be required to limit their action to Data Portability only.

6. Business models

A possible business model for the PIMS based architecture could be this:

- A service provider that reuses data from a PIMS pays a fee to the PIMS
- A service provider that helps the PIMS to collect information gets paid by the PIMS
- An external actor that helps to build Public reference databases get paid by the PIMS

IV. Standards and formats

1. User centric approach

Complex formats would be detrimental to the user experience and slow down adoption. Individuals should always be central when designing new formats.

New data Portability use cases would frame the format debate.

2. Not reinventing the wheel

Industry specific formats often already exist (ex: Schema.org for E-commerce) and should be preferred. A step by step approach would allow to build a sound representation of all the data that concern individuals.

3. Debating with PIMS

In order to simplify standards and formats debates, PIMS should be at the center of it as they would be use cases driven and have a cross industry view. In our opinion it is PIMS role to organize this debate, with industries and regulators.

Beispiele aus der Energiewirtschaft

Die Unternehmensarten und Marktrollen

Das Energiewirtschaftsgesetz (EnWG) trennt die Arbeitsprozesse vom Kraftwerk bis zur Steckdose in einzelne Segmente auf, die von getrennten („entbündelten“) Unternehmen angeboten werden. Das EnWG definiert folgende Tätigkeitsegmente, die dort als „Marktrollen“ bezeichnet werden:

- Die Übertragungsnetzbetreiber (ÜNB, früher Ferngasgesellschaft, Hochspannungsnetzbetreiber): Die 6 ÜNB in Deutschland (4xStrom, 2xGas) haben keinen Bezug zum Endkunden und hält keine Endkundendaten. Sie erhalten im zukünftigen Smart Meter-Regime täglich die vollständig anonymisierten Lastgänge sämtlicher Lieferstellen aus sämtlichen Verteilnetzen (s.u.) in ihrem Netzbereich.
- Die Verteilnetzbetreiber (VNB, vulgo: Stadtwerke, Gemeindewerke, Überlandwerke, in Deutschland etwa 1550 für Strom und Gas) betreiben die regionalen und lokalen Netze und stellen dem Kunden den Anschluss bereit und bedienen die dezentralen Einspeiser (Photovoltaik, Windenergie, BHKW, Biogas). Ihr Kundenkontakt beschränkt auf die An- und Abmeldung eines Anschlusses, sowie bei Schadensbehebung, Notfällen oder Zählertausch (bei Strom beispielsweise alle 8 bis 16 Jahre). In häufig wechselnden Mietverhältnissen oder erhöhter Schadensanfälligkeit entstehen Kundenkontakte bis hin zu 1 x pro Jahr, im Allgemeinen aber deutlich seltener. Während des Belieferungsverhältnisses hat der Netzbetreiber in der Regel keinen Kontakt mit dem Kunden. Es besteht kein personalisiertes Leistungs. Und Dauerschuldverhältnis zwischen Netzbetreiber und Kunden. Seine Beistellung des Netzanschlusses bietet er dem jeweiligen Lieferanten (s.u.) als Vorleistung an. Die vom Netzbetreiber gehaltenen Kundendaten sind in erster Linie Daten zur Lieferstelle, die für sie den technischen Endpunkt ihres Netzes und die technische Kundenschnittstelle darstellt.
- Die Lieferanten: Die etwa 1.200 Strom- und 900 Gaslieferanten haben den mit Abstand intensivsten Kundenkontakt. Sie sind reine Handelsunternehmen, ohne eigene Energieinfrastruktur. Sie halten die Daten sowohl für die technische Verbrauchsstelle als auch die persönlichen Kundendaten. Sie bündeln gegenüber dem Endkunden sämtliche laufenden Leistungen: Belieferung, Anschlussbereitstellung, Messung, sowie Abrechnung und Kundenbetreuung. Für die Frage der Datenportabilität und das Halten der persönlichen Daten stehen die Energielieferanten besonders im Fokus.
- Die Messstellenbetreiber (MSB): Historisch wurde der Zähler vom Verteilnetzbetreiber bereitgestellt und betrieben. Dies erfolgt bei größeren Verteilnetzen meist über eine sog. entbündelte Tochtergesellschaft oder einen Dienstleister. Die konkreten regulatorischen Anforderungen an diese Entbündelung bzw. Entflechtung befindet sich aktuell noch in der Diskussion. Der Trend geht jedoch stark zur Bildung von Verbünden, in denen mehrere Netzbetreiber gemeinschaftlich eine Messstellenbetriebsgesellschaft halten. Bisher organisierte der Messstellenbetreiber auch die Ablesung und Erfassung der Messergebnisse. In einer Zukunft des Smart Metering wird er keine Messergebnisse mehr erhalten. Sein Kundenkontakt beschränkt sich dann hauptsächlich auf den Zählertausch (vorr. alle 8 Jahre) und erforderlichenfalls eine Reparatur.
- Der Smart Meter Gateway Administrator (SMGA): ist eine „Funktionsrolle“ des MSB und nimmt somit keine eigenständige Marktrolle wahr. Der SMGA ist für den technischen Betrieb des intelligenten Messsystems (iMsys) verantwortlich. Neben Installation, Betrieb und Wartung der neuen Messinfrastruktur erbringt der SMGA eine hochgradig gesicherte Übertragung

der Messergebnisse aus dem einzelnen Zähler hin zum Empfangsberechtigten. Bei intelligenten Messsystemen soll dies demnächst in Form der sternförmigen Kommunikation geschehen, d.h. die Daten werden direkt von den Gateways zu den Empfangsberechtigten geschickt, z.B. zu den ÜNBs, VNBs oder Lieferanten. Der SMGA/MSB kann und soll somit nicht mehr wie bisher die Daten „einsehen“. Selbst dort, wo keine iMSys im Einsatz sind und somit keine direkte Übertragung aus den Gateways an den Empfangsberechtigten erfolgt, kann der SMGA/MSB die Messwerte nicht mehr einsehen, da sie für ihn verschlüsselt sind und nur in dieser Form an die Empfangsberechtigten weitergeleitet werden dürfen. In diesem Sinne ist spielt der SMGA/MSG nur noch die Rolle eines „Kanals“ und reicht die Datenpakete, ohne den Inhalt zu kennen, an die Empfangsberechtigten weiter.

Die Marktrolle des SMGWA in Verbindung mit dem MSB ist in dieser Form neu und es gibt noch wenig Betriebserfahrung, zumal es noch keine durch das BSI zertifizierten Gateways und somit iMsys gibt (fehlende sogenannte „Markterklärung“ durch die BNetzA). Derzeit werden „nur“ moderne Messeinrichtungen ausgerollt, die ohne Smart Meter Gateway arbeiten und als erste Grundlage für die neue Messinfrastruktur dienen. Auch ist abzusehen, dass ein solches Konstrukt für den Gasmarkt nicht eingeführt werden wird.

Summa Summarum: Der Energielieferant ist für über 95% aller Fälle der alleinige Ansprechpartner des Kunden, bei ihm findet sich im Zweifelsfall der breiteste Datenbestand. Die Prozesse des Lieferanten sind im Vergleich die am wenigsten regulierten. Alle anderen Akteure agieren in ihrer Datenerfassung und Datenverarbeitung in hohem Maße nach Vorgaben und Datenformaten, die von der Bundesnetzagentur vorgeschrieben sind. Aus diesem Grund konzentriert sich der vorliegende Artikel rein aus Platzgründen auf das Beispiel des Energielieferanten.

a. Allgemeine Fragen

In der bisherigen Energieversorgung galt die Verarbeitung der Daten in zum einen der Beantwortung von Fragen aus Netzsicht (Lastprofil, Art des Stromzählers, etc.). Hinzu kamen die klassischen kaufmännischen Daten, wie sie für ein Dauerschuldverhältnis typisch sind: jährliche Verbrauchsdaten, Zahlwege, Abschlagshöhe, Guthabenauszahlung/Nachzahlung am Turnusende, evtl. Zahlungsverzüge und Mahnprozesse, u.ä.

Neue Datenarten durch Smart Metering

Der zunehmende Wettbewerbsdruck und die anstehende Einführung des Smart Metering führen hier für einen Teil der Kunden zu einer Zäsur, die sich in folgenden Formen auswirkt:

a. Diejenigen Kunden, die einer Übermittlung der Lastkurven an ihren Lieferanten zustimmen, übergeben einen deutlich größeren Datenumfang als bisher üblich. Die Lastkurve wird in 96 Tagesintervallen à 15 Minuten erfasst und im Rahmen der Aufbewahrungspflicht hinweg gespeichert.
b. Unabhängig von der Art des Zählers werden Neukunden oft einem Scoring unterzogen. Die Lieferzusage erfolgt in Abhängigkeit von diesem Scoring. Dies gilt im Allgemeinen nicht für den sogenannten Grundversorger. Noch werden etwa 2/3 aller deutschen Haushalte durch den Grundversorger beliefert.

c. Bedingt durch den Wettbewerbsdruck entwickeln Lieferanten neue Produkte und Lösungen, z.B. im Bereich der Photovoltaikanlagen oder der Kraft-Wärme-Kopplung. Hinzu kommen Dienstleistungen wie etwa die Energieberatung oder Verlustanalyse. Hierfür kommen i. Allg. nur bestimmte Kundensegmente infrage, insbesondere die Immobilienbesitzer sowie Kunden, deren Jahresverbrauch im oberen Segment liegt. Lieferanten führen hier seit einer Reihe von Jahren neue Formen der Berechnung und Kundenbewertung durch.
d. Die Bundesregierung zielt mit ihrem „Gesetzt zur Digitalisierung der Energiewende“ u.a. auf die indirekte Steuerung von Verbräuchen und das Setzen von Anreizen, hausinterne Verbräuche stärker an der Verfügbarkeit von erneuerbaren Energien auszurichten. In diesem Fall ist der Lieferant auf die Lastkurve angewiesen, seine Empfehlung interagiert eng mit dem Verbrauchsverhalten im privaten Haushalt des Kunden. Noch steckt die Umsetzung hierzu in bescheidenen Anfängen, ein nennenswerter Aufwuchs ist (noch) nicht zu erkennen. Auch neue Belieferungsformen, wie etwa der sogenannten „Nachbarschaftsstrom“ (dem netzentgeltreduzierten Zuliefern erneuerbarer Energien unter Nachbarn) führen zu weiteren Zählern, zu weiteren Lastkurven und damit zu weiteren Nutzerdaten. Die aktuelle Verbreitung ist minimal, es wird – auch vom Initiator BMWi – ein ausgesprochen moderates Wachstum erwartet.

Ein Hinweis: der Kunden benötigt die ihm Rahmen der Weitergabe erhaltenen Daten nicht für weitere zukünftige Lieferverhältnisse. Die für den Lieferantenwechsel und Lieferübergang notwendigen Daten tauschen die Beteiligten (Altlieferant, Neulieferant, Netzbetreiber, Messstellenbetreiber) in BNetzA-definierten Formaten und Prozessen miteinander aus. Der Smart-Meter-Gateway-Administrator organisiert diesen Austausch. Die für einen Lieferantenwechsel notwendigen Daten findet der Kunde bereits heute auf seiner Rechnung (Zählpunkt-ID, Postadresse der Abnahmestelle, Gerätenummer, Vertragslaufzeit und Kündigungsfristen des aktuellen Liefervertrages, Netzbetreiber).

Wie eng oder weit ist die Weitergabe zu verstehen?
Die im vorigen Abschnitt unter a. bis d. beschriebenen Daten kommen zu den bisherigen Stamm- und Belieferungsdaten des Kunden hinzu. Sie sind geeignet, beim Lieferanten den Datenbestand pro Kunden in relevantem Umfang zu vergrößern. Dies betrifft insbesondere die Kunden neuer Lieferanten und die Nutzer neuer Dienstleistungsformen. Es betrifft ebenfalls sehr stark diejenigen Kunden, die über einen online angebundenen Smart Meter gemessen werden und bei ihrem Messstellenbetreiber auch tatsächlich die Auslesung der täglichen Lastkurven beauftragt haben. Die grundversorgten Kunden sind bis dato nur in minderem Maße von diesen Veränderungen betroffen.

Für die aus dem Zähler extrahierten Daten stellt die Datenweitergabe gemäß DSGVO nach erster Einschätzung keine relevante Veränderung dar. Soweit beim zuständigen Messstellenbetreiber einmal bestellt erhält der Kunde auch heute schon den vollständigen Tageslastgang in gängigem Datenformat (in >95% der Fälle in MSExcel-kompatiblem Format), selbst wenn er diesen Lastgang dem Lieferanten gar nicht zugänglich macht. Dies betrifft die Punkte a. und d. Für Daten aus dem Segment b. könnten Vergleiche mit Scoring-intensiveren Marktsegmenten einen Anhaltspunkt liefern. Für Daten aus dem Segment c. kann sehr wohl eine bisher nicht bekannte Form der Datenanforderung durch einen Kunden entstehen.

Hilfreich ist auch ein Blick auf bereits bestehende Datenweitergabe-Prozesse. So ist im Fall eines Lieferantenwechsels die automatisierte Datenweitergabe bereits seit über 10 Jahren verpflichtende Praxis. Die Bundesnetzagentur regelt diese Datenweitergabe in detailliertester Form. Sämtliche

Datentelegramme, die im Rahmen sog. EDIFACT-Dienste zwischen Lieferanten und Netzbetreibern ausgetauscht werden.

Ein Mehr an informationeller Selbstbestimmung?
Für die aus dem Zähler extrahierten und in eine Rechnung konvertierten Daten bringt die DSGVO kein erkennbares Mehr. Die betreffenden Daten erhält der Kunden entweder bereits auf der Rechnung oder der Rechnungsanlage, oder er kann sie (im Fall von Lastgängen) als elektronische Zusendung abonnieren. Auch bei den kundenspezifischen Aspekten der Belieferung – in erster Linie dem Strommix – bringt die DSGVO keine erkennbare Veränderung. Hier sind aus der Gesetzgebung, der Regulierung sowie einschlägigen Musterurteilen bereits umfangreiche Vorgaben ergangen.

Bei zukünftigen höherwertigen Smart Meter-Dienstleistungen kann sich ein solcher Mehrwert möglicherweise ergeben, insbesondere dann, wenn auf Basis der Smart-Meter Lastkurven ein komplexeres Interagieren zwischen Lieferant und Kunde erfolgt (z.B. dynamische Preisindikation, Empfehlung zur Lastverschiebung, steuerungsähnliches Signal z.B. zum Laden eines Elektromobils). Hier wäre zu prüfen, inwieweit die zugrundeliegenden Interaktionsprinzipien bereits in Vertrag, Rechnung oder Kündigungsbestätigung ausreichend ausgewiesen sind und ggf. eine Weitergabe im Sinne der DSGVO erfolgen muss.

Auch im Fall weitergehender Installations- und Betriebsdienstleistungen für Kraft-Wärme-Kopplung, Photovoltaikanlagen oder Batteriespeicher kann der Nutzer potentiell von der DSGVO profitieren. In diesem Geschäftsfeld unterscheidet sich der Energieversorger jedoch nicht mehr nennenswert von den zahlreichen Anlagendienstleistern in diesem Marktsegment. Weitergabe-relevante Daten können insbesondere auch dann anfallen, wenn der Kunde komplexere Web-Portalangebote des Lieferanten nutzt und dort durch Angaben des Nutzers eine Art Nutzerprofil entsteht. Solche Portale deuten sich bei komplexeren Interaktionen zwischen Lieferanten und Kunden an, ebenso bei Kunden mit Eigenerzeugung vor Ort (sogenannten „Prosumern“).

Insgesamt gibt es hier zurzeit jedoch nur wenige richtungsweisende Beispiele. Dies liegt nicht zuletzt daran, dass der eigentliche Smart Meter-Rollout erst am Anfang steht. Erst im Jahr 2032 ist eine flächendeckende Abdeckung vorgesehen. Die Bundesrepublik steht hier EU-weit vermutlich an vorletzter Stelle. Aus diesem Grund ist es sinnvoll, bei den neuen Energieanwendungen in einem Smart Grid ins deutlich ambitioniertere Ausland zu schauen, etwa nach Frankreich, Dänemark oder die Niederlande, die Deutschland hier etwa 10 Jahre vorauseilen. Dort muss die EU-DSGVO dank raschen Rollouts viel früher auf die zu erwartenden Webportale und ggf. damit verbundenen Nutzerprofile angewendet werden. Hintergrund dieses massiven Verzuges sind nicht zuletzt die hohen Kosten der komplexen deutschen Lösung, die weit über allen anderen europäischen Lösungen liegen.

b. Technikbezogene Fragen

Anforderungen an das Format
Die fraglichen Daten werden bei den Lieferanten in Datenbanken gehalten. Ein Export der Daten ist grundsätzlich in einem gängigen Format möglich (Text, Liste; elektronisch z.B. als odt, .doc, .pdf, .rtf oder .xls). Von den aktuell etwa 1550 Strom- und Gaslieferanten werden nur einige sehr wenige Kleinstlieferanten (etwa kleine Gemeindewerke oder einige Dutzend privater Erzeuger und

Grundversorger in ländlichen Regionen speziell Süddeutschlands) Schwierigkeiten haben, diese Daten revisionssicher zu exportieren. Diese Situation betrifft vermutlich weniger als 1% aller deutschen Energiekunden.

Entscheidend für eine erfolgreiche Erzeugung eines Datensatzes und seine Weitergabe ist die klare Festlegung dessen, was weiterzugeben ist. Der Regulierer BNetzA hat, gestützt auf Beratungsgremien aus der Energiebranche und von Energiefachleuten, in den vergangenen zwei Jahrzehnten bereits häufiger Festlegungen über die Datenweitergabe zwischen den Beteiligten getroffen. Hierbei hat er sich für das EDIFACT-Format entschieden, welches für die Kommunikation mit dem Bürger ungeeignet ist. Ein schrittweiser Übergang zu XML-Datenformaten steht zu erwarten. Dies ist für eine Weitergabe an Endkunden eher geeignet, sofern eine entsprechende Extraktionshilfe mitgeliefert wird. Auch die Weitergabe von Daten und Informationen auf der Kundenrechnung ist umfassend durch Verordnungen des BMWi, Entscheidungen der Beschlusskammern der BNetzA sowie durch einschlägige Gerichtsurteile reguliert. Diese Vorgaben könnten zu Festlegung des Umfangs der weiterzugebenden Daten zu Rate gezogen werden.

Vorteil eines branchenspezifischen Formates

Die Belieferung mit Energie ist in erster Linie ein technischer Prozess, in zweiter Linie ein kaufmännischer. Ein sektorübergreifendes Format ist hier keineswegs auszuschließen, kann jedoch u.U. einen beträchtlichen Overhead mit sich bringen und dazu führen, dass in nennenswertem Umfang leere Felder und redundante Angaben „mitgeschleppt“ werden. Eine Verdichtung von Information wie etwa auf der (elektronischen) Kundenrechnung, den Lieferantenwechsel-Datensätzen oder den elektronisch übermittelten Lastgängen geben viel mehr ein Beispiel dafür, wie kundenspezifische Daten relativ redundanzarm übermittelt werden. Es ist naheliegend, vor der Festlegung eines Formates zur Datenweitergabe diese praxisbewährten Beispiele zu Rate zu ziehen.

Verschränkung von Daten

Eine Verschränkung der Daten eines Energielieferanten ist am ehesten mit den benachbarten Bereichen der energienahen Dienstleistungen und Energiemanagementdienste zu erwarten. Auch sog. „Smart-Home“-Anwendungen und -Dienstleistungen, wie etwa aus dem Bereich der Sicherheits- oder der Seniorendienstleistungen können hier u.U. Schnittstellen bilden.

Die Verzahnung der klassischen Energiebelieferung mit komplexeren Energiedienstleistungen steht noch in einer Anfangsphase, sie ist jedoch deutlich zu erkennen. Diese Dienstleistungen werden häufig durch mit dem Lieferanten verbundenen oder ihm nahestehende Unternehmen erbracht. Feste Muster dieser Verzahnung bzw. Verschränkung müssen sich jedoch erst noch herausbilden.

Die Verbindung zu Smart-Home-Anwendungen ist bisher noch wenig ausgeprägt. Noch werden z.B. Sicherheits- und Betreuungsdienstleistungen meist über dedizierte Systeme und Plattformen erbracht, die nicht mit den Energiesystemen interagieren. Smart-Home-Systeme decken jedoch neben dem Energie- und Gerätemanagement jedoch vermehrt auch andere Funktionsbereiche des alltäglichen Lebens ab. Insofern ist mittelfristig eine Verschränkung der Energiedaten mit anderen haushaltsnahen Anwendungsbereichen zu erwarten.

c. Branchenspezifische Fragen

Durchführbarkeit

In Deutschland werden vermutlich über 80% aller Privatkunden von einem Lieferanten betreut, der diese Rechnungen mit Hilfe von SAP IS-U erstellt. In diesem Fall ist eine Datenexportfunktion dann revisionssicher umsetzbar, wenn sie deterministisch formuliert ist und algorithmisch umsetzbar ist. Dafür notwendig ist eine klare Festlegung der Daten und Parameter, die von einer Weitergabe betroffen sind. Die verbleibenden 20% wiederum werden zum größten Teil von Lieferanten betreut, die ebenfalls ein bewährtes Abrechnungs- und ERP-System anwenden und die kundenbezogene Datenweitergabe gemäß BNetzA bereits seit Jahren erfolgreich und sicher praktizieren. Auch hier besteht – eine klare Vorgabe und ein ausreichender Umsetzungszeitraum vorausgesetzt – kein Durchführungshindernis.

Entscheidend ist einzig und allein eine rechtzeitige und algorithmisch umsetzbare Vorgabe für Inhalt und Umfang der weiterzugebenden Daten, sowie eine Fokussierung auf ein oder zwei Datenformate. Entscheidend ist außerdem, dass der Kunde für sämtliche umfangreicheren Datenmengen einen validen elektronischen Übermittlungsweg angibt. Dies sollte im Normalfall ein Internet-Schließfach sein, welches die marktgängigen Datenmengen in verschlüsselter Form entgegennehmen kann.

Für die Weitergabe von Lastkurven ist Folgendes zu beachten: Je nach Granularität und Kundenwunsch können hier über die Jahre beträchtliche Datenmengen entstehen. Dies ist vor allem dann relevant, wenn der Kunde eine über 15 Minuten hinausgehende höhere Abtastdichte (heutiger Standard, entsprich etwa 35.000 Messwerten pro Jahr) wünscht. So erhöht sich beispielsweise bei minütlicher Erfassung die Zahl der Messwerte auf über eine halbe Million. Eine sekündliche Erfassung ist technisch möglich. Sollte der Kunde dies wünschen, so liegt die Datenmenge bei über 30 Mio. Messwerten pro Jahr. Als „Normalfall“ gilt die 10-Jahres-Aufbewahrungsfrist. Im Fall eines sehr hohen Datenvolumens steht zu erwarten, dass der Lieferant die Daten vor der Archivierung verdichtet, so dass „historische“ Lastkurven nicht mehr die gleiche Granularität aufweisen, wie sie zum Erfassungszeitpunkt bestanden hat.

Branche

Ergänzend zur oben beschriebenen Rollenverteilung ist für das Segment der Energielieferanten folgendes festzuhalten:

- Die Branche erfährt eine Konsolidierung. Kleinere Grundversorger bündeln sich zunehmend in Kooperationen (sog. „Shared Service“) oder lagern ihre IT an einen Dienstleister aus. Die Umsetzung der DSGVO geht operativ damit auf eine größere Leistungseinheit über. Auch unter den freien Lieferanten findet ein Konsolidierungsprozess statt.
- Die Abgrenzung der Branche gegenüber anderen Branchen ist sehr exakt zu erkennen. Sämtliche Marktteilnehmer im Sinne des EnWG verfügen über eine entsprechende Genehmigungs-Nummer, welche von den Zollbehörden des Bundes verwaltet werden.
- Ungeachtet einer gewissen Dominanz großer Marktakteure ist zu erkennen, dass sich die deutschen Energiekunden heute auf deutlich mehr – größere und auch mittelgroße – Anbieter verteilen als noch zu Beginn der Liberalisierung des Marktes um die Jahrtausendwende.

Informationstechnische Abbildung eines Kunden

Es gibt keinen umfassenden und verbindlichen Datensatz. Durch die Datenaustauschvorgaben der BNetzA (u.a. durch die Verordnungen GPKE, GeLi Gas und WiM) ist ein de-fakto-Standard entstanden, der einen Großteil der relevanten Kundendaten beinhaltet und von jedem Marktteilnehmer erzeugt und gelesen werden kann. Der hier verwendete EDIFACT-Standard ist jedoch nicht „Bürgerkompatibel". Aufgrund der Tatsache, dass ein Großteil der Lieferanten auf SAP IS-U zurückgreift und die Systemanpassungen von einigen Dutzend Spezialfirmen in Deutschland erledigt werden, ergibt sich eine weitere Tendenz zur „Verähnlichung" von Kundendaten. Ein wirklicher Standard existiert jedoch nicht. Energielieferanten pflegen hier durchaus eigene Ausprägungen, die sich insbesondere bei der Preisstellung und Tarifmodellierung zeigen.

Hierzu folgendes Beispiel: viele Rechnungen werden nach wie vor nach der i.d.R. jahresbezogenen Formel „Kosten = Grundpreis + Menge x Arbeitspreis" berechnet. Hier sind die Daten- und Tarifmodelle bei vielen Systemen ähnlich oder gar identisch. Ein Kunde, der jedoch einen sog. indexbasierten Tarif gewählt hat und bei dem z.B. der monatliche Durchschnittsbörsenpreis für Strom zugrunde gelegt wird, muss an einigen wichtigen Stellen anders behandelt werden, wie der „Standardkunde". Auch eine Wärmepumpe führt zu einem angepassten Tarifdatenmodell. Hinzu kommen oft sehr individuelle Rabattmodelle, die sich gegen eine Vereinheitlichung sperren.

Vereinheitlichung der Datenübergabe

In dem hier aufgeführten Rahmen ist eine vereinheitlichte Datenweitergabe für das Segment der Energielieferanten machbar. Als Orientierung sollten hier die Datenfelder der bereits bestehenden Datenweitergabe gemäß GPKE, GeLi und WiM dienen. Diese können durch Daten und Parameter des Vertrages und der praktizierten Rechnungslegung angereichert werden. Hinsichtlich des Formates muss ein endkundenpraktikables Format festgelegt werden, welches nicht das gegenwärtige EDIFACT-Format sein kann.

Abgrenzung zwischen bereitgestellten und verarbeiteten Daten

Die Daten eines Privatkunden werden in der Energiewirtschaft sofort nach der Bestellung weiterverarbeitet und fließt in sämtliche Beschaffungskalkulationen, Portfolio-Bewertungen, Umsatz- und Ertragsabschätzungen sowie Risikokalkulationen mit ein.

Auch bereits bei Lieferanfrage ist eine Weiterverarbeitung durchaus wahrscheinlich. So klären Lieferanten häufig noch vor der eigentlichen Bestellung, ob ein – ggf. auch kleiner – „Bestellschub" in einem spezifischen Netzgebiet ihr aktuelles Beschaffungsportfolio beeinflusst, oder aber ob in dem betreffenden Netzgebiet dadurch ein erhöhtes Risiko von Mehr-/Mindermengenkosten in der Bilanzierung mit dem lokalen Netzbetreiber droht. Dank der heute gebräuchlichen Standardlastprofile ist diese Klärung relativ einfach. In einer zukünftigen Situation mit Smart Meter-Geräten und damit ohne Standardlastprofil wird diese Klärung komplexer. Schon die Annahme von einem Dutzend Kunden mit größeren Elektrofahrzeugen kann die Kalkulation in dem betreffenden Netzgebiet „durcheinander" bringen und zu einer Einzelfallklärung führen. Übrigens sind auch Netzbetreiber mit einem Dutzend Ladestationen in einem Netzstrang durchaus herausgefordert. Eine Lieferzusage kann dann ggf. erst nach weiteren Netzinvestitionen gegeben werden. Eine solche Bestellung erfordert sowohl beim Netzbetreiber wie auch beim Lieferanten eine detailliertere Klärung.

Die hier gefragte Abgrenzung ist im Bereich der energiewirtschaftlich geprägten Belieferungsfragen recht eindeutig zu finden. Sobald der Kunde anonymisiert und auf seine Rolle als „Energiesenke“ (und ggf. zusätzlich auch Energiequelle) reduziert wird, verschwindet er in einer Art „Verbrauchsmenge“, die nach vorgegebenen Kriterien gerastert ist (insbesondere nach Netzgebiet, Art des Standardlastprofils und Art des Zählers). Weniger deterministisch ist diese Trennlinie dann, wenn der Kunden in weitere vertriebliche Aktivitäten einbezogen wird, etwa zum Vertrieb von Erzeugungs- und Speichergeräten, für Smart Home-Anwendungen, oder aber branchenfremden Angeboten. Da dies zurzeit nur in Einzelfällen und in (noch) sehr geringem Umfang praktiziert wird, fehlen hierzu die Erfahrungswerte.

Zugrundeliegende IT-Systeme

Wie im obigen Kapitel skizziert, werden in Deutschland vermutlich etwa 80% aller Lieferstellen mithilfe von SAP IS-U abgerechnet. Die verbleibenden Marktanteile werden von etwa einem Dutzend ERP-Anbieter von mittelständischer Herkunft bedient. In allen Systemen ist der massenhafte und revisionssichere Datenaustausch verankert. Erfolgsentscheidend für die technisch-betriebliche Umsetzung ist einzig und allein ein deterministisch abgegrenzter und algorithmisch umsetzbarer Datenexportauftrag.

Neu auf dem Markt sind rein Cloud-basierte Systeme. Diese stehen noch ganz am Anfang ihres Markteinsatzes, die notwendigen Betriebserfahrungen stehen deshalb noch aus. Sie arbeiten jedoch unter dem gleichen regulatorischen Regime der revisionssicheren Datenweitergabe. Insofern sind hier keine grundsätzlichen Unterschiede zu erwarten.

Praktische Umsetzbarkeit der Datenportabilität im Bereich der medizinischen Forschung

Sammelband der Stiftung Datenschutz

Autoren: Johannes Drepper*, Irene Schlünder*, Karoline Buckow*

* Geschäftsstelle TMF e.V., www.tmf-ev.de

I. Einleitung

Das mit der Regelung in Art. 20 der EU-DSGVO neu eingeführte Recht auf Datenübertragbarkeit (Datenportabilität) zielt auf eine Stärkung der Kontrolle über die Verarbeitung personenbezogener Daten durch die Betroffenen. Dieses angestrebte „Empowerment" der Betroffenen[1] ist auch im Bereich der medizinischen Forschung klar zu befürworten und zu unterstützen. Die folgende Analyse soll einen ersten Eindruck davon vermitteln, ob und ggf. in welchem Umfang dieses „Empowerment" durch den aktuellen Regelungsansatz tatsächlich erreicht werden kann und welche Probleme und offenen Fragen damit noch verbunden sind.

II. Welcher Mehrwert kann für die Betroffenen generiert werden?

Um den Mehrwert zu ermessen, der durch diese neue Regelung geschaffen werden kann, sind die dadurch unterstützten oder ermöglichten Anwendungsfälle zu betrachten, wobei hier zunächst nicht auf technische oder rechtliche und in weiteren Abschnitten noch gesondert zu analysierende Beschränkungen eingegangen wird. Die Regelung in Art. 20 EU-DSGVO unterscheidet bereits zwei Anwendungsfälle, in dem sowohl die Übermittlung der Daten an den Betroffenen selbst (Abs. 1) als auch die direkte Übermittlung von einem Verantwortlichen zum anderen (Abs. 2) als Umsetzungsmöglichkeiten der Datenportabilität gefordert werden. Allerdings wird im Zusammenhang mit der Übermittlung der Daten an den Betroffenen selbst gleich ergänzend mit darauf hingewiesen, dass dieser auch das Recht hat, die Daten dann wiederum einem anderen Verantwortlichen zur Verfügung zu stellen. Entsprechend entsteht der Eindruck, dass die Nutzung der zur Verfügung gestellten Daten durch den Betroffenen selbst weniger im Fokus des Gesetzgebers stand und hauptsächlich der direkte oder indirekte Transfer der Daten von einem Verantwortlichen zum anderen als wichtiges Ziel gesehen wurde.

Diese Gewichtung ist für das Feld der medizinischen Forschung grundsätzlich nachvollziehbar, wenngleich einschränkend hinzugefügt werden muss, dass in Einzelfällen durchaus auch die Nutzung oder Verwaltung der Daten durch die Betroffenen selbst von diesen gewünscht sein kann. Auch wenn der Begriff des „Patient Empowerment" häufig unscharf und mit wenig konkreten Beispielen unterlegt verwendet wird, ist doch festzustellen, dass sich Patienten heute mehr für ihren eigenen Gesundheitszustand und aussagekräftige Daten hierzu interessieren als früher. Oft wird jedoch die Komplexität der heute typischerweise erfassten Gesundheitsdaten und deren Interpretationsbedürftigkeit den Nutzen der Daten in der Hand der Betroffenen allein stark

[1] Die Article 29 Data Protection Working Group spricht in ihrer Guideline zur Datenportabilität von einem „user empowerment", siehe Artikel-29-WP *Guidelines on the right to data portability. Adopted on 13 December 2016. As last Revised and adopted on 5 April 2017*. 2017. Article 29 Data Protection Working Party, WP 242, rev.01, http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (Abruf: 2017-07-31)., S. 3

einschränken. Nichtsdestotrotz können Betroffene und insbesondere Patienten natürlich indirekt davon profitieren, dass mehr Einrichtungen auf ihre elektronischen Gesundheitsdaten zugreifen können, so dass die Steuerung des hierfür verantwortlichen Prozesses auch im guten Sinne als Patient Empowerment verstanden werden kann.

Somit kann auch die Bereitstellung eigener Daten für die Forschung bzw. der Transfer der Daten von einer Stelle zu einer anderen im Interesse des Betroffenen sein, indem damit z. B. die Forschung zu seiner Krankheit unterstützt wird. Entsprechend ist die Frage zu stellen, welchen Nutzen der Transfer von Forschungsdaten von einer forschenden zur anderen forschenden Stelle stiften kann. Zunächst ist festzuhalten, dass es sehr unterschiedliche Arten von medizinischen Forschungsprojekten gibt[2], so dass eine pauschale Antwort immer fehlgehen muss. Experimentelle klinische Prüfungen, die mit dem Arzneimittelrecht einer eigene Regulierung unterliegen, sind typischerweise als Einheit zu verstehen, derart, dass die Durchführung von Anfang bis Ende bei ein und derselben verantwortlichen Stelle liegt. Insofern ist hier kaum der Anwendungsfall zu sehen, dass eine neue verantwortliche Stelle die klinische Prüfung einer anderen Forschungseinrichtung weiterführt und auf die bisher erhobenen Daten angewiesen wäre. Im Bereich von über einen längeren Zeitraum laufenden epidemiologischen Forschungsvorhaben ist schon eher davon auszugehen, dass in bestimmten Fällen auch Interesse an den Daten einer Vorerhebung bestehen kann. Aber auch dieser Anwendungsfall wird aller Erwartung nach nicht sehr häufig vorkommen. Ein mögliches Szenario wäre, dass beispielsweise für eine Kohortenstudie bestimmte Ein- und Ausschlusskriterien bestehen und die Rekrutierung für diese Studie davon profitiert, dass Daten aus einer früheren Erhebung mit ausgewertet werden können. Wenn die Probanden bereit wären, ihre Daten aus der früheren Erhebung zur Verfügung zu stellen, könnte dann ggf. das Screening vereinfacht werden.

Spannender sind Anwendungsfälle, die die Grenze zwischen medizinischer Versorgung und Forschung überschreiten bzw. sich auf integrierte und übergreifende Datensammlungen beziehen. Die Nachnutzung klinischer Versorgungsdaten in der Forschung wird häufig als Sekundärnutzung klinischer Daten angesprochen und umfasst eine ganze Reihe unterschiedlicher Anwendungsfälle. Diese reichen von Machbarkeitsanalysen über die Rekrutierungsunterstützung bis hin zur direkten Verwendung von Versorgungsdaten in der Forschung nach dem Single-Source-Paradigma.[3] Nicht alle diese Anwendungsfälle werden von einer besser unterstützten Datenportabilität, die ja immer nur dann notwendig ist, wenn unterschiedliche Stellen involviert sind, gleichermaßen profitieren und auch der Nutzen der Betroffenen kann sich sehr unterscheiden und wird regelmäßig ein nur mittelbarer sein, da die Forschungsprojekte den Betroffenen selbst oft nicht direkt helfen können.

Bei bestimmten Erkrankungen, für die noch keine ausreichende und standardisierte Therapie existiert und die daher intensiv beforscht werden – z. B. im Bereich der Onkologie oder der seltenen Erkrankungen – besteht heute eine sehr intensive Verzahnung von Forschung und Versorgung, was auch Konsequenzen für die Datenhaltung und –übermittlung hat. In diesen Fällen können Forschungsergebnisse auch sehr direkt für Patienten von Nutzen sein und die enge Kooperation forschender und behandelnder Einrichtungen ist sowohl für die Behandlung wie für die weitere Forschung essentiell. Beispielsweise kann sich ein bestimmter, im Rahmen eines Forschungsprojekts

[2] siehe Röhrig, B., Prel, J.-B.d., Wachtlin, D., Blettner, M., *Studientypen in der medizinischen Forschung.* Dtsch Arztebl International, 2009. **106**(15): S. 262-268.

[3] Übersicht und weiterführende Literatur in Drepper, J., Prokosch, H.U., Dugas, M., Semler, S.C., *Sekundärnutzung klinischer Daten*, in *IT-Infrastrukturen in der patientenorientierten Forschung ‚Aktueller Stand und Handlungsbedarf 2016*, Hrsg.: J. Drepper and S.C. Semler. 2016. S. 165-193.

festgestellter Genotyp eines Patienten später als hoch behandlungsrelevant herausstellen. Das Behandlungsergebnis wiederum wäre als Datensatz für die weitere Forschung von großem Interesse. Darüber hinaus könnte das Einholen einer Zweitmeinung zur weiteren Behandlung auf Basis von Daten aus der Versorgung oder auch der Forschung für Patienten von Interesse sein.

Vor dem Hintergrund solcher Anwendungsfälle und auf der Basis darüber hinaus gehender Überlegungen hat das Bundesministerium für Bildung und Forschung (BMBF) 2015 das „Förderkonzept Medizininformatik“ vorgestellt.[4] Im Rahmen dieses groß angelegten Förderprojekts werden bundesweit an vielen universitätsklinischen Standorten Datenintegrationszentren entstehen, deren Aufgabe es ist, die Daten aus der Versorgung der Patienten und aus durchgeführten Forschungsprojekten in integrierter Form sowohl für die Behandlung als auch für die Forschung zur Verfügung zu stellen. Dieses langfristig angelegte Projekt wird darüber hinaus auch die vermehrte Entwicklung und Anwendung von Datenstandards in Forschung und Versorgung befördern und somit auch bessere Voraussetzungen für die Datenportabilität im Bereich der Medizin schaffen.

Angesichts dieser Entwicklungen kann das neu eingeführte Recht auf Datenübertragbarkeit die aktuelle Entwicklung unterstützen, die Betroffenen zu aktiven und gestaltenden Akteuren in einem hoch dynamischen und von intensiver Datennutzung geprägten Umfeld machen.

III. Welche Einrichtungen sind betroffen?

Wie bereits gezeigt, sind im medizinischen Bereich Forschungsdaten und Behandlungsdaten vielfach verschränkt, da klinische Studien auch Teil der Behandlung sind und umgekehrt Routinedaten aus der Behandlung zur Forschung – sowohl der biomedizinische Forschung als auch der Versorgungsforschung herangezogen werden. Wenngleich eine Abgrenzung aus datenschutzrechtlicher Sicht vielfach von den Datenschutzaufsichtsbehörden eingefordert wird, weil der Verwendung von Behandlungsdaten für Forschungszwecke regelmäßig eine Zweckänderung innewohnt, die einer Rechtsgrundlage bedarf, so fragt es sich doch, inwieweit eine Abgrenzung aus Sicht des Patienten relevant ist. Für ihn sind Gesundheitsdaten eben Gesundheitsdaten, unabhängig davon wofür sie erhoben wurden. Eher interessant dürfte es für ihn sein, wo sie gespeichert sind und von wem sie genutzt werden. Auch im Rahmen der Portabilität liegt das erste Interesse des Patienten darin, sich an diejenige Einrichtung zu wenden, die über die größte Schnittmenge an Daten verfügt. Dies dürfte in vielen Fällen die behandelnde Einrichtung sein, unabhängig davon, ob diese Studienzentrum im Rahmen einer klinischen Prüfung war und in diesem Kontext Daten erhoben wurden, die im reinen Behandlungszusammenhang nicht erhoben worden wären, oder der Patient im Krankenhaus tatsächlich nur behandelt wurde.

Entsprechend sind für viele klinische Forschungsprojekte zunächst behandelnde Einrichtungen zu berücksichtigen, die Studien verantwortlich durchführen. Dies sind alle Universitätsklinika in Deutschland, sicher aber auch viele andere größere Krankenhäuser. Arztpraxen oder Medizinische Versorgungszentren (MVZ) werden hingegen eher im Einzelfall zu berücksichtigen sein, da diese deutlich seltener eigenverantwortlich Forschungsprojekte durchführen. Zusätzlich sind institutionalisierte Forschungseinrichtungen bzw. Institute der großen Forschungsverbünde in Deutschland zu betrachten. Hierzu gehören diejenigen Institute der Fraunhofer-Gesellschaft, der Leibniz-Gemeinschaft, der Helmholtz-Gemeinschaft sowie der Max-Planck-Gesellschaft, die ebenfalls

[4] siehe BMBF *Förderkonzept Medizininformatik. Daten vernetzen – Gesundheitsversorgung verbessern*. 2015. Bundesministerium für Bildung und Forschung (BMBF), Referat Methoden- und Strukturentwicklung in den Lebenswissenschaften, https://www.bmbf.de/pub/Medizininformatik.pdf (Abruf: 2017-11-09).

eigenverantwortlich medizinische Forschungsprojekte durchführen und in diesem Rahmen personenbezogene Daten erheben oder verarbeiten.

Im industriellen Bereich sind natürlich die forschenden Arzneimittelhersteller anzusprechen, die im Rahmen der Zulassung neuer Arzneimittel oder veränderter Indikationen klinische Prüfungen oder auch Beobachtungsstudien durchführen. Letztere werden zudem auch von vielen Herstellern nicht zulassungspflichtiger Medikamente durchgeführt. Neben den Arzneimittelstudien sind aber auch Studien zur Evaluation und Zulassung von Medizingeräten wie etwa Diagnostika zu betrachten, die von den Produktherstellern durchgeführt werden.

Viele der genannten Firmen und Hersteller bedienen sich bei der Durchführung ihrer Studien sogenannter Auftragforschungseinrichtungen, so dass je nach konkreter Aufgabenverteilung und Verantwortlichkeit von der Pflicht zur Gewährung der Datenportabilität auch diese Institutionen betroffen sein können.

Daneben gibt es eine Vielzahl kleinerer Organisationen, Institute und Gesellschaften, die Forschungsprojekte unterschiedlichster Art durchführen. Zu nennen wären hier etwa Patientenverbände (die z. T. Register zu ihren Erkrankungen aufbauen und betreuen), Fachgesellschaften (die z. T. ebenfalls Register betreiben) sowie für einzelne Forschungsanliegen als Verein, Stiftung oder auch GmbH gegründete Institutionen.

Somit wird deutlich, dass die Anforderungen zur Unterstützung der Datenportabilität im Bereich der medizinischen Forschung auf eine Vielzahl sehr unterschiedlich aufgestellter Einrichtungen treffen, so dass sich zu den Umsetzungsvoraussetzungen diesbezüglich alle pauschalen Aussagen verbieten.

IV. Welche Daten müssen portabel gemacht werden?

1. Für medizinische Forschungsprojekte relevante Datenarten

Wie bereits gezeigt, ist in Bezug auf die Datenportabilität in der medizinischen Forschung immer ein sektorübergreifender Blick notwendig, der die Gesundheitsversorgung von Patienten immer mit einschließt. Auch hinsichtlich der Daten ist von einer großen Überschneidung beider Bereiche auszugehen. In beiden Sektoren werden primär Gesundheitsdaten nach Art. 9 (1) EU-DSGVO erhoben und verarbeitet, was zunächst übersichtlicher klingt, als es tatsächlich ist. Da wären zuerst einmal die Krankheiten selbst, welche beschrieben sein wollen. Aber schon dabei ist zusätzlich zu unterscheiden, was Symptome, was Ursachen und was vielleicht die Folgen einer Erkrankung sind. Zusätzlich zu den konkreten Ursachen sind vielleicht auch noch allgemeine Risikofaktoren zu berücksichtigen, die gerade in der präventiven Medizin von immenser Bedeutung sind. Je verfeinerter die eingesetzte Diagnostik, desto detaillierter muss auch die diagnostische Methode selbst dokumentiert werden. Von besonderer Bedeutung ist in diesem Zusammenhang die genetische Diagnostik, die zu immer kleineren Subgruppen in Bezug auf die Auswahl der Therapie führt, was häufig mit dem Schlagwort der Präzisions- oder personalisierten Medizin belegt wird.

Der Umfang der notwendigen medizinischen Dokumentation geht allerdings weit über die Erfassung und Beschreibung von Krankheiten hinaus. Nicht nur diagnostische, auch therapeutische Maßnahmen sind zu dokumentieren. Hier wären als Beispiele die zahllosen Medikamente oder die immer komplexer werdenden chirurgischen Eingriffe zu nennen. Schon die Arzneimitteldokumentation weist bei Berücksichtigung der Wirksubstanzen, des Wirkprinzips bzw. bestimmter chemischer Eigenschaften, der Darreichungsform, der Indikation und nicht zuletzt ggf. eines oder mehrerer Handelsnamen eine erhebliche Komplexität auf.

Wer meint, die medizinische Dokumentation erschöpfe sich in Diagnostik und Therapie, hat allerdings „die Rechnung ohne den Wirt“ gemacht. In diesem Falle wären als namhafte Wirte in unserem Gesundheitswesen z. B. die Kostenträger zu nennen, die insbesondere ein Interesse an den finanziellen Aspekten von Krankheiten und deren Behandlungsmöglichkeiten haben. Dieses Interesse führt mehr oder weniger direkt zu einer ganzen Reihe dokumentatorischer Anforderungen, die mindestens teilweise eher organisatorischer als rein medizinischer Natur sind. Organisatorische Detailinformationen in der Dokumentation spiegeln jedoch nicht immer nur das Interesse des Controllings oder der Kostenträger wieder, sondern können auch auf haftungsrechtliche oder ethische Gründe zurückgehen. Als Informationen mit nicht primär medizinischer Relevanz wären beispielsweise solche zur Identifikation eines Patienten, seiner Kassenzugehörigkeit, bzw. seines Abrechnungsstatus oder seiner Überweisungs- und Verlegungshistorie zu nennen.

Nicht nur die medizinischen im Rahmen von Diagnostik und Therapie erhobenen Daten sind potentiell auch für die Forschung von Interesse. Auch die zuletzt genannten administrativen Daten können im Kontext der Versorgungsforschung bedeutsam werden, um z. B. das problematische Spannungsfeld zwischen medizinischen und ökonomischen Notwendigkeiten auszuleuchten.

In den letzten Jahren werden zudem zunehmend Gesundheitsdaten von Patienten und gesunden Bürgern selbst erfasst, seien dies beispielsweise mit Hilfe von „Wearables“ gemessene Vitaldaten oder sogenannte Patient Reported Outcomes (PRO) im Rahmen von Studien, wie sie etwa in Form von Patiententagebüchern oder Online-Fragebögen erfasst werden.

Noch einmal umfangreicher wird die Datensammlung, wenn auch im Rahmen der Forschung zusätzlich erhobene Daten zu berücksichtigen sind. Neben Patienten werden dann ggf. auch noch gesunde Kontrollprobanden eingeschlossen, untersucht und dokumentiert. Wichtig sind beispielsweise Informationen zum Untersuchungsansatz, zur Zugehörigkeit eines Probanden zu einer experimentellen Gruppe, zum Zusammenhang einer Nebenwirkung mit der zu untersuchenden Heilmethode, zu Ein- und Ausschlusskriterien für eine Studienteilnahme und schlussendlich auch zur Entblindung eines Datensatzes.

Nun kann berechtigterweise gefragt werden, ob alle diese Daten auch in personenbeziehbarer Weise für die Forschung benötigt werden. Nur in diesem Falle wären sie von der Anforderung einer Herausgabe an den Betroffenen oder andere Diensteanbieter im Rahmen der Datenportabilität betroffen. Aber schon wenn administrative oder medizinische Daten z. B. für die Untersuchung der Versorgungshistorie über verschiedene Einrichtungen hinweg zusammengeführt werden sollen, geht dies regelmäßig nur in personenbeziehbarer bzw. pseudonymer Art und Weise.

2. Einschränkungen gemäß Art. 20 DSGVO

Gemäß Art. 20 Abs. 1 DSGVO unterliegen nur solche Daten dem Portabilitätsgebot, die personenbezogen sind und die vom Datensubjekt selbst dem Verantwortlichen bereitgestellt wurden. Während es sich von selbst versteht, dass anonyme Daten nicht an den Betroffenen herausgegeben werden können, weil ja Voraussetzung der Anonymität ist, dass eben nicht mehr nachvollziehbar ist, wer der Betroffene hinter den Daten war, ist die Abgrenzung bezüglich des Merkmals „selbst bereitgestellt“ wesentlich schwieriger. Denn man darf sicherlich davon ausgehen, dass es sich nicht allein um Daten handeln soll, die ausdrücklich vom Datensubjekt übergeben wurden etwa durch Eintippen in eine Maske. Dies bestätigt auch die Art. 29 Arbeitsgruppe in ihren „Guidelines on the right to data portability“, nach der auch „Beobachtungsdaten“ zu den vom Datensubjekt

bereitgestellten Daten gehören sollen.[5] Im Gegensatz dazu stehen Daten, die vom Verantwortlichen generiert wurden, wie z. B. Kreditscorings und der Gesundheitsstatus eines Menschen. Die Art. 29 WP führt hierzu aus:

> *"A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":*
> *- Data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.)*
> *- Observed data provided by the data subject by virtue of the use of the service or the device. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device."*[6]

In anderen Worten: Beobachtungsdaten, die das Verhalten eines Menschen lediglich widerspiegeln, sollen erfasst sein, Ergebnisse von Analysen dieser Daten aber nicht. Dies klingt zunächst einleuchtend, ist es aber bei näherer Betrachtung kaum. Denn häufig liegt in der Bobachtung bereits eine mehr oder weniger umfassende Analyse. Denn beobachten heißt auch immer messen, und messen kann man nur unter Anwendung oder zumindest Voraussetzung bestimmter wissenschaftlicher Methoden. Wenn man sich das Beispiel genauer anschaut, dass die Art. 29 Arbeitsgruppe für reine Beobachtungsdaten anführt, nämlich die Herzaktivität bei Fitnessaktivitäten, so wird schnell deutlich, dass bereits dieser Messung eine komplexe Technologie zugrunde liegt. Bei sogenannten Wearables, die umfassende Verhaltens- und Gesundheitsdaten protokollieren, wird das noch deutlicher. Eine andere Idee wäre, daran anzuknüpfen, ob ein Datensubjekt grundsätzlich in der Lage wäre, die Analyse selbst durchzuführen. So gibt es inzwischen diverse Analysemaßnahmen zur Selbstanwendung, wie etwa Messungen des Blutzuckerspiegels oder Schwangerschaftstests.

Umgekehrt kann man sich zu Recht fragen, ob z. B. die reinen Genomsequenzdaten oder andere genetische Daten tatsächlich interpretierte Daten sind oder nicht eher den sogenannten Rohdaten zuzuordnen. In diesem Sinne werden genetische Daten etwa von Fleischer, Winkler, Schickhardt und Taupitz in Bezug auf die heute bestehenden Auskunftsrechte dann als Rohdaten eingeordnet, wenn zwei Voraussetzungen erfüllt sind: Die Daten müssen erstens aus einem anfänglichen oder intermediären Arbeitsschritt resultieren und dürfen selbst noch keine wissenschaftlichen Ergebnisse darstellen. Die Daten dürfen zweitens bezüglich ihrer spezifischen medizinischen (und sozialen) Bedeutung für den Betroffenen noch nicht näher differenziert, bestimmt oder interpretiert worden sein.[7]

Im Ergebnis wird klar, dass das Kriterium der Bereitstellung der Daten durch das Datensubjekt eine deutliche Einschränkung in Bezug auf die in der medizinischen Forschung verwendeten und gespeicherten Daten darstellt. Andererseits werden Umfang und Vielfalt der für die Datenportabilität relevanten Daten unter Einschluss sogenannter Beobachtungsdaten immer noch erheblich sein. Und

---

[5] Artikel-29-WP *Guidelines on the right to data portability. Adopted on 13 December 2016. As last Revised and adopted on 5 April 2017*. 2017. Article 29 Data Protection Working Party, WP 242, rev.01, http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (Abruf: 2017-07-31).

[6] ebd.

[7] Fleischer, H., Schickhardt, C., Taupitz, J., Winkler, E.C., *Das Recht von Patienten und Probanden auf Herausgabe ihrer genetischen Rohdaten. Eine rechtliche und ethische Analyse samt einer Empfehlung für die Praxis.* MedR, 2016. **2016**(34): S. 481-491.

letztlich macht gerade der erste Interpretationsversuch der Art. 29 Arbeitsgruppe klar, dass noch eine erhebliche Rechtsunsicherheit dahingehend besteht, ab wann Daten nicht mehr als vom Betroffenen selbst bereitgestellt angesehen werden können.

Gemäß Art. 20 Abs. 4 DSGVO darf das Recht auf Portabilität, das auch das Recht einschließt, die Daten auf Wunsch des Datensubjekts direkt an einen Dritten zu übermitteln, zudem die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Insofern muss nach Aussage der Art. 29 Arbeitsgruppe für die Übertragung der Daten Dritter ein eigener Rechtsgrund bestehen. Im Rahmen medizinischer Forschungsvorhaben stellt sich das Problem der Rechte Dritter allerdings nicht erst seit dem Recht auf Portabilität. In Anamnesen werden beispielsweise regelmäßig Informationen zum Gesundheitsstatus naher Verwandter abgefragt, eventuell auch zum Familienleben. Auch die genetische Diagnostik kann zu Ergebnissen führen, die auch die Rechte Dritter berühren. Dabei wird deutlich, dass eine starke Einschränkung auf das Kriterium der Bereitstellung durch das Datensubjekt selbst, auch das Problemfeld der Rechte Dritter helfen könnte einzugrenzen. Da das Datensubjekt im engeren Sinne selbst bereitgestellte Daten offensichtlich hinsichtlich des darin enthaltenen Informationsgehalts auch anderen Einrichtungen zur Verfügung stellen kann, führt das Recht auf Datenportabilität zunächst nicht zu einer neuen Art von Risiko für die Rechte Dritter. Nichtsdestotrotz bleibt die Prüfung notwendigerweise eine Aufgabe der verantwortlichen Institution, so dass auch diesbezüglich von einer erheblichen Rechtsunsicherheit auszugehen ist, die Forschungseinrichtungen nicht unerheblich belasten kann.

Unabhängig von dem neuen Recht auf Datenportabilität bestehen weiterhin umfangreiche Auskunftsrechte, in der DSGVO in Art. 15 geregelt. Diese beziehen sich auf alle personenbeziehbaren Daten und unterliegen nicht den oben genannten Einschränkungen. Insofern sind auch abgeleitete bzw. nicht vom Datensubjekt selbst bereitgestellte Daten davon umfasst. Auf diese bereits heute bestehenden Rechte wird in den Einwilligungserklärungen in Forschungsprojekten hingewiesen und entsprechende Umsetzungen sind üblicherweise implementiert. Allerdings führen auch diese Rechte, insbesondere aufgrund der Einbeziehung neuer Befunde und abgeleiteter Daten, auch heute schon zu schwer lösbaren Konflikten. So können genetische Untersuchungen zu schwer einschätzbaren Risikohinweisen führen, die für die Betroffenen ein starkes Verunsicherungspotential bergen. Das Gendiagnostikgesetz sieht für solche Rückmeldungen daher entsprechend hohe Auflagen vor. Da das Gendiagnostikgesetz jedoch die Forschung explizit ausnimmt und das Datenschutzrecht auf solche Problemstellungen nicht eingeht, stehen die medizinischen Forscher hier vor der Herausforderung, eigene Lösungen zum Umgang mit diesem Auskunftsanspruch zu finden.[8]

V. Welche Datenformate bieten sich an?

Die Datenschutzgrundverordnung (DSGVO) beschreibt das Recht auf den Erhalt personenbezogener Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“. Was bedeutet das? Und inwiefern sind Daten, die diese Anforderungen erfüllen, für eine Nachnutzung geeignet? Im Folgenden werden die Anforderungen an eine Kompatibilität beschrieben, die einen Austausch und nachgelagerte Weiternutzung von Daten – auch sektor- und branchenübergreifend – ermöglichen.

1. Anforderungen an ein kompatibles Format

Ausgehend von der Forderung in der Datenschutzgrundverordnung müssen die bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format vorliegen – eine Formulierung, die

[8] zur internationalen Diskussion vergl. etwa Knoppers, B.M., Zawati, M.H., Senecal, K., *Return of genetic testing results in the era of whole-genome sequencing.* Nat Rev Genet, 2015. **16**(9): S. 553-559.

angesichts der in vielen Bereichen des Gesundheitswesens fehlenden Standardisierungsvorgaben sehr viel Spielraum für Umsetzungen lässt, die vermutlich sehr zweckgerichtet angegangen werden. Eine Herausgabe von Daten in einem kompatiblen Format ist nicht gefordert und wäre auch nicht ausreichend konkret. Kompatibilität in Bezug auf den Austausch von Daten wird erreicht, wenn zwei Systeme derart aufeinander abgestimmt sind, dass Daten ohne einen Zwischenbearbeitungsschritt von dem einen in das andere System überführt werden können. Im Gesundheitswesen gibt es eine Reihe branchen- und sektorspezifischer Formate. Ein Datenaustausch über diese Grenzen hinweg wäre damit nicht gelöst. Gerade dieser wäre jedoch notwendig, um denkbare Anwendungsfälle für Datenportabilität im Gesundheitswesen bedienen zu können, wie beispielsweise

- der Transfer klinischer Versorgungsdaten in eine elektronische Patientenakte,
- die Mitnahme von Behandlungsdaten im Falle eines Arztwechsels oder im Zuge einer Überweisung,
- die Entscheidung für eine Data Donation persönlicher Gesundheits- oder Behand-lungsdaten für Forschungszwecke und die damit verbundene Übertragung relevanter Daten sowie
- die Befüllung klinischer Krankheitsregister mit Versorgungsdaten.

Die Anforderungen für entsprechende Nachnutzung oder sektorübergreifende Weitergabe von Daten gehen einen Schritt weiter und bedürfen einer Interoperabilität – denn Interope-rabilität erlaubt einen Datenaustausch zwischen verschiedenen Systemen ohne bedeutenden Informationsverlust. Auch die DSGVO nennt in Erwägungsgrund 68 als Anforderung das Kriterium der Interoperabilität. Dabei sind verschiedene Ebenen zu berücksichtigen: die strukturelle Interoperabilität (ein gemeinsames Datenmodell), die syntaktische Interoperabilität (eine gemeinsame Syntax) und die semantische Interoperabilität (ein gemeinsames Verständnis der Dateninhalte).[9] Nur unter Berücksichtigung aller drei Ebenen kann ein Informationsverlust beim Austausch von Daten so gering wie möglich gehalten und damit ein gemeinsames Verständnis der Daten gewährleistet werden.

Interoperabilität erfordert die Verwendung abgestimmter Standards – gerade dieser Abstimmungsprozess ist komplex, da viele Interessensvertreter eingebunden werden, die Heterogenität der Daten im deutschen Gesundheitswesen und der gesamte Datenlebenszyklus berücksichtigt werden müssen. Dieser Aufgabe stellt sich aktuell die vom Bundesministerium für Bildung und Forschung geförderte Medizininformatik-Initiative[10], die es sich zum Ziel setzt, den Austausch von Forschungs- und Versorgungsdaten durch IT-Lösungen zu ermöglichen. Die Arbeitsgruppe Interoperabilität der Initiative beschäftigt sich in diesem Zusammenhang mit der Abstimmung von Standards und Formaten um eine Auswertung von Daten über Standorte hinweg zu realisieren. In einem ersten Schritt wurde die erste Version eines Kerndatensatzes erarbeitet, der modular aufgebaut und damit für zukünftige Anforderungen erweiterbar ist (siehe Abbildung 1).

[9] Rühle, S. *Kleines Handbuch Metadaten - Metadaten*. 2012. Kompetenzzentrum Interoperable Metadaten (KIM), http://www.kim-forum.org/Subsites/kim/SharedDocs/Downloads/DE/Handbuch/metadaten.html (Abruf: 2017-09-10).

[10] www.medizininformatik-initiative.de

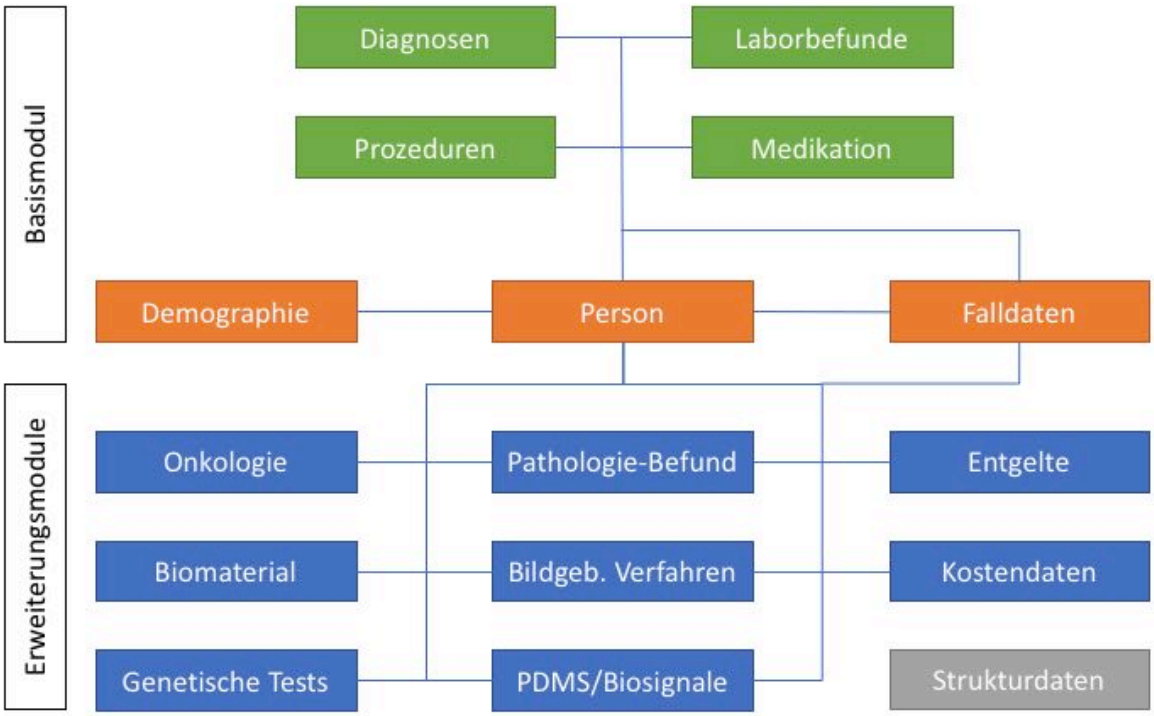


Abbildung 1 – Kerndatensatz der Medizininformatik-Initiative
Schematische Darstellung des Kerndatensatzes der von der Arbeitsgruppe Interoperabilität im Rahmen der vom BMBF geförderten Medizininformatik-Initiative entwickelt wurde. Der Kerndatensatz ist modular aufgebaut und umfasst ein umfangreiches Basismodul sowie verschiedene Erweiterungsmodule.

Das Kerndatensatz-Dokument führt in der aktuellen Ausbaustufe für jedes Modul Vorschläge zur Strukturierung und Codierung sowie zum Vorgehen hin zu einer übergreifenden Auswertbarkeit der in dem Modul enthaltenen Daten auf. Eine Harmonisierung der Daten über alle Standorte der MI-Initiative hinweg ist notwendig um übergreifende Auswertungen mit überschaubarem Aufwand bedienen zu können und stellt gleichzeitig einen Meilenstein für das Datenmanagement im deutschen Gesundheitswesen dar.

2. Vergleich branchenspezifischer und sektorübergreifender Formate

Schon allein im Bereich der medizinischen Versorgung ist die Zahl der verwendeten und propagierten Standards immens. Daher soll hier auf die wichtigsten Vertreter aus Forschung und Versorgung und ihre jeweilige Bedeutung für die Datenportabilität fokussiert werden. Nicht zuletzt ist von Interesse, in welchen Bereichen derzeit der größte Entwicklungsbedarf gesehen wird und inwiefern eine Harmonisierung der verwendeten Standards in Forschung und Versorgung zur Unterstützung übergreifender Anwendungsfälle der Datenübertragbarkeit möglich ist.

Die Trennung von durch Betroffene selbst eingegebenen bzw. direkt beobachtbaren Daten und davon abgeleiteten oder anderweitig durch die verantwortliche Einrichtung generierten Daten spielt allerdings bisher in der Kommunikation medizinischer Daten weder in Versorgung noch Forschung irgendeine Rolle. Entsprechend kann diese Unterscheidung auch nicht bei der Betrachtung möglicher relevanter Standards für die Datenübertragbarkeit herangezogen werden.

Üblicherweise wird in einem ersten Schritt zwischen Standardisierungen auf den Ebenen der Syntax und der Semantik unterschieden. Während syntaktische Konventionen festlegen, wie eine Kommunikationsnachricht oder ein Dokument strukturiert und aufgebaut ist, müssen die eigentlichen

Inhalte auf der semantischen Ebene einheitlich festgelegt werden. Nur wenn beide Ebenen ausreichend standardisiert sind, ist eine Interoperabilität zweier Systeme möglich (s. o.).

Als Beispiel für eine syntaktische Standardisierung der nachrichtenbasierten Kommunikation unterschiedlicher medizinischer Informationssysteme wird üblicherweise der sehr weit verbreitete Standard HL7 in Version 2.x genannt. Obwohl bereits seit Jahren mit der Version 3 eine wesentlich umfangreichere und aufwändiger strukturierte Standardisierungsgrundlage bereit steht, ist in der praktischen Anwendung als Kommunikationsformat unterschiedlicher Softwaresysteme die Version 2.x immer noch weit verbreitet. Derzeit steht allerdings mit dem neuen Ansatz der Fast Healthcare Interoperability Resources (FHIR) von HL7 ein Paradigmenwechsel bevor, da der neue Standard sowohl besser an aktuelle und webbasierte Entwicklungsparadigmen als auch an die Einbindung mobiler Endgeräte mit ihrem Anwendungsumfeld angepasst ist. Aber auch diese Nachrichtenformate stellen nicht nur den syntaktischen Rahmen einer Kommunikation dar sondern transportieren auch schon selbst semantische Inhalte. So sind neben Ausprägungskatalogen für einzelne Felder verschiedener Nachrichten auch die Nachrichtenformate selbst in Bezug auf ihre Zugehörigkeit zu bestimmten Ereignissen eindeutig festgelegt. Die Liste möglicher, nachrichtenauslösender Ereignisse (Events) ist somit auch ein standardisierter Merkmalskatalog, dessen semantische Festlegungen allerdings eher die Ebene organisatorischer Daten als jene der medizinischen Fallbeschreibung betreffen. So ist z. B. eindeutig festgelegt, wie sich die Nachricht einer Untersuchungsanforderung von einer Diagnosemitteilung oder der Bekanntgabe einer stationären Aufnahme eines Patienten unterscheidet.

Nun kann man zu Recht fragen, ob Standards für die Kommunikation einzelner Mitteilungen bzw. Nachrichten für die Umsetzung der Datenportabilität tatsächlich geeignet sind. Hier ist doch eher an die zusammengefasste Übermittlung aller in einem bestimmten Zeitraum angefallenen Daten gedacht, was bei nachrichtenbasierter Übermittlung im Regelfall zu einer Vielzahl von Übermittlungsvorgängen führen dürfte. Besser geeignet dürften hingegen dokumentenorientierte Formate sein, die in strukturierter Form eine Vielzahl von Informationen integriert darstellen und übermitteln können. Ein passender Kandidat hierfür stammt ebenfalls von HL7 und ist für klinische Dokumente wie z. B. Arztbriefe gedacht. Die Basis hierfür bildet die Clinical Document Architecture (CDA), ein XML-basierter Standard für die Strukturierung medizinischer Informationen, wobei unterschiedliche Level der Granularität möglich sind. Das interessante an diesem Ansatz ist, dass zusätzlich zur Abbildung der Detailinformationen im XML-Schema auch die Präsentation der Informationen für menschliche Nutzer über Stylesheets mit spezifizierbar ist. Gerade diese Eigenschaft könnte neben dem Recht auf Datenübertragbarkeit auch die Wahrnehmung der Informationsrechte der Betroffenen unterstützen. Zudem ist für den Standard CDA, insbesondere aufgrund eines schon seit längerem standardisierten Arztbriefs, eine gewisse Verbreitung und Unterstützung durch Softwarehersteller zu konstatieren.[11]

In der Welt der ambulanten Versorgung durch Arztpraxen und Medizinische Versorgungszentren (MVZ) herrschen seit vielen Jahren unverändert als universelle Austauschformate die xDT-Standards der KBV vor, die in einer zeilenorientierten Textdatei die einzelnen Feldinhalte der Praxisverwaltungssysteme bzw. Arztinformationssysteme unstrukturiert wiedergeben.

Im Umfeld der klinischen Forschung gibt es lediglich für den weitgehend standardisierten Bereich der klinischen Prüfungen nach Arzneimittel- oder Medizinproduktegesetz ein standardisiertes „Rahmen-„ oder „Trägerformat“, welches die strukturierte Speicherung und Übertragung aller Daten und

[11] http://hl7.de/themen/hl7-cda-clinical-document-architecture/

Metadaten einer Studie erlaubt. Das Operational Data Model (ODM) des internationalen Clinical Data Interchange Standards Consortium (CDISC) ist ebenfalls XML-basiert und wird bereits von einer Reihe von Softwaresystemen zum Datenmanagement in klinischen Studien unterstützt. Dass es darüber hinaus auch zumindest die Metadaten anderer Arten von Forschungsprojekten und auch aus der Versorgung weitgehend abbilden kann, zeigt das Portal der Medical Data Models der Universität Münster[12], welches aufbauend auf dem ODM-Format Dokumentationsformulare aus ganz unterschiedlichen Kontexten beschreibt und zudem den Export dieser Beschreibungen unterstützt.[13]

Wie aber können die eigentlichen medizinischen Inhalte im Rahmen solcher „Trägerformate" standardisiert übertragen werden? Diese Frage leitet von der Syntax der Datenübermittlung über zur Semantik der übertragenen Daten. Im Rahmen der Spezifikation eines Kerndatensatzes für die MI-Initiative des BMBF wurden für die einzelnen Module bereits erste Vorschläge zur Nutzung von Klassifikationen und Terminologien für die einzelnen Inhalte erarbeitet. Eine vollständige Widergabe der Überlegungen und Festlegungen zur ersten Version des Kerndatensatzes der MI-Initiative verbietet sich hier allerdings schon aus Platzgründen. Zudem sind nicht alle Module für den Anwendungsfall der Datenportabilität nach Art. 20 EU-DSGVO gleich interessant. Daher folgt hier nur eine Auswahl der wichtigsten Festlegungen und Überlegungen zu relevanten Standards zur Codierung ausgewählter medizinischer Sachverhalte.

Für die demographischen Basisdaten eines Patienten sowie die wichtigsten Falldaten samt Diagnosen und durchgeführten therapeutischen Prozeduren wird auf ein hoch standardisiertes tabellarisch strukturiertes Exportformat verwiesen. Diese Datensammlung muss in der vorgegebenen Form nach § 21 des Krankenhausentgeltgesetzes von allen Krankenhäusern zur Verfügung gestellt werden und ein standardisierter Export wird daher von allen Krankenhausinformationssystemen unterstützt. Die darin enthaltenen Diagnosen sind nach dem innerhalb Deutschlands vom DIMDI festgelegten und zur Verfügung gestellten Klassifikationsstandard ICD10 codiert. Für die Prozeduren wird der ebenfalls vom DIMDI bereitgestellte OPS-Katalog verwendet. Der breiten Verfügbarkeit und hohen Standardisierung dieser Informationen stehen allerdings noch inhaltliche Unzulänglichkeiten gegenüber, da z. B. einige zeitliche Charakteristika von Diagnosen nicht in der eigentlich gewünschten Genauigkeit abgebildet werden.

Für Laborbefunde gibt es mit den Logical Observations Identifiers Names and Codes (LOINC) ein etabliertes Kodiersystem des Regenstrief Institutes, welches lizenzkostenfrei samt Unterstützungstools angeboten wird. Die tatsächliche Verbreitung lässt allerdings immer noch sehr zu wünschen übrig, was mangels alternativen Systemen überrascht.[14] Dieses Beispiel macht leider deutlich, wie gering die Standardisierungsneigung ist, wenn kein gesetzlicher oder finanzieller Druck besteht. LOINC wird auch im Rahmen des Kerndatensatzes der MI-Initiative für Laboruntersuchungen empfohlen, in Verbindung mit dem Unified Code for Units of Measures (UCUM) für Maßeinheiten, einem ebenfalls vom Regenstrief Institute angebotenen und im medizinischen Umfeld alternativlosen System, wenn man Maßeinheiten verwechslungssicher und standardisiert abbilden möchte.

[12] www.medical-data-models.org

[13] Dugas, M., Neuhaus, P., Meidt, A., Doods, J., Storck, M., Bruland, P., Varghese, J., *Portal of medical data models: information infrastructure for medical research and healthcare.* Database, 2016. **2016**.

[14] Semler, S.C., Röhrig, R., *LOINC – Internationale Nomenklatur zur Kodierung von medizinischen Untersuchungen und Befunden*, in *Terminologien und Ordnungssysteme in der Medizin*, Hrsg.: O. Rienhoff and S.C. Semler. 2015, Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin. S. 97-134.

Schwieriger gestaltet sich die Repräsentation von Medikationsdaten. Für die Kodierung von Wirkstoffen kann die frei verfügbare Anatomisch-Therapeutisch-Chemische (ATC) Klassifikation der WHO genutzt werden, ergänzt um die Pharmazentralnummer (PZN) für konkrete Präparate. Einheiten können wiederum mit UCUM kodiert werden. Inwiefern hier perspektivisch auch das relativ neue System der Identification of Medicinal Products (IDMP) der ISO eingesetzt wird bzw. Verbreitung findet, bleibt abzuwarten.[15]

Im Umfeld der digitalen Bildgebung gibt es Beispiele heute schon gelebter Datenportabilität, die vermutlich viele Patienten schon erlebt haben. Nach dem Besuch einer radiologischen Praxis bekommt man die CD mit den Bildern gleich in die Hand gedrückt, während der eigentliche Befund per Fax an den Hausarzt geht, der einen zum Röntgen oder einer anderen Art der Bildgebung überwiesen hat. Dank des Standards Digital Imaging and Communications in Medicine (DICOM) sind die Bilddaten auf der CD samt der notwendigen Metadaten tatsächlich von fast allen Empfängern lesbar, auch wenn sie wohl in den meisten Arztpraxen lediglich angesehen und nicht systematisch in die elektronische Dokumentation übernommen werden. Im Regelfall findet sich auf der CD zudem ein frei verfügbarer DICOM-Viewer, mit dem sich auch der Patient selbst die Bilder ohne Einschränkungen anschauen kann. Allerdings muss darauf hingewiesen werden, dass DICOM zwar im radiologischen Umfeld weit verbreitet ist, es aber andere Bildgebungsdomänen wie Ultraschall oder die digitale Pathologie gibt, in denen die Standardisierung noch deutlich weniger weit entwickelt ist.

Für die semantisch standardisierte Darstellung von Daten aus klinischen Zulassungsstudien gibt es mit dem Study Data Tabulation Model (SDTM) zudem noch eine Formatvorgabe der CDISC-Organisation, die in enger Abstimmung mit der US-amerikanischen Zulassungsbehörde FDA entwickelt wurde. Wenn auch an vielen Stellen des Standards noch auf eine eigene Terminologie bzw. ein spezifisches kontrolliertes Vokabular verwiesen wird, ist doch für Laborwerte immerhin auch eine Kodierung mit Hilfe von LOINC möglich.

Nun wären noch viele andere Bereiche der medizinischen Diagnostik und Therapie zu nennen, in denen Daten anfallen können, die möglicherweise und in bestimmten Zusammenhängen auch für die Datenübertragung nach Art. 20 EU-DSGVO relevant werden könnten. Aber auch bis hierher lässt sich schon feststellen, dass zwar für viele Bereiche einigermaßen passende und verwendbare Standards existieren, dass aber diese ohne entsprechenden Druck finanzieller oder gesetzlicher Art kaum genutzt werden.[16]

3. Interoperabilität bei unterschiedlichen „gängigen“ Formaten

Eine Interoperabilität in dem oben genannten Sinne bei unterschiedlichen Formaten lässt sich nur erreichen, wenn diese sinnvoll ineinander übersetzt werden können. Hierzu müssen die beiden beteiligten Formate ausreichend detailliert beschrieben und dokumentiert sein und dies sowohl hinsichtlich Syntax als auch Semantik. Als Mindestfall ist von einer ausführlichen Beschreibung auf Papier auszugehen, so dass eine Übersetzung im Notfall „von Hand“ oder in individuell programmierter Art und Weise erfolgen kann. Ein modernerer Ansatz ist allerdings die Hinterlegung aller notwendigen Spezifika eines Datenformats bzw. zu einem Datensatz in Form selbst wiederum standardisierter und damit maschinenlesbarer Metadaten. Solche Metadatenbeschreibungen erlauben

[15] eine aktuelle Darstellung der verschiedenen Standards und damit verbundener Herausforderungen findet sich in Haas, C., *Herausforderungen an Interoperabilität im Arzneimittelbereich*, ebd. S. 135-148.

[16] Ein aktueller Überblick hierzu findet sich in Rienhoff, O., Semler, S.C., Hrsg. *Terminologien und Ordnungssysteme in der Medizin*. 2015, Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin.

dann im Idealfall eine automatische Übersetzung unterschiedlich standardisierter Datensätze ineinander. Ein moderner und internationaler Ansatz für die disziplinübergreifende Standardisierung solcher Metadaten ist der Standard ISO/IEC 11179.[17] Eine aktuelle Übersicht zur Verwendung von Metadaten findet sich ebenfalls im IT-Report der TMF.[18]

VI. Was ist bei der technischen Umsetzung zu berücksichtigen?

1. Allgemeine Rahmenbedingungen für die technische Umsetzung

Eine aktuelle Übersicht über die IT in der patientenorientierten Forschung zeigt eine starke Heterogenität der Softwarelandschaft, mit sehr unterschiedlicher Charakteristik der eingesetzten Systeme je nach Forschungsart und Forschungsbereich.[19] Während für die Erhebung und Verwaltung der Daten in klinischen Studien ein Markt für kommerzielle Softwaresysteme besteht, ist die Softwareunterstützung weniger standardisierter Forschungsprojekte wie etwa Register und Kohorten viel stärker projektgetrieben organisiert und von Eigen- oder Spezialentwicklungen geprägt. Letzteres kann als deutlich schlechtere Voraussetzung für die schnelle und breite Unterstützung der Datenportabilität angesehen werden.

Zu der aktuellen Situation der in den Krankenhäusern eingesetzten Krankenhausinformationssysteme findet sich ein grober Überblick samt weiterer Verweise ebenfalls in dem IT-Report der TMF.[20] Hier überwiegen aber sehr weitgehend Systeme kommerzieller Hersteller, so dass mit einer Unterstützung gesetzlich geforderter weiterer Funktionen grundsätzlich gerechnet werden kann, auch wenn die Finanzierung solcher Entwicklungen sicher im Einzelfall nicht immer ganz unstrittig zu lösen sein wird. Zudem ist festzustellen, dass in einem durchschnittlichen Klinikum schon eine große Zahl unterschiedlicher IT-Systeme für die Aufnahme, Produktion und Verwaltung von Daten zuständig ist, die ggf. im Sinne einer gesamtheitlichen Datenübertragung zusammenspielen müssten.

Eine besondere technische Herausforderung würde jedoch die Auftrennung von Daten nach solchen, die vom Patienten selbst bereitgestellt wurden bzw. direkt beobachtbar sind und anderen Daten darstellen (vergl. Kap. IV.2). Bisher spielt diese in Art. 20 Abs. 1 festgelegte Aufteilung von Daten in der Kommunikation medizinischer Sachverhalte weder in der Versorgung noch in der Forschung irgendeine Rolle, so dass diese Unterscheidung auch von keinem Kommunikationsformat unterstützt wird.

Eine weitere technische Herausforderung wäre dann zu bewältigen, wenn man auch Daten aus der medizinischen Bildgebung mit zu den Beobachtungsdaten zählt und diese somit auch vom Recht auf Datenübertragbarkeit umfasst wären. In diesem Falle wäre bei einer Reihe moderner Bildgebungsverfahren mit erheblichen Datenmengen zu rechnen, die kaum praktikabel per E-Mail an

---

[17] vergl. Ngouongo, S.M., Löbe, M., Stausberg, J., *The ISO/IEC 11179 norm for metadata registries: does it cover healthcare standards in empirical research?* J Biomed Inform, 2013. **46**(2): S. 318 - 327.

[18] siehe Price, N., Magis, A., Earls, J. et al., *A wellness study of 108 individuals using personal, dense, dynamic data clouds.* Nature Biotechnology, 2017.

[19] siehe Drepper, J., Semler, S.C., Hrsg. *IT-Infrastrukturen in der patientenorientierten Forschung. Aktueller Stand und Handlungsbedarf – 2015. Verfasst und vorgelegt vom IT-Reviewing-Board der TMF.* 2016, AKA, Berlin, http://www.tmf-ev.de/Produkte/ITReport.

[20] Drepper, J., Prokosch, H.U., Dugas, M., Semler, S.C., *Sekundärnutzung klinischer Daten*, in *IT-Infrastrukturen in der patientenorientierten Forschung ‚Aktueller Stand und Handlungsbedarf 2016*, Hrsg.: J. Drepper and S.C. Semler. 2016. S. 165-193.

Patienten verschickt oder von einer Webseite heruntergeladen werden könnten. Ähnliche Probleme wären zu erwarten, wenn auch die bei einer Sequenzierung des Genoms anfallenden Daten zu übertragen wären.

Eine nahezu ideale technische Basis für die Umsetzung der Anforderungen der Datenübertragbarkeit könnten elektronische Gesundheitsakten sein, die alle medizinischen Informationen der Betroffenen in strukturierter Form sammeln und vom Betroffenen hinsichtlich der Inhalte und Zugriffe gesteuert werden können. Der Gesetzgeber hat mit der Spezifikation der elektronischen Gesundheitskarte (eGK) in § 291a SGB V bereits einen gesetzlichen Rahmen hierfür – dort „elektronische Patientenakte" genannt – geschaffen, wenn die Verwaltung über die eGK geschieht. Bisher ist allerdings weitgehend unklar, wer auf Basis eines nachhaltigen Geschäftsmodells als dauerhafter Betreiber solcher Gesundheitsakten in Frage kommt und nach welchem Strukturierungsschema und auf Basis welcher Standards die Daten zwischen behandelnden Einrichtungen und solchen elektronischen Gesundheitsakten ausgetauscht werden können.[21] Immerhin machen sich aktuell mit der AOK und der Techniker Krankenkasse zwei große Krankenkassen auf den Weg, zusammen mit potenten Industriepartnern, solche Gesundheits- oder auch Patientenakten für ihre Versicherten aufzubauen.[22] Hier bleibt abzuwarten, ob solche Pilotprojekte auch als Chance zur Umsetzung der Datenübertragbarkeit gesehen werden und insbesondere, ob auch eine Datenübertragbarkeit zwischen den Patientenakten unterschiedlicher Anbieter realisiert wird.[23]

2. Berücksichtigung im Datenschutzmanagementsystem

Die Art. 29 Arbeitsgruppe der Datenschutzbeauftragten weist zu Recht darauf hin, dass bei einer Übertragung der personenbezogenen Daten ausreichende Sicherheitsmaßnahmen – wie etwa eine Ende-zu-Ende-Verschlüsselung der Daten nach dem Stand der Technik während des Transports – zu gewährleisten sind. Auch muss in jedem Fall eine sichere Identifikation und Authentifizierung des Betroffenen erreicht werden. Nicht zuletzt sollten die verantwortlichen Einrichtungen die Betroffenen auf die Risiken einer eigenen Speicherung der Daten in einer ggf. technisch unsicheren Umgebung hinweisen.[24]

Wenn man sich vergegenwärtigt, dass klinische und Forschungseinrichtungen in der Medizin besonders sensible Gesundheitsdaten verarbeiten, wird deutlich, dass diese Empfehlungen und Maßgaben der Art. 29. Arbeitsgruppe in diesem Umfeld sehr ernst genommen werden müssen. Insofern besteht hier eine besondere Herausforderung darin, sichere Kommunikationswege mit den Betroffenen zu finden, die typischerweise jedoch keinerlei Voraussetzungen hierfür mitbringen. Es ist

[21] einen aktuellen Überblick hierzu gibt Haas, P. *Elektronische Patientenakten. Einrichtungsübergreifende Elektronische Patientenakten als Basis für integrierte patientenzentrierte Behandlungsmanagement-Plattformen*. 2017. Bertelsmann Stiftung, https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/VV_eEPA_Expertise_final.pdf (Abruf: 2017-04-24).

[22] siehe http://aok-bv.de/presse/pressemitteilungen/2017/index_18768.html und http://e-health-com.de/details-news/techniker-holt-krankenhaeuser-an-bord/219ecc62a0c3e8e1022229088d697441/

[23] In § 291d SGB V sind Anforderungen an offene und standardisierte Schnittstellen der relevanten IT-Systeme normiert. Es ist aber offen, ob diese Regelungen tatsächlich Datenportabilität sicherstellen können.

[24] Artikel-29-WP *Guidelines on the right to data portability. Adopted on 13 December 2016. As last Revised and adopted on 5 April 2017*. 2017. Article 29 Data Protection Working Party, WP 242, rev.01, http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (Abruf: 2017-07-31).

eine seit langem beklagte Binsenweisheit, dass es zwar die technischen Voraussetzungen für eine sichere Kommunikation digitaler Inhalte gibt, diese aber so gut wie nicht angewendet werden. Der Bundestagsabgeordnete Thomas Jarzombek hat hierzu vor einigen Jahren schon festgestellt: „E-Mail-Verschlüsselung ist wie Teenagersex: Alle reden darüber und jeder denkt, der andere macht es. Doch tatsächlich machen es die Wenigsten, und bei denen läuft es auch noch schlecht." Als ein wichtiger Grund für diese Misere wird von Fachleuten die fehlende Nutzerfreundlichkeit entsprechender Software angegeben.[25] Vor diesem Hintergrund stellt die Anforderung zur Gewährung der Datenportabilität in Bezug auf sensible Gesundheitsdaten eine enorme Herausforderung für die mit klinischer Forschung befassten Einrichtungen dar. Eine naheliegende Lösung scheint der Aufbau eines sicheren Webportals zum verschlüsselten Download der Daten nach sicherer Authentifizierung zu sein. Allerdings sollten auch hier die technischen und organisatorischen Anforderungen nicht unterschätzt werden.

In der Forschung kommt als zusätzliche Herausforderung die typischerweise pseudonyme Speicherung und Verwaltung der Daten hinzu, die vor der Bereitstellung der Daten eine Depseudonymisierung erfordert, die entweder die mit der Pseudonymisierung beabsichtigte informationelle Gewaltenteilung durchbricht oder die Einbindung mehrerer Organisationseinheiten oder sogar Einrichtungen voraussetzt. Hintergrund dieser Problematik ist der Umstand, dass die Forscher selbst die Identität der Betroffenen im Regelfall für die Auswertung der Daten nicht benötigen und daher aus Datensparsamkeitsgründen auch nicht kennen sollten. Da aber beispielsweise für die Rekrutierung von Probanden für neue Studien oder für die Rückmeldung wichtiger Ergebnisse oder auch für die Zusammenführung nacheinander erhobener Daten der Zusammenhang der Daten zu der Person doch benötigt wird, muss eine andere Stelle als die Forschungsstelle selbst diesen Zusammenhang speichern und verwalten.[26] Die Anforderung der Aufhebung der Pseudonymisierung besteht allerdings für die allermeisten mit Forschung befassten Einrichtungen im Rahmen der Gewährung der Widerspruchs-, Korrektur- und Auskunftsrechte auch schon heute. Spannend wird hier aber, ob das Recht auf Datenportabilität zu einer Vermehrung der Anfragen und damit einem Anstieg der dadurch verursachten Aufwände führt.

VII. Welche Grenzen und Einschränkungen der Datenportabilität sind zu erwarten?

1. Datenverarbeitung im öffentlichen Interesse

In Artikel 20 Abs. 3 Satz 2 wird festgelegt, dass das Recht auf Datenübertragbarkeit nicht für eine Verarbeitung gilt, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Auch wenn man bei Datenverarbeitungen im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt zunächst an spezifisch gesetzlich geregelte Sachverhalte denkt, ist hier doch festzuhalten, dass das Recht auf Datenübertragbarkeit nach Abs. 1 sowieso nur für Fälle gilt, in denen eine Einwilligung der Betroffenen erfolgt ist oder ein entsprechender Vertrag geschlossen wurde.

[25] Schmeh, K., *Weg aus dem Elfenbeinturm. Warum Kryptografie in der Praxis oft versagt.* ix, 2016. **2016**(8): S. 54-59.

[26] Beispielhafte und von der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder empfohlene Pseudonymisierungsschemata für unterschiedliche Forschungsprojekte finden sich in Pommerening, K., Drepper, J., Helbing, K., Ganslandt, T., *Leitfaden zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF 2.0*. 2014, Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin.

Insofern stellt sich hier die Frage nach den vom Gesetzgeber mit diesen Einschränkungen adressierten Anwendungsfällen, also Verarbeitungen im öffentlichen Interesse auf der Basis einer Einwilligung der Betroffenen. Ob auch öffentlich geförderte Forschung mit dieser Ausnahme adressiert werden sollte, ist leider aktuell völlig unklar, so dass sich hier eine Rechtsunsicherheit konstatieren lässt, die noch der Klärung bedarf.

2. Abgrenzung faktischer Unmöglichkeit von ungerechtfertigter Behinderung

Zunächst ist zu fragen, was für Gründe für eine faktische Unmöglichkeit der Datenübertragbarkeit sprechen können. Hier können zunächst naheliegende technische Aspekte eine Rolle spielen, z. B. wenn die verwendete Software keine ausreichende Exportfunktion besitzt und aufgrund einer Spezialentwicklung keine neues Release mit erweiterter Funktion zu erwarten ist. Wie bereits weiter oben aufgezeigt, können solche Konstellationen durchaus in bestimmten Bereichen der medizinischen Forschung nicht ausgeschlossen werden. Häufiger – und sowohl im Bereich der medizinischen Forschung als auch der Versorgung – wird jedoch das Problem bestehen, dass die Exportfunktionen (und die Exportformate) keine Trennung zwischen von den Betroffenen selbst eingegebenen und anderen Daten unterstützen. Inwiefern eine solche Beschränkung als faktische Unmöglichkeit herangezogen werden kann, ist jedoch zum jetzigen Zeitpunkt nicht abschließend zu entscheiden. Eine wichtige Frage wird in diesem Zusammenhang sein, ob und ggf. mit welchem Aufwand eine Trennung der Daten nach einem Export vorgenommen werden kann. In Erwägungsgrund 68 der EU-DSGVO ist zudem festgehalten, dass das Recht auf Datenübertragbarkeit nicht zu der Pflicht für den Verantwortlichen führen sollte, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten.

Ganz anders ist die Frage nach den notwendigen Formaten und der geforderten Verbreitung dieser Formate gelagert. Wie ausführlich dargelegt, ist nicht davon auszugehen, dass kurzfristig breit unterstützte und tatsächlich Interoperabilität schaffende Formate und Standards zur Verfügung stehen werden. Ggf. wird hier zunächst mit einfachen Exportformaten (CSV) und einer entsprechenden, die Interpretation der Daten unterstützenden Dokumentation zu operieren sein, auch wenn dies für die verantwortlichen Stellen einerseits sehr aufwendig sein kann und andererseits damit die gewünschte Interoperabilität kaum erreicht werden wird.

3. Rechtsunsicherheiten in Bezug auf andere ggf. geltende Regelungen

§ 630g BGB normiert das Recht des Patienten, in seine Krankenakte Einsicht zu nehmen. Auch elektronische Abschriften sind vorgesehen. Allerdings steht dieses Recht unter der Einschränkung, dass „der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen“. Während letzteres auch eine Einschränkung im Sinne der Portabilität nach DSGVO darstellt, kennt die DSGVO nicht den Ablehnungsgrund der „erheblichen therapeutischen Gründe“. Hierbei dürfte es sich vor allem um Fälle handeln, in denen der Arzt der Auffassung ist, dass eine bestimmte Informationen für den Patienten erhebliche psychische Belastungen mit sich bringt, die angesichts seines Gesundheitszustandes nicht verantwortbar scheinen. Es ist allerdings fraglich, ob das Recht aus § 630g BGB hinsichtlich des relevanten Datenumfangs vollkommen deckungsgleich ist mit dem Recht auf Portabilität. Denn zur vollständigen Krankenakte dürften auch Diagnosen des Arztes sowie andere generierte Daten gehören, die nicht als vom Patienten zur Verfügung gestellt eingeordnet werden dürften. In diesem Bereich dürften wohl auch die größten Risiken im Sinne therapeutischer Gründe liegen, denn reine Rohdaten sagen Patienten in der Regel wenig. Die DSGVO sieht allerdings in Art. 23 für den nationalen Gesetzgeber die Möglichkeit vor, Einschränkungen auch für das Recht auf Datenportabilität zu definieren, die etwa nach Art. 23 Abs. 1 Satz 1 Buchstabe i) den Schutz der

betroffenen Person oder der Rechte und Freiheiten anderer Personen sicherstellen. Insofern können die in § 630g BGB normierten Einschränkungen der Einsichtnahme auch als mit der DSGVO konforme Einschränkung des Rechts auf Datenportabilität verstanden werden, wobei allerdings die DSGVO im Sinne der lex posterior entgegenstehendes Recht zunächst grundsätzlich beseitigt. Zudem ist wiederum fraglich, ob die Ausnahme auch dann gelten kann, wenn der Patient die direkte Übertragung an eine andere Stelle, also etwa an einen anderen Arzt, begehrt.

Hinzuweisen wäre noch auf die Regelung zur elektronischen Patientenakte nach § 291a SGB V, die in Abs. 8 selbst die einwilligungsbasierte Nutzung der Daten für Sekundärzwecke zu untersagen scheint. Ziel dieser Regelung ist es, dass Arbeitgeber oder Versicherungen oder andere nicht berechtigte Institutionen nicht Mittel an die Hand bekommen sollen, um qua ihrer Machtstellung den Arbeit- bzw. Versicherungsnehmer unter Druck setzen zu können, sensible Daten preiszugeben. Wie weiter oben schon dargestellt, bildet § 291a SGB V einen gesetzlichen Rahmen für umfangreiche Datensammlungen wie z. B. elektronische Patientenakten, die über die eGK verwaltet werden, ohne dass es aber hierzu auch schon Umsetzungen gäbe. Insofern ist die Frage eines möglichen Widerspruchs heute noch ohne praktische Relevanz. Der deutsche Gesetzgeber sollte aber prüfen, ob er hier im Sinne einer weitergehenden Rechtsklarheit zur und Unterstützung der Datenportabilität eine Anpassung des gesetzlichen Rahmens vornehmen kann. Dies wäre letztlich auch im Sinne der Forschung, die dann auf Basis einer Einwilligung rechtssicher auf diese ggf. sehr wertvollen Daten zugreifen könnte.[27]

VIII. Fazit und Ausblick

Derzeit lassen sich die Aufwände für die Umsetzung des Anspruchs auf Datenübertragung gemäß Artikel 20 EU-DSGVO kaum abschätzen. Es finden sich aber viele Indizien dafür, dass man diese Aufwände nicht zu gering schätzen sollte, insbesondere dann, wenn die Datenübertragung im Sinne der Betroffenen sein und tatsächlich Mehrwert für diese generieren soll. Im positiven Sinne kann diese Regelung auch ein weiterer Anstoß zur Entwicklung und Nutzung übergreifender Standards und Terminologien sein, die die Interoperabilität und Nachnutzung von Daten stärkt.

Allerdings ist auch festzustellen, dass es unabhängig von dieser gesetzlichen Regelung bereits eine Reihe von Initiativen und Projekten gibt, die ebenfalls eine Stärkung der Datenautonomie der Betroffenen und in diesem Sinne ein Patient Empowerment anstreben und dabei sogar über den Rahmen der Datenportabilität hinausgehen. Insbesondere die im Rahmen der Datenportabilität vorgesehene Trennung von Daten, die der Betroffene selbst bereitgestellt hat samt ggf. reinen Beobachtungsdaten und solchen Daten, die die verantwortliche Stelle erst durch weitere Verarbeitung geschaffen hat, findet derzeit in der Kommunikation medizinischer Daten und damit verbundenen Anwendungsfällen keine Entsprechung. Die Unterstützung sinnvoller Anwendungsfälle und eine Stärkung der Patientenautonomie ist alleine auf dieser Basis nicht zu erreichen. Es wird den Patienten in den allermeisten Fällen wenig helfen, reine Beobachtungsdaten zu erhalten, aber nicht die daraus resultierende Diagnose.

Insofern wäre es auch problematisch, wenn die Regelungen zur Datenportabilität die Entwicklung von Standards und Formaten anstoßen sollten, die diese im Bereich der medizinischen Forschung und Versorgung nicht hilfreiche Trennung nachvollziehen. Letztlich zeigt sich in dieser hier vorgesehenen Trennung nach selbst bereitgestellten und anderen Daten, dass die Regeln zur Datenportabilität mit

[27] Ein ausführliches Gutachten samt konkretem Änderungsvorschlag zu § 291a SGB V findet sich in Schneider, U.K., *Sekundärnutzung klinischer Daten - Rechtliche Rahmenbedingungen*. 2015 ebd.

Blick auf bestimmte Anwendungsfälle und Anbieter wie z. B. soziale Netzwerke aufgestellt wurden, aber jetzt in undifferenzierter Art und Weise auch ganz andere Anwendungsfelder und Anbieter treffen, auf die sie jedoch nicht in gleicher Weise passen.

Insofern bleibt zu hoffen, dass viele der hier aufgeführten offenen Fragen im Sinne der Betroffenen und der für die Verbesserung der gesundheitlichen Versorgung der Betroffenen notwendigen Forschung beantwortet werden können. Es besteht allerdings im Zusammenhang mit den hier analysierten Regelungen zum Recht auf Datenübertragbarkeit die Sorge, dass knappe Ressourcen eher in die Umsetzung spezifischer gesetzlicher Erfordernisse als in die Realisierung eines echten Mehrwerts für die Betroffenen im Anwendungsfeld der medizinischen Forschung und Versorgung investiert werden könnten.

IX. Abkürzungsverzeichnis

AOK	Allgemeine Ortskrankenkasse (www.aok.de)
ATC	Anatomisch-Therapeutisch-Chemische Klassifikation: Klassifikation von Arzneimittelwirkstoffen entsprechend dem Organ oder Organsystem, auf das sie einwirken, und nach ihren chemischen, pharmakologischen und therapeutischen Eigenschaften
BDT	Behandlungsdatenträger, Standard der KBV für den Datenaustausch zwischen Praxis-Softwaresystemen für Befund- und Verlaufsdaten
BGB	Bürgerliches Gesetzbuch
BMBF	Bundesministerium für Bildung und Forschung (www.bmbf.de)
CD	Compact Disc
CDA	Clinical Document Architecture, HL7-Standard für den Austausch klinischer Dokumente
CDISC	Clinical Data Interchange Standards Consortium (www.cdisc.org)
CSV	Comma separated Values
DICOM	Digital Imaging and Communications in Medicine (http://medical.nema.org)
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information (www.dimdi.de)
DSGVO	siehe EU-DSGVO
EG	Europäische Gemeinschaft
eGK	elektronische Gesundheitskarte
EPA	Elektronische Patientenakte
EU-DSGVO	Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (Verordnung 2016/679)
FDA	US Food and Drug Administration (www.fda.gov)
FHIR	Fast Healthcare Interoperability Resources; HL7-Standard (http://hl7.org/fhir)
GDT	Gerätedatenträger, Standard der KBV für den Datenaustausch zwischen Geräten und Praxis-Softwaresystemen für Gerätedaten
HL7	Health Level Seven; Internationale SDO für den Bereich der Interoperabilität von IT-Systemen im Gesundheitswesen (www.hl7.org)
ICD-10	International Statistical Classification of Diseases and Related Health Problems, 10. Revision

ICH	International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (www.ich.org)
IDMP	Identification of Medicinal Products; Gruppe von ISO-Standards zur Beschreibung von Arzneimitteln, Darreichungsformen, Maßeinheiten, Produktnamen und Substanzen
IEC	International Electrotechnical Commission (www.iec.ch)
ISO	International Organization for Standardization (www.iso.org)
KBV	Kassenärztliche Bundesvereinigung (www.kbv.de)
LDT	Labordatenträger, Standard der KBV für den Datenaustausch zwischen Labor- und Praxis-Softwaresystemen für Labordaten
LOINC	Logical Observation Identifiers Names and Codes (www.loinc.org)
MedR	Medizinrecht
MI	Medizininformatik
MI-Initiative	Medizininformatik-Initiative des BMBF (www.medizininformatik-initiative.de)
MVZ	Medizinisches Versorgungszentrum
ODM	Operational Data Model (CDISC-Standard)
OPS	Operationen- und Prozedurenschlüssel; vom DIMDI herausgegebener Katalog zur Verschlüsselung medizinischer Prozeduren im Krankenhaus und ambulanter Operationen
PRO	Patient Reported Outcome
PZN	Pharmazentralnummer
SDO	Standards Development Organization
SDTM	Study Data Tabulation Model (CDISC-Standard)
SGB	Sozialgesetzbuch
TMF	TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (www.tmf-ev.de)
UCUM	Unified Code for Units of Measure (http://unitsofmeasure.org)
WHO	World Health Organization (www.who.org)
WP	Working Party der Europäischen Arbeitsgruppe zum Datenschutz gemäß Artikel 29 der Richtlinie 95/46/EG
xDT	Oberbegriff für die Datenträger-Standards der KBV, z. B. BDT, LDT und GDT
XML	extensible Markup Language

The Importance of Data Portability and Interoperability in the Social Web

Sebastian Göndör, TU Berlin, Service-centric Networking

Since the dawn of the Social Web in the late 1990's, Online Social Network (OSN) services have conquered more and more aspects of our daily digital lives. The original use case of OSN services, being to model connections to friends and acquaintances, was augmented and extended to offer more and more rich experiences to the users of OSN services. Nowadays, organizing events and inviting guests, representing companies and brands including handling customer feedback, expressing opinions, text and voice-based communication, as well as reading the news have moved to OSN services [1]. Unknowingly, by specifying who their friends and acquaintances are and generating content in their social profiles, users of OSN services have been creating a global network of social connections - a *"global mapping of everybody and how they are related"* referred to as *the Social Graph* [2]. Such a dataset, telling the story of how a significant portion of the world's population is connected including information about personal preferences, habits, or connections, obviously attracts the interest of not only marketers, employers, credit rating agencies, insuring agencies, the police, and intelligence agencies, but also of spammers, phishers, and other criminals [3]. Using intelligent algorithms, the information comprised in the social graph can be made visible by creating highly detailed user profiles for everyone who left their traces in it. With Facebook's extraordinarily powerful position in the OSN market came doubts and concerns regarding to data privacy and protection. People started to feel apprehensive about the fact that one or few companies had access to all their social profile data while claiming full ownership of all content at the same time. The fact that these companies use the - partly very personal - information for targeted advertisements led to Facebook, as well as other OSN service providers, being perceived as an all seeing, all knowing *Big Brother*.

But we already had become too dependent on the social web to simply walk away. We put all our data, our friends and connections, and our memories on the social web, where it remains tightly locked up in the various services we signed up with. With the dependence on OSN services came the problem of being bound to the service one signed up with in the first place, as services did not support interoperability between each other. Existing network effects were cleverly exploited by the platforms, as the more users use the same service, the more value a membership for any user has [4]. Much too late, users realized they were locked into walled gardens, where all their created content legally belonged to the OSN platform operator and connectivity to other OSN services was mostly inhibited. We voluntarily created and continuously fed an all-seeing, all-knowing leviathan, controlled by large corporations that use their power to sell us out.

The Social Web Today is a Landscape of Isolated Islands

Most of today's major OSN platforms are implemented in a closed, proprietary fashion. Even though access to the services' functionality is being made available via proprietary interfaces, today's OSN services keep their users from seamlessly connecting to users of other services to create well-calculated *lock-in effects*. This hinders users from being able to freely communicate with OSN services run by a competitor while at the same time the individual cost of migrating to a competitor's service is intentionally kept high. This creates a positive feedback loop for users signing up with large OSN services, as the more users a certain OSN platform is able to attract, the more likely it is for any user to find a specific friend's user profile on this platform. This *network effect* keeps users from using other OSN services, leading to the current situation of isolated islands of OSN services, in which users are locked into walled gardens - proprietary platforms in which the provider has full control over applications, content, and communication, effectively binding

their users to the platform. Analysis showed that OSN services don't experience the benefits of a so-called *first-to-market effect* after being launched, as network effects in OSN services are weak in early stages due to the low number of users [4]. Anyhow, after a critical mass of users is reached a giant cluster forms in the social graph, causing implicit network effects to take effect that cause the service to become *self sustainable*, meaning that it attracts more users because of it's sheer mass. These effects are able to drive smaller services out of the market, as most users will choose to sign up with the dominating service, leaving no room for a second place on the OSN market [5]. The simple explanation for this effect is that for a potential new user of OSN services, it is more reasonable to register with an OSN platform most of his friends are already using instead of signing up with a different service, even though it might be better suited for this user's demands or expectations. As OSN services do not allow seamless communication between different OSN platforms, choosing a platform not used by the majority of OSN users will essentially cut one off from communication with most other OSN users.

The term *lock-in effect* originally stems from the field of economics where *vendor lock-ins* inhibit customers to use a competitor's product, and make switching to a competitor's product unreasonably expensive [6]. Applied to OSN services, lock-in effects describe a technological barrier disallowing interoperability and data portability, causing that abandoning an OSN platform for a another one results in losing one's social profile along with all content and connections to other individuals. Naturally, the more content and information one created by using the service and the more friends are using the same OSN service, the stronger the OSN lock-in effect gets. This way, users and their data are bound to the OSN service operator, unable to move away or freely communicate with outside services.

As network effects cause the global user-base to converge in few OSN platforms on a global scale, sensible and personal data of billions of users is stored and managed by only a small number of companies [7]. This practice resulted in an ever ongoing conflict of interests, as OSN providers often automatically claim ownership of the managed data, including personal information, pictures, and text messages, which is then used for targeted advertisement and data analysis [8][9]. Facebook, for example, states in their terms and conditions that they claim *"non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content"* that is posted on the platform, and further sharing information about their users with vendors, service providers, and other partners. Naturally, the implications of this concerns users as control over one's data privacy is essentially lost [2].

As of 2016, data portability has been regulated in the General Data Protection Regulation (GDPR) by the European Union (EU) [10]. The regulation addresses a mandatory ability to export personal information *"in a structured, commonly used, machine-readable, and interoperable format"*, including the ability to transmit the exported information to other services. With the intention to further strengthen the control over one's data, the regulation is enforceable as of May 2018, yet lacks a technical implementation of how data should be exported, described, or re-imported.

To alleviate the current situation of one OSN platform dominating the entire OSN market, proposals have been made to mandate regulatory action based on European competition laws where two aspects should be addressed in specific, being data portability and interoperability. According to Graef [11], data portability in the domain of OSN services would be a user's ability to automatically move their social profile data including photos, posts, and friend lists to a competitor's service, where *"technical standards have to be developed to ensure that data portability can be effectively implemented"* so that it is made *"possible for data extracted from one social network to be seamlessly inserted into another [OSN service]"*. Yet Graef argues further that implementation of interoperability between different OSN services is additionally required, as it would give users the ability to *"connect and interact with each other irrespective of their social network provider"*, thus being even more powerful than data portability alone. Implementing such a form of OSN network interoperability would be *"a way to redress network effects and increase competition in the [OSN] market [reducing] switching costs and the degree of user lock-in [as] the number of people that*

a user can reach is not limited anymore to the number of users on the social network that the user decided to join". While this would affect the business models of OSN services, it would encourage new services to enter the market and therefore lead to more and healthy competition and consumer choice. Ultimately, this hence would result in a better protection of the rights and interests of users of OSN services [11].

Towards a Truly Open and Heterogeneous Online Social Network Federation

The intention of data portability in the GDPR is to allow individual users to not only be able to know and monitor what data is stored related to them, but also to keep using data they created or submitted to a service after they started to use a competitor's service. Examples for such scenarios could be a cloud storage service, a web-based photo album, or an OSN service, where a user extracts his user profile including all included information and transfers it to another service where it is automatically imported in order to allow the user to seamlessly continue using the user profile and enclosed data.

As of today, several large service providers already implemented a takeout feature that allows users to download an archive of all their personal information. For example, Facebook and Google allow users to request an archive of their personal data from the service that contains all personal data of oneself that is stored and managed by the services. When requested, the data can be downloaded as a compressed archive that contains the requested personal data. While most data is stored in open data formats such as comma separated value (csv) lists, JSON objects, or HTML pages, their semantics are mostly not included, hindering services from seamlessly importing the data to another service. This effectively renders data portability useless for migration of user accounts, as even though one can access and download his or her user profile and data, one is still locked in with the old service as he cannot directly use the data in another service.

Especially for OSN services accumulating vast amounts of information about their customers, giving users the possibility to not only extract their personal data, but also import all data into another OSN service would enable migration of user accounts between competing OSN services. For this, not only common and standardized interfaces for export and import of user account information and data would be required, but also a set of common data formats and standards that could be used to transfer and parse the information of an exported dataset. After all, the service a user profile is being migrated to needs to be able to read and understand the information enclosed in the data.

Furthermore, users and data objects in web services are usually identified by a unique identifier that uniquely identifies and locates the user or data object in the service's domain. A user in the OSN Facebook is for example uniquely identified by the link `https://www.facebook.com/zuck`, a photograph by `https://www.facebook.com/photo.php?fbid=10101026493146301`, where all links contain the service's domain name, `facebook.com`. Due to the nature of OSN services, these identifiers are implicitly used by other users to link to each other's profiles and data. After migrating a user profile to a new service, these identifiers will inevitably break, as the enclosed domain name would still point to the old, now invalid location of the data [12]. Hence, a holistic way to migrate user profiles and data in web services not only requires a set of standard protocols and data formats, but also a solution to deal with links and identifiers that are bound to a specific service domain.

The right to migrate OSN user profiles and the technology to support it bears the potential to free users from the walled gardens their digital lives are currently being held captive in. Still, without an automated way to import extracted user profiles in other services, users would be still confined in the OSN platform their user profile is managed by. Hence in addition to data portability mechanisms, open protocols that facilitate seamless interoperability between different OSN services are required, allowing a user on Facebook to invite guests from Google+ to a hosted event, while discussing topics with users of VKontakte and RenRen [13]. Interoperability, once implemented on a broad scale, would give users the ability to connect and

interact with each other irrespective of their social network provider [11]. Borders between different OSN platforms would become transparent to users, rendering it irrelevant at which OSN service someone signed up with. The social web would be free again, as every user would be able to decide to whom to entrust his or her personal data. In consequence, the strong network effects that nowadays draw users towards the market leaders' OSN platforms and effectively binds them there would be eradicated, giving rise to new ways of competition in the OSN service market. OSN providers would once more need to compete directly with each other in order not only to attract, but also to keep users on their platform as a dissatisfied user would be able to simply move on to another, more suitable solution offered by a competitor. Small OSN services could again begin to compete with large players in the OSN market, a situation that is considered to foster innovation and diversity. New services would be encouraged to enter the market, leading to more and healthy competition and consumer choice, paving the way towards a landscape of OSN services with better protection of the rights and interests of users of OSN services [11]. Ultimately, the social web as we know it today would be freed from its borders and restrictions, as users would be given the means to take back control over their data in an open and heterogeneous federation of OSN services.

[1] S. Greenwood, A. Perrin, and M. Duggan. *Social Media Update 2016*. Tech. rep. http://www.pewinternet.org/2016/11/11/social-media-update-2016/ Accessed on 30.5.2017. PEW Research Center, 2016.

[2] B. Fitzpatrick and D. Recordon. *Thoughts on the Social Graph*. http://bradfitz.com/social-graph-problem/ Accessed: 15.5.2017. 2007.

[3] J. Bonneau, J. Anderson, R. Anderson, and F. Stajano. "Eight Friends are Enough: Social Graph Approximation via Public Listings". In: *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*. ACM. 2009, pp. 13–18.

[4] J. C. Westland. "Critical Mass and Willingness to Pay for Social Networks". In: *Electronic Commerce Research and Applications* 9.1 (2010), pp. 6–19.

[5] M. Seemann. *Dezentrale Social Networks - Warum sie scheitern und es gehen könnte*. http://14.re-publica.de/session/dezentrale-social-networks-warum-sie-scheitern-und-es-gehen-koennte Accessed: 14.5.2017. re:publica 14, 2014.

[6] M. L. Katz and C. Shapiro. "Network Externalities, Competition, and Compatibility". In: *The American economic review* 75.3 (1985), pp. 424–440.

[7] S. Gilbertson. *Slap in the Facebook: It's time for social networks to open up*. https://www.wired.com/2007/08/open-social-net/ Accessed: 21.5.2017. 2007.

[8] O. Malik. *Is Facebook Beacon a Privacy Nightmare?* Tech. rep. https://gigaom.com/2007/11/06/facebook-beacon-privacy-issues/. Accessed: 6.6.2017. 2007.

[9] C. Yeung, I. Liccardi, K. Lu, O. Seneviratne, and T. Berners-Lee. "Decentralization: The Future of Online Social Networking". In: *W3C Workshop on the Future of Social Networking Position Papers*. Vol. 2. 2009.

[10] European Parliament. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Accessed: 16.9.2017. 2016.

[11] I. Graef. "Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union". In: *Telecommunications Policy* 39.6 (2015), pp. 502–514.

[12] S. Göndör, F. Beierle, S. Sharhan, and A. Küpper. “Distributed and Domain-Independent Identity Management for User Profiles in the SONIC Online Social Network Federation”. In: *International Conference on Computational Social Networks*. Springer. 2016, pp. 226–238.

[13] S. Göndör, F. Beierle, S. Sharhan, H. Hebbo, E. Küçükbayraktar, and A. Küpper. “SONIC: Bridging the Gap between Different Online Social Network Platforms”. In: *Social Computing and Networking (SocialCom), 2015 IEEE 8th International Conference on*. IEEE. 2015.

The Right to data portability between legal possibilities and technical boundaries

Armin Gerl, Dirk Pohl*

Keywords: Privacy, Data Portability, Portability Format, Ontology-Matching, Data- and Information Law

I. Introduction

The General Data Protection Regulation is designed to be 'technology-neutral'. This concept was intended to allow for a high degree of flexibility in order to address the so-called 'law lag' problem[1]: The Law is often unable to keep up with the rapid technological change. In fact, many social media services started offering (albeit limited[2]) data portability interfaces as early as 2008[3], when the discussion about a new Data Protection Right within the European Union was still at its' infancy.

However, wide and flexible provisions like Art. 20 GDPR introducing the Right to Data Portability may on the other hand create a high degree of legal ambiguity.

Without further guidelines, this may well be a risk for a useful practical implementation and the Right to Data Portability might fail to achieve the ambitious and manifold aims of granting benefits to the 'Data Subject' (Art. 4 No. 1 GDPR) by allowing a free choice of services due to convenient and easy moving of data[4], as well as enabling him or her to be in control of their information ('informational self-determination'[5]) and to boost consumer protection[6] while also creating advantages for the (especially non-market dominant) Controller[7] (Art. 4 No. 7 GDPR) and increasing economic interests to support the portability of user data.

---

*_Armin Gerl_ is Research Assistant and Ph.D. student at the Dept. of Distributed and Multimedia Information Systems and at the Dept. of Civil Law, German and European Legal History, University of Passau; _Dirk Pohl_ is Research Assistant and Ph.D. student at the Dept. of Public Law, Information- and Media Law, University of Passau.

[1]For a detailed account on the problem see Stephan Hobe, "Technological Development as a Challenge for the Development of Air and Space Law", in *A New International Legal Order*, ed. Chia-Jui Cheng (Leiden: Brill, 2016), 295 ff.

[2]*Inge Graef*, *"Mandating portability and interoperability in online social networks"*, Telecommunications Policy 39 (2015): 506.

[3]See Bill Greenwood, *"My Space, Facebook, Google integrate data portability"*, Information Today 6 (2008): 27; a comprehensive account of the origins of the right to data portability can be found in *Barbara* Van der Auwermeulen, *"How to attribute the right to data portability in Europe: A comparative analysis of legislation"*, Computer Law & Security Review 33 (2017): 58 f.

[4]Peter Swire/Yianni Lagos, *„Why the right to data portability likely reduces consumer wellfare"*, Maryland Law Review 335 (2013): 344 f.

[5]See Stefan Weiss, *"Privacy threat model for data portability in social network applications"*, International Journal of Information Management 29 (2009): 249; Eva Fialová, "*data portability and informational self-determination",* Masaryk Journal of Law and Technology 8:1(2014): 46; European Commission Staff Working Paper, SEC(2012) 72 final (2012): 43.

[6]Barbara Van der Auwermeulen, *"How to attribute the right to data portability in Europe: A comparative analysis of legislation"*, Computer Law & Security Review 33 (2017): 59.

[7]Barbara Van der Auwermeulen, *"How to attribute the right to data portability in Europe: A comparative analysis of legislation",* Computer Law & Security Review 33 (2017): 60.

Furthermore, as long as a Controller is not able to foresee his legal responsibilities under Art. 20 GDPR with a reasonable certainty, it seems doubtful whether the administrative fees for infringements as contained in Art. 83(5) lit b) GDPR ('up to 20.000.000 € or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher') can be enforced.[8]

This article shall first describe the current legal claims to data portability as laid down in Art. 20 GDPR, as well as the legal limitations (II.1). Then scenarios to enable data portability from a technical perspective are developed in accordance with the legal requirements (II.2). The requirements for a portability format are then to be assessed in detail from a technical as well as legal perspective (III.), followed by an assessment of the specific requirements of the Negotiation Process, when data are being transferred from one Controller to another (IV.). Subsequently some additional requirements not directly related to data portability itself, but nevertheless important during a data transfer, shall be discussed (V.). The possible effects of the Right to Data Portability as one of the few true innovations within the GDPR[9] are then to be critically evaluated (VI.).

II. Data Portability Scenarios

Prior to a detailed assessment of the possibilities and problems regarding data portability, the two scenarios as stipulated by Art. 20(1) GDPR and Art. 20(2) GDPR are to be described and critically discussed (II.1). Subsequently, technical scenarios are to be developed in accordance (II.2).

1. Legal claims

Art 20 GDPR grants two different Rights to Data Portability to the Data Subject. The right contained in Art. 20(1) GDPR shall be referred to as a 'Right to obtain a copy of the data', while Art. 20(2) contains a different and distinguishable 'Right to data transfer'.[10]

The basic conditions for the exercise of both rights are identical. As does the GDPR, the Right to Data Portability only applies to 'personal data' as defined in Art. 4 No. 1 GDPR, and specifically those processed by automated means (see Art. 2(1) GDPR). More restrictively it only applies to those data provided by the Data Subject to the Controller. Additionally, only such data are to be included that were processed based on the consent of the Data Subject or where the basis for processing has been a contract (Art. 6(1) lit. b GDPR).

A substantial limitation is placed on both claims within the Right to Data Portability by Art. 20(4) GDPR. The exercise of the right to data portability may not adversely affect the rights and freedoms of others. The complex problems that may arise from this provision can-

[8]See Dirk Pohl, *„Durchsetzungsdefizite der DSGVO? Der schmale Grat zwischen Flexibilität und Unbestimmtheit",* PinG 3 (2017): 85.

[9]See amongst others Tim Jülicher/ Charlotte Röttgen/Max v. Schönfeld, *„Das Recht auf Datenübertragbarkeit"*, ZD 8 (2016): 358.

[10]Terminology found in Eva Fialová*, "data portability and informational self-determination",* Masaryk Journal of Law and Technology 8:1 (2014): 45.

not be discussed here. Especially in a social media context this could lead to great amounts of data being excluded from the Right to Data Portability.

1.1. Right to obtain a copy of the data

Undoubtedly Art. 20(1) GDPR establishes a right of the Data Subject to receive his data from the Controller. On its own and strictly speaking this cannot be considered a true Right to Data Portability. It bears more similarities to the Right to Access as granted by Art. 15 GDPR. The Data Subject merely receives a copy of certain data (see in detail III.2) from one Controller and is then required to negotiate the import of this data with the target Controller by him or herself. (see II.2.1).

1.2. Right to data transfer

True portability of data is only granted under Art. 20(2) GDPR. The Data Subject can demand that data are being transferred from one Controller directly to another. The Data Subject itself only initiates the transfer, but is otherwise not involved. However, this right is considerably limited by the fact that there is no corresponding obligation of the target Controller to receive such transfer of data by another controller (II.1.2.1) and further by the limitation to cases, where such transfer is 'technically feasible'.

1.2.1.No obligation to import data

On a literal interpretation Art. 20(2) GDPR does not seem to place any obligation on the target Controller to provide any feasible measure of acceptance for such data that have been transferred. The target Controller is not even mentioned. The requirement to allow a transfer 'without hindrance' within Art. 20(1) GDPR is only aimed at the first Controller as well.
While the spirit and purpose (French *raison d'être)* of this provision may point into a different direction in order to guarantee its' effectiveness, Recital 68 to the GDPR clarifies the intentions of the legislator. It states that the Right to Data Portability shall not create any obligation for a Controller to adopt or maintain compatible processing systems.

1.2.2.Is a legal claim to importation of data desirable?

At first sight the missing obligation for the target Controller to import the data seems to be an odd outcome. It warrants a discussion of the necessity to introduce such obligation in future legislation.
A starting point for the debate may be the two (often competing) goals of the GDPR as stipulated in Art. 16(2) TFEU. It mandates the European Union to lay down rules relating to the protection of personal data, as well as rules relating to the free movement of personal data. The GDPR has to strike a balance between these goals.
Considering the perspective of the Data Subject, it seems reasonable to state that a broader right to Data Portability generally strengthens his or her position. As postulated by Recital 68 to the GDPR, it allows the Data Subject to 'further strengthen the control over his or her data'.
Contrary to many other discussions regarding the GDPR, the second aim of promoting the free movement of data does not seem to warrant another outcome. A broad and robust right

to Data Portability may also increase the free movement of personal data. With both aims of the GDPR seem pointing in another direction, the assertion of a very limited right to Data Portability is even more surprising.

However, even though the Right to Data Portability was included in the GDPR and thus formally is part of the data protection laws of the Union, the legal nature of the right is broader than its' formal localisation may suggest. Art. 20 GDPR may well be – and often is – seen as an element of competition law within the GDPR. So from a systematic point of view, the 'data protection perspective' must not be the sole basis of interpretation.

An obligation to accept data transferred by another controller in any format that fulfils the general criteria of Art. 20 GDPR (see III.1) may be beneficial for the data subjects' informational self-determination and the free movement of data, but can cause several problems within the market.[11] It has to be taken into account that Art. 20 GDPR applies to 'a garage start-up software company just as it does to a monopolist'.[12] On the one hand, a Right to Data Portability can strengthen the position of small companies, since it enables them to share in the large volumes of data gathered by the well-established companies in the market and thereby avoid market entrance barriers.[13] On the other hand, especially the business model of smaller companies or start-up companies may be endangered if the Right to Data Protection were to be understood as establishing an obligation to import formats from another controller. They would be forced to provide feasible means of acceptance for the potentially very different but common formats of their larger competitors.

Once the market effects are taken into account, it seems arguable that Art. 20 GDPR strikes a reasonable balance between the various interests. Thus, an obligation for the target Controller to import the data does not seem desirable. However, it must be noted that such a careful approach also minimises the regulatory effects of the Right to Data Portability.

The effective implementation of the right could be improved by legal regulations for accompanying measures (see also V.). Instead of requiring the import itself, it seems more reasonable to require Controllers to publish information about formats they are willing to accept for import, so a competitor – if willing – may transfer the data in a suitable format causing no additional efforts for the target Controller.[14]

---

[11] For an analysis see Barbara Engels, *"Data portability among online platforms"*, Internet Policy Review 5:2 (2016): 13.

[12] Barbara Engels, *"Data portability among online platforms"*, Internet Policy Review 5:2 (2016): 4; Peter Swire/Yianni Lagos, *„Why the right to data portability likely reduces consumer wellfare"*, Maryland Law Review 335 (2013): 339.

[13] Barbara Van der Auwermeulen, *"How to attribute the right to data portability in Europe: A comparative analysis of legislation"*, Computer Law & Security Review 33 (2017): 57; Lucio Scudiero, *"Bringing Your Data Everywhere: A Legal Reading Of The Right To Data Portability"*, EDPL 1 (2017): 119.

[14] For extensive description of other methods to ensure interoperability see Sih Yuliana Wahyuningtyas, *"Interoperability for data portability between social networking sites (SNS)"*, Queen Mary Journal of Intellectual Property 5:1 (2015): 46 ff.

1.2.3.Transfer must be technically feasible

The Controllers is required to transfer data to another Controller under Art. 20(2) GDPR as far as such transfer is 'technically feasible'. While this is said to be a limitation to the Right to Data Portability in a legal sense, the effect of this 'limitation' has to be assed from the view of the (possibly wide) technical possibilities. It seems unlikely that the transfer itself as required by Art. 20(2) GDPR causes any significant problems. However, in cases of obvious incompatibility between formats it may be possible for a Controller to invoke this exception instead initiating a transfer with no chance for an effective outcome.
In any case the Data Subject may still receive a copy of the data as described in Art. 20(1) GDPR.

2. Technical Scenarios

In general the legal requirements as described above allow for the interpretation of two technical scenarios.
On the one hand it is stated that a Data Subject has the right to receive its personal data from a Controller and may transfer this personal data to a target Controller thereafter (Art. 20(1) GDPR, see II.1.1). We denote this scenario as Data Subject Negotiation.
On the other hand it is stated that the Data Subject has the right to enforce a transfer between Controllers as far as this is technically feasible (Art. 20(2) GDPR, see II.1.2). We denote this scenario as Controller Negotiation.
Both the Data Subject Negotiation and Controller Negotiation will be described and discussed in the following.

2.1. Data Subject Negotiation

In this scenario we assume the following general procedure for data portability when the Data Subject shall be enabled to receive and transfer personal data:

> Data Subject DS1 wants to port personal data from Controller C1 to Controller C2. DS1 requests data-portability task from C1 for all its personal data P1 in Format F1. Controller C1 transfers P1 in F1 to DS1. C2 has Format F2. DS1 requests C2 to port P1 and therefore transfers P1 in F1. C2 negotiates with DS1, if necessary, to convert F1 to F2 to store P1.

This scenario has the advantage for the Data Subject that the data may be stored on any device of him or her and therefore usage of the data by the Data Subject is possible. This usage may include the transfer of the data to a target Controller as well as all basic operations (create, read, update, delete). With the possibility to store data on any device of the Data Subject, the responsibility of protecting the data from malicious actions also lies with the Data Subject. The Data Subject has to initiate the request for the data portability as well as the transfer to the target Controller or several target Controllers.
A Controller has to fulfil two roles in this scenario. A Controller has to be able to accept data portability requests and transfer data to the Data Subject. Additionally a Controller has to be able to process data received from a Data Subject. Hereby further interaction with the Data

Subject is a feasible option. The Data Format for such a transfer has to be generalized in a way that data transfer from any Controller Format to any other Controller Format will be allowed. For the Negotiation between the Data Subject and the target Controller it is possible to introduce a user interface as a supporting measure within the data transfer process.

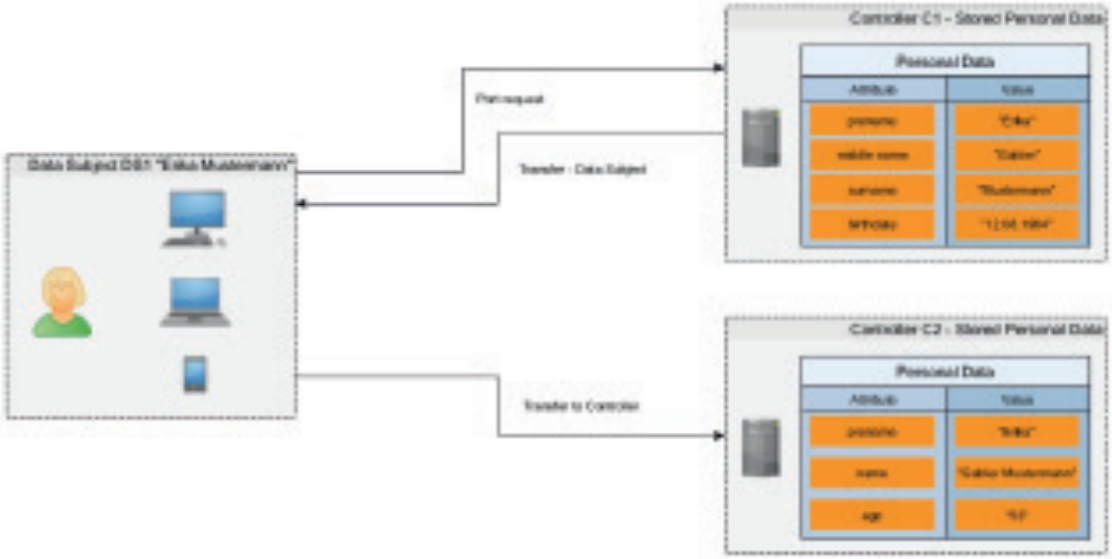


Figure 1: Data Subject Negotiation scenario showing the Data Subject DS 1 requesting and receiving personal data from Controller C1 and transferring it to Controller C2.

2.2. Controller Negotiation

In this scenario we assume the following general procedure for data portability if the Data Subject shall be able to receive and transfer the personal data:

> Data Subject DS1 wants to port personal data P1 from Controller C1 to Controller C2. DS1 has personal data P1 in Format F1 stored at Controller C1. DS1 has 1) an account for C2 or 2) no account for C2. DS1 requests C1 to port P1 in F1 to C2. C1 therefore transfers P1 in F1 to C2. C2 negotiates with C1, if necessary, to convert F1 to F2 to store P1. Additionally we assume that DS1 will be notified by C1 or C2 when the transfer is completed.

In this scenario the Data Subject initiates the Transfer of the Data between two Controllers without directly influencing the transfer process. The source Controller has to negotiate with the target Controller for the modalities of the transfer. Assuming that there is a common Format for the transfer of personal data between Controllers then this Format will be utilized. If we assume that no such Format is defined, then the Controllers have to agree on a Format and execute the transfer. This is likely to introduce domain-specific Formats. In any case the negotiation and transfer between Controllers has to be automated and therefore the Format has to be machine-readable. The transfer has to be carried out 'without hindrance' requiring both an export- and import-module.[15]

[15] Peter Swire/Yianni Lagos, *„Why the right to data portability likely reduces consumer welfare"*, Maryland Law Review 335 (2013): 344 f., see also Lucio Scudiero, *"Bringing Your Data Everywhere: A Legal Reading Of The Right To Data Portability"*, EDPL 1 (2017): 120.

The Controller should also inform the Data Subject about the outcome of the transfer this could include the registration of a new account. This can be executed by the source or target Controller or both of them. Art. 20 GDPR itself does not contain any provision concerning such information, but the general rule of Art. 12(2) and (3) GDPR may be applied to the source Controller, while the target Controller is under additional informational obligations as stipulated by Art. 13 GDPR since he is collecting personal data from the Data Subject.

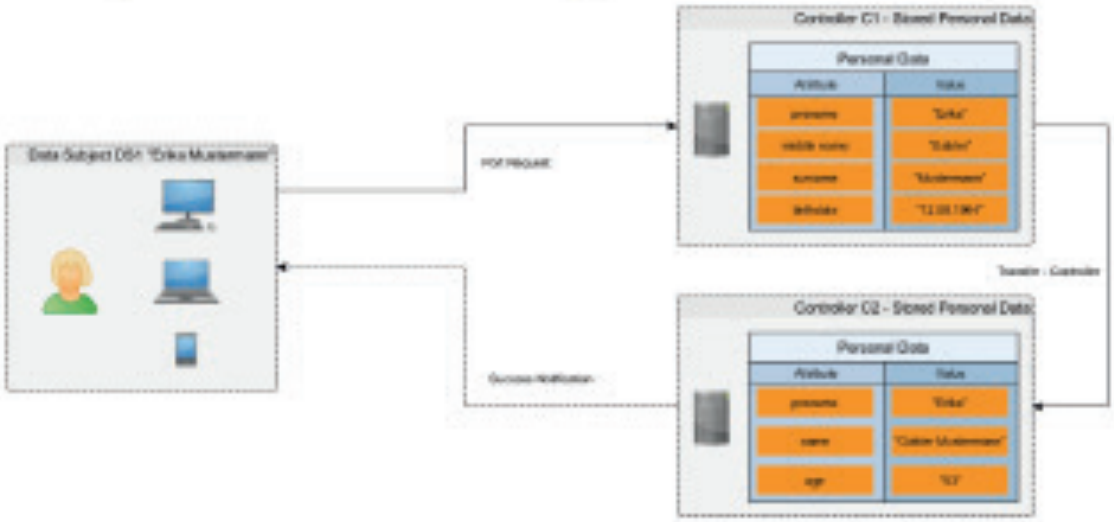


Figure 2: Controller Negotiation scenario showing the Data Subject DS1 initializing the Transfer of its personal data from Controller C1 to Controller C2 and receiving a success notification from Controller C2.

III. Data portability requirements

The following part shall describe the subject matter of the claims described in II.1. As already mentioned, there is no general Right to Data Portability. The Data Subject may not require any format which seems suitable for his or her needs, but only one fulfilling the 'interoperability' requirements (III.1.1). Also only personal data provided by the Data Subject to the Controller can be requested, when the processing was based on his consent or based on a contract (III.2.1).

1. Data Format

The requirements regarding the format may be discussed from a legal and technical perspective.

1.1. Legal

Art. 20 GDPR sets some basic standards for the format of the data that are given to the data subject or transferred to another controller. They can be summarized under the term 'interoperability'[16]. At this point it should be noted that only the interoperability of the format is required, not one of the services themselves.[17] The term interoperable is not used within Art. 20 GDPR, but in Recital 68. The GDPR lacks a definition of interoperability.

[16]Art. 29-Group, Guidelines to the right to data portability (Working Paper 242), 13.12.2016, 13.

[17]See discussion in Barbara Engels, *"Data portability among online platforms"*, Internet Policy Review 5:2 (2016): 4; Andreas Wiebe, *"Von Datenrechten zu Datenzugang"*, CR 2 (2017): 89.

The apparently only other legal document of the Union containing a definition of the term is the Computer Programs Directive.[18] The definition in general seems to be of limited use for the problems discussed here as it targets problems of interoperability of hard- and software in general, not format. The last part of the definition may have some merit: 'interoperability can be defined as the ability to exchange information and mutually to use the information which has been exchanged'. This can also be identified as the main aim of Art. 20 GDPR, but Art. 20 GDPR specifies additional qualities of an 'interoperable' format: it has to be structured, commonly used, and machine-readable.

The term 'structured' can be understood as referring to the arrangement of the information. In contrast to the draft by the European Commission, the perspective to be taken seems to one of the Controller. The formulation within the draft version 'to be further processed by the Data Subject' was replaced early in the negotiation process.

The additional criteria of machine-readability can only be a useful limitation if it is interpreted in a way, that machine-readability must not only be possible (e.g. OCR-readability), but the format shall be specifically designed to be machine-readable, possibly even requiring electronic form[19].

As opposed to the two criteria above, the term 'commonly used' is not a technical requirement. Whether a format is 'commonly used' is determined by market conditions. Thus it seems possible to have more than one commonly used format at a time. Considering the fast development of IT technology, the (temporary) existence of new markets without any commonly used format seems likely.[20] While some argue that proprietary formats can never fulfil this requirement[21], the wording of the norm itself does not seem to be that restrictive as long as a proprietary format is commonly used. The access to proprietary formats should be regarded a separate issue, which has already been approached by competition law.[22]

Art. 20 GDPR sets out minimal requirements to facilitate the interoperability of data formats.[23] However, this neither ensures compatibility, nor does it guarantee an outcome with regards to the interoperability of the systems. Again, this may be a consideration taking the competition law perspective into account. In comparison to other approaches, the one taken by the European Union seems to lack ambition. The Art. 45 of the ECOWAS Data Protection

[18]Directive 2009/24/EC, Recital 10.

[19]v. Lewinski, "Art. 20 DSGVO", in *BeckOK-DS*, ed. Heinrich A. Wolff/Stefan Brink, Rn. 74 ff.

[20] v. Lewinski, "Art. 20 DSGVO", in *BeckOK-DS*, ed. Heinrich A. Wolff/Stefan Brink, Rn. 78 ff.

[21]Art. 29-Group, Guidelines to the right to data portability (Working Paper 242) 13.12.2016, 13.

[22]EuG, 17.9.2007 – T-201/04, Slg. 2007, II-3601 – Microsoft/Kommission

[23]Lucio Scudiero, "Bringing Your Data Everywhere: A Legal Reading Of The Right To Data Portability", EDPL 1 (2017): 120.

Act for example is said to essentially guarantee the interoperability of technical devices by ensuring that any standard device or system can interpret processed personal data.[24]

1.2. Technical

Both the Data Subject and the Controller Negotiation scenario are based on legal requirements set by Article 20 GDPR. For the Data Subject Negotiation the Data Format in which the personal data are transmitted to the Data Subject can be either generalized for data portability or for uniform Data Subject Negotiation scenario enabling the Negotiation between Data Subject and Controller.

For the Controller Negotiation the Format can either be domain-specific as negotiated between the Controllers or it can be a generalized machine-readable Format.

Because both scenarios have to be considered, the properties (like shown in IV.) should be considered for a common Portability Format if no common set of personal data attributes can be defined. Otherwise if such a set of personal data attributes is defined, then a more specific Data Format could be defined. However, this is rather unlikely because a variety of attributes can identify a person uniquely.

Furthermore several combinations of personal attributes may lead to the identification of a Data Subject. Globally collecting all possible personal data attributes and forming a Data Format by them therefore seems not feasible, especially because it is debatable what belongs to the set of personal data attributes (see III.2.2).

2. Extent of data to be provided

Not all data linked to the account of a Data Subject at a certain Controller are to be transferred. This legal limits set by Art.20 GDPR again have to be implemented on a technical level.

2.1. Legal requirements

The extent of data to be provided to the data subject is limited by two criteria. As a part of the GDPR the right to data portability is limited to personal data concerning a data subject, which has to be interpreted as including only those personal data defined in Art. 4 Nr. 1 GDPR (‘any information relating to an identified or identifiable natural person’).

The second criterion leading to more significant limitation is that only such data may be received by the data subject which he or she has provided to the Controller. Clearly the Data Subject has to receive data entered into a registration form or pictures uploaded by the person. The concerns raised about further data especially outside social media applications[25] may only be mentioned here.

---

[24] *See* Uchena Jerome Orji, *“A Comparative Review of the ECOWAS Data Protection Act“*; CRi 4 (2016): 116; However, there are few specifics on the effect of this requirement in practise.

[25] For the debate within the banking see for example the statement of ‘The German Banking Industry Committee’ , accessed August 29, 2017, https://bankenverband.de/media/files/150903_DK_Stellungnahme_DSGVO.pdf.

The addition of the second criterion leads to certain legal peculiarities. A great example are pictures of the Data Subject uploaded by a third party[26]: While clearly meeting the requirement of 'personal data concerning the Data Subject', they would not fall under the right to data portability as introduced by Art. 20 GDPR because they have not been provided to the Controller by the Data Subject itself. Additionally, this criterion is not a requirement for claiming the right to access (Art. 15 GDPR) which may lead to some unclarity[27] (see V.2.2).
While this seems to be an odd outcome from a data protection perspective, it is another symptom of the broader legal nature of the right: Even though the Right to Data Portability is contained within the GDPR and thus formally part of the data protection laws of the Union, the legal nature of right is broader than its' formal localisation may suggest (see II.1.2.2).

2.2. Technical distinction

From a technical perspective for each Controller it has to be encoded which attributes are classified as personal data, have been provided by the Data Subject and which are related to other Data Subjects.
Attributes from a privacy-preserving point of view are classified in four groups. Explicit identifiers can identify a Data Subject on their own. Quasi identifiers can identify a Data Subject if a set of them is used. Sensitive attributes contain valuable information about the Data Subject but cannot identify him or her. Non-Sensitive attributes do not contain any valuable information.[28]
Personal Data as defined in Art. 4 No. 1 GDPR can directly or indirectly identify a Data Subject and therefore the classifications of explicit identifiers and quasi identifiers are contained within this legal definition. But it was shown that also sensitive attributes can be used to identify a Data Subject[29] and they should therefore be covered by the GDPR or more specifically the Right to Data Portability. Additional concerns may be raised by services making use of combined data and the value derived from them.[30] The more data become available, the more likely such side effects occur and the combination of attributes can enable the identification of the Data Subject.

---

[26]See Inge Graef, *"Mandating portability and interoperability in online social networks"*, Telecommunications Policy 39 (2015): 507.

[27]Lucio Scudiero, *"Bringing Your Data Everywhere: A Legal Reading Of The Right To Data Portability"*, EDPL 1 (2017): 122.

[28]Latanya Sweeney, *„k-anonymity: A model for protecting privacy"*, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,10:5 (2002): 557.

[29]Ashwin Machanavajjhala/Daniel Kifer/Johannes Gehrke/Muthuramakrishnan Venkitasubramaniam, *„Diversity: Privacy Beyond k-Anonymity"*, ACM Trans.Knowl. Discov. Data, (2007): 1, accessed August 29, 2017 doi:10.1145/1217299.1217302.

[30]Stefan Weiss, *„privacy threat model for data portability in social network applications",* International Journal of Information Management 29 (2009). 251.

Therefore only non-sensitive attributes will not be covered by the Right to Data Portability. Such data might be sensor data which is not related to any Data Subject, e.g. process monitoring in Industry 4.0[31].

Any Data Subject related attribute like comments in a forum, tweets in Twitter or smart health data might be exploited to identify a Data Subject. This type of information is also most likely to cause problems with regard to the distinction between attributes only relating to the Data Subject and such Data also relating to other natural persons, which are excluded from the scope of the Right to Data Portability. For example a Tweet created by a Data Subject is basically text with some additional meta-information like the creation date. The task for the Controller is now to distinguish if this Tweet is classified as personal data or not based on this text. Classifying the Tweet as personal data based on the text is a serious problem.

IV. The Negotiation Process

During the Negotiation of both scenarios described above (II.2) it is possible that one or more of the following processes have to be applied when a source scheme F_source, with the attributes A_source1 … A_sourceN, has to be matched against the target scheme F_target, with the attributes A_target1 … A_targetM. Hereby the number of attributes can differ (N != M). For each attribute we consider an identifier, e.g. 'name' and the format of the attribute, e.g. 'text' or 'number'. Additionally we assume that the format of the can be more specialized by adding constraints, e.g. 'text(300)' defining that the text has maximal 300 characters.

- **Attribute Exact Match:** Assuming an attribute A_source1 of F_source1 and an attribute A_target1 of F_target1 with the same identifier 'surname' and attribute 'text'. Then the value of A_source1 can be migrated without alteration. Therefore a Data Format enabling data portability has to have the ability to model an identifier and attribute format for each value.
- **Attribute Semantic Match:** Assuming an attribute A_source1 of F_source1 with the identifier 'surname' and an attribute A_target1 of F_target1 with the identifier 'name'. The format is 'text' in both cases. This resembles a semantic variety between the source and the target scheme. Therefore a Data Format enabling data portability has to support different notations for the same value to support semantic matching. For example a list of identifiers for a value could be allowed. The list could be extended by the Controller every time a identifier is unknown or a central data portability repository is introduced that can be used to lookup unknown identifiers for Controllers which also submit their own identifiers. This would lead to new questions like who is responsible for maintaining and administrating such a central data portability repository.
- **Attribute Value Segregation:** Assuming an attribute A_source1 of F_source1 with the identifier 'address', an attribute A_target1 with the identifier 'street' and an

[31] BMBF, *„Industrie 4.0, Innovationen für die Produktion von morgen"*, accessed August 29, 2017, https://www.bmbf.de/pub/Industrie_4.0.pdf.

attribute A_target2 with the identifier ‘streetNumber’ of F_target1. The format is ‘text’ in both cases. We assume that for F_source1 the address will be separated as ‘STREET STREET_NUMBER’ within the actual value. Therefore a Data Format enabling data portability has to support the segregation of values. This could be done by a fine-grained description of the format of the attribute including additional sub-identifier and sub-formats for the source Format F_source1.

- **Attribute Value Junction:** Assuming an attribute A_source1 with the identifier ‘street’ and an attribute A_source2 with the identifier ‘streetNumber’ of F_source1 and an attribute A_target1 with the identifier ‘address’ of F_target1. The format is ‘text’ in both cases. We assume that for F_target1 the address will be separated as ‘STREET STREET_NUMBER’ within the actual value. Therefore a Data Format enabling data portability has not only to support segregation but also the junction of values. This could be done by the same method described above for the target Format F_target1.
- **Attribute Processing:** Assuming an attribute A_source1 with the identifier ‘birth-date’ and the format ‘date’ of F_source1 and an attribute A_target1 with the identifier ‘age’ and the format ‘number’ of F_target1. Based on the birth-date and the current date it is possible to compute the age. With this setup not only the identifier differs but also the format. Therefore a Data Format enabling data portability has to support processing of one or more attributes to compute a value for a target attribute. First of all the semantic relation between identifiers has to be established. Based on this processing rules have to be defined that can be executed on the target Controller. This is also necessary when the format of two attributes with the same identifier differ. For example assuming an attribute A_source1 with the identifier ‘birth-date’ and the format ‘date’ of F_source1 and an attribute A_target1 with the identifier ‘birth-date’ and the format ‘text’ of F_target1. Within this scenario the format ‘date’ has to be processed to ‘text’.
- **Attribute Miss:** Assuming an attribute A_source1 with the identifier ‘birth-date’ and the format ‘date’ of F_source1 and a set of attributes A_target1 … A_targetM of F_target1 with no matching identifier to A_source1. In this scenario the target Format misses an attribute in the source Format. It is also possible that the source Format misses an attribute of the target Format. In both cases an appropriate handling for the missing attribute has to be applied.
- **Manual Attribute Matching:** For the Data Subject Negotiation scenario we assume that the Data Subject can assist the Negotiation process with a user interface. In such a user interface the user could assign source attributes to target attributes to verify or correct attribute assignments by previous processes. To allow the user to understand both the source and target Data Format it is necessary to add human readable labels to each attribute.

A Portability Format PF supporting data portability should support all mentioned processes on the attribute level, even for complex data structures. Assuming such a Portability Format exists, and then both the source Format and the target Format, described with the Portability Format, can be ported. Related work has been done for the semantic web with a focus on ontology matching based on metadata.[32] During the Negotiation process the source Controller C_source has its data stored in the Data Format F_source. When this data is transferred to the target Controller C_target it first has to be transformed to the Portability Format resulting in PF(F_source) which adds additional metadata. During the Negotiation step the target Controller C_target first has to provide its own Data Format F_target as the Portability Format PF(F_target). Then both provided Portability Formats are used to match the attributes resulting in the port to the Data Format F_target. For the matching of the source Format F_source to the target Format F_target during the Negotiation not only the metadata but also rules for applying suitable matching methods have to be considered[33].

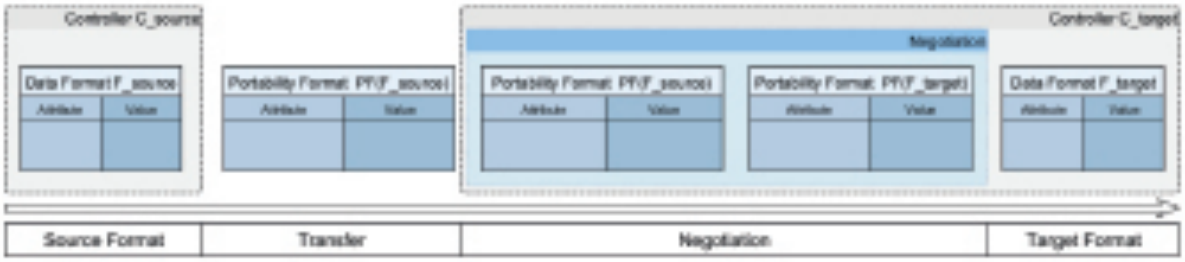


Figure 3: Transfer of personal data from Controller C_source to C_target utilizing the Portability Format for the Negotiation.

V. Additional non-format related requirements

Art. 20 GDPR is a rather short norm not considering many aspects of the data transfer process itself. For some it can be referred to the general provisions of the GDPR. Others would be desirable to create a consistent framework of Data Protection rules and a workable right to Data Portability.

1. Security and Access Control

From a legal perspective there are only very broad specifications as to the security aspects of the data transfer process: They may be derived from the general requirements stipulated in Art. 5(1) lit. d ('accurate') and lit. f ('integrity and confidentiality'). The Right to Data Transfer does not require any additional security provisions.

Default security measures have to be applied to meet the above requirements. For example the transfer of the personal data between a Controller and Data Subject or a Controller and

[32] Jens Hartmann/ Elena P. Bontas/Raúl Palma/Asunción Gómez-Pérez, "DEMO - Design Environment for Metadata Ontologies, The Semantic Web: Research and Applications", in *3rd European Semantic Web Conference, ESWC 2006 Budva, Montenegro, June 11-14, 2006 Proceedings* (Berlin/Heidelberg: Springer, 2006), 441.

[33] M. Mochol, E. Paslaru and B. Simperl, "A High-Level Architecture of a Metadata-based Ontology Matching Framework", in *17th International Workshop on Database and Expert Systems Applications (DEXA'06)* (Krakow, 2006), 354-358, Accessed August 29, 2017, doi: 10.1109/DEXA.2006.9.

another Controller could be threatened by a Man-in-the-Middle attack which can lead to the leak of the personal data to the attacker. A risk casually mentioned in the data portability context[34] is the additional risk of multi-platform identity theft once the offender gained access to one service supporting data portability functionalities. Therefore an end-to-end encrypted transfer[35] should be applied. But encrypting the connection may not be sufficient on its own to prevent such attacks, as long as the communication partners are not authenticated[36].
Additionally only the Data Subject related to the personal data should be able to initiate data portability and therefore has to be authorized. This requires the appliance of suitable access control measures for the data portability process.
Further security measures have to be applied to prevent additional possible attacks, e.g. like those described in the OWASP Top Ten[37]. It has to be considered that new attack schemes might arise based on data portability functionalities since any additional interface may cause additional risks.

2. Human-readability

Providing of a human-readable version of the personal data to be transferred upon a request of Data Portability also seems a topic worthy of discussion. It would be highly beneficial to strengthen the informational self-determination of the individual. The Article 29 Data Protection Working Party thus recommends that the Data Subject shall have the possibility to choose between several types of data he may or may not want to receive. This requires a human-readable representation. Additionally, the informational requirements of the GDPR (see II.2.2) could be fulfilled within the necessary user interface.

2.1. Technical requirements

Based on the Data Subject Negotiation scenario (see II.2.1) it is possible that the Data Subject is participating in the Negotiation process, therefore a user interface is required. Even within the Controller Negotiation scenario (see II.2.2) a transfer is initiated only on request by the Data Subject which requires at least a minimalistic version of a user interface. This user interface should be capable to support the user in assigning attributes from the source Data Format described by the Portability Format to the target Data Format. Hereby the Data Subject may aid the negotiation process by manually matching attributes which could not be assigned or add additional required information. This can either be done by integrating human-readable descriptions in the Portability Format on the attribute level or the Source Controller

---

[34]See Peter Swire/Yianni Lagos, *„Why the right to data portability likely reduces consumer wellfare“*, Maryland Law Review 335 (2013), 339.

[35]BSI, *„IT-Grundschutz, M4.101 Sicherheitsgateways und Verschlüsselung“*, accessed August 29, 2017, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04101.html.

[36]BSI, *“IT-Grundschutz, G 5.143 Man-in-the-Middle-Angriff”*, accessed August 29, 2017, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05143.html.

[37]OWASP Top Ten Project, accessed August 29, 2017, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

has to provide an interface managing requests from target Controllers. The later method would cause several additional problems considering that several versions may have been to be supported in the long term, which would just be included in the specific Portability Format file describing the personal data of a Data Subject at a specific point in time.
Introducing human-readable descriptions in the Portability Format would furthermore allow for a generic Portability Format Viewer enabling the Data Subject to inspect his or her personal data. This is possible if the Portability Format is designed as a standardised format.

2.2. Right to receive data in human-readable form?

A legal basis to receive data in a human-readable form can be found in Art. 15 GDPR ('Right of access by the data subject'). Art. 15(3) GDPR also allows the controller to provide the data as described in Art. 15 GDPR in a 'commonly used electronic form', unless the Data Subject requests otherwise. Recital 63 even encourages the Controller to provide direct access to the data where possible.
While it must be noted that the rights in Art. 15 and 20 GDPR fulfil different purposes and there is no legal requirement within Art. 20 GDPR to present a human-readable form during the transfer process, a technical system as shown above (V.2.1) can easily be designed to ensure compliance with both norms.
Careful consideration must be paid to the fact that the right of access in Art. 15(1) GDPR requires the Controller to allow access to all the personal data concerning the Data Subject that are being processed, while Art. 20(1) GDPR only grants a right to data portability when in addition the data where provided to the Controller by the Data Subject.
A unification of the two requirements as proposed by the European Parliament in an earlier draft [38] should be reconsidered, as the right to Data Portability may be seen as a mere specification of the right to data access.[39]

3. Domain-specific data

There are no clear legal rules as to which services are addressed by the Data Portability requirements. It is clear that the obligation was aiming at social media services, but in there is no such limitation within the GDPR.
Additional Problems may arise when two services – while operating within the same general branch – are in detail offering very different functions. While this could be considered a technical boundary (■II.1.2.3.), it seems more appropriate to treat the incompatibility of two business models as a separate problem. Irrespective of the classification, this will place significant limits on the Right to Data Portability in practise.
Data portability of domain-specific personal data may be possible for well-defined Data Formats but will not always be possible even within the same branch. For example, it seems unlikely to transfer personal data from Facebook to a Twitter account. Although basic regis-

[38]COM(2012)0011 – C7-0025/2012 – 2012/0011 (COD), p. 92 f.

[39]W. Gregory Voss, *„One year an loads of data later, Where are we? An update on the proposed European Union General Data Protection Regulation"*, Journal of Internet Law 10:10 (2013): 21.

tration forms may be transferable, other content is simply not meant to be displayed within the other system; e.g. Twitter allows a maximum length of 140 characters for a Tweet[40] but Facebook allows longer posts for a profiles' feed[41].

As a counter-example one may assume two Controllers C1 and C2 providing an e-mail service. If a Data Subject wants to transfer his or her e-mails (as part of personal data) from C1 to C2 then this might be feasible, because the format for e-mails is standardised[42] and the services offered are alike. However, the transfer of data between competing services on the other hand raises the most sensitive competition law issues.[43]

VI. Conclusion

The right to data portability as contained in Art. 20 GDPR is of limited scope and only sets broad boundaries[44]. While there are some plausible reasons, especially from a market perspective, that data portability should not be an 'all-or-nothing' feature'[45] to avoid (possibly unintentional) damages to competition, it does not seem too far-fetched to state that the future development of data portability will mainly be driven be technological development, as well as the willingness of the market players, which in turn is largely based on the question whether Data Portability provides economic benefits. This may be underpinned by the fact the establishment of data portability technologies by global players predate the earliest drafts of the GDPR. The law as of now will be of limited influence.

For the technical realization of the right to data portability it is necessary to find a common and formally described Portability Format with properties enabling and supporting the Negotiation process for both the Data Subject Negotiation and Controller Negotiation scenario. To strengthen the information self-determination it is desirable to introduce human-readability as a requirement for the Portability Format to both inform the Data Subject and assist the Negotiation process by allowing manual intervention. Such a Portability Format has to be researched and the interfaces for the Controller enabling the right to data portability have to be defined in the future to avoid proprietary solutions. Such a Portability Format shall include sufficient metadata to enable the Negotiation process. It would clearly be beneficial if associations and other bodies representing Controllers would make use of the possibilities to prepare code of conducts (Art. 40 GDPR) in order to ease to exercise of the Right to Data Port-

---

[40] Twitter Developer Documentation, accessed August 29, 2017, https://dev.twitter.com/basics/counting-characters.

[41] Facebook Graph API Documentation, accessed August 29, 2017, https://developers.facebook.com/docs/graph-api/reference/post.

[42] W3C, RFC822: Standard for ARPA Internet Text Messages, accessed August 29, 2017, https://www.w3.org/Protocols/rfc822/.

[43] Barbara Engels, *"Data portability among online platforms"*, Internet Policy Review 5:2 (2016): 5.

[44] Some even refer to a rather symbolic motivation, v. Lewinski, "Art. 20 DSGVO", in *BeckOK-DS*, ed. Heinrich A. Wolff/Stefan Brink, Rn. 1.1.

[45] Barbara Engels, *"Data portability among online platforms"*, Internet Policy Review 5:2 (2016): 5.

ability by the Data subject. However, it is doubtful whether the economic advantages are strong enough to warrant such market behaviour.

The legal requirements as set by Art .20 GDPR thus can only be a starting point to target the most extensive limits to portability.[46] A true and valuable Right to Data Portability should not only be more consistent with other rights within the GDPR (e.g. Art. 15) but must also consider a broader perspective. Not only the competition law perspective on market access and interoperability have to be considered. The different requirements of Art. 15 GDPR also show the imminent need for a consistent Data- and Informational Law within the Union, establishing a legal quality of 'Data' and clarifying 'ownership' of data especially when related to multiple Data Subjects. Careful consideration also should be paid to the fact, that non-personal data may also have economic value[47]. This again calls for a broader perspective on data portability including both personal and non-personal data provided by a Data Subject.

As long as a true, unified Data- and Informational Law of the Union is still at its' infancy, the Data Protection law should focus on the guarantee of 'flanking policy frameworks'[48] regarding security, authentication, access control, human readability as discussed in V., as well as the development of criteria to distinguish services that are so similar that data transfer is a general option from purely domain specific data that are not compatible with services from other domains.

[46] eg contractual restrictions to offer additional portability tools, see http://europa.eu/rapid/press-release_SPEECH-12-372_en.htm, accessed August 29, 2017.

[47] Recital 13 in Com 2015 (634); „Digital content is often supplied not in exchange for a price but against counter-performance other than money i.e. by giving access to personal data **or other data**".

[48] Barbara Engels, *"Data portability among online platforms"*, Internet Policy Review 5:2 (2016): 14.

Notizen

Notizen

Notizen

Notizen

II. Technisches Gutachten – SCRC e.V. Leipzig

Expertise zur Datenportabilität

Oktober 2017

Leipzig, 04.10.2017

Inhalt

Verfasser:
Dr. Gunnar Hempel
Karl Schmid
(SCRC e.V. Leipzig, an der Universität Leipzig, Lehrstuhl für Wirtschaftsinformatik, Prof. Dr. Rainer Alt)

Oktober 2017

1 Ziel des vorliegenden Dokuments

Mit dem Recht auf Datenportabilität kommt ab dem 25. Mai 2018 eine gesetzliche Neuerung auf datenverarbeitende Stellen zu. Betroffene Personen erhalten nach Art. 20 Abs. 1 DSGVO das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder diese Daten an einen anderen Verantwortlichen übermitteln zu lassen. Damit sollen dem Verbraucher zum einen der Wechsel von einem Anbieter zu einem anderen Anbieter von Diensten erleichtert und somit zum anderen LOCK-in-Effekte verhindert werden.

Die gesetzlichen Vorschriften selbst geben nur grundlegende Anforderungen vor. Dabei bleiben sie rechtsdogmatisch insgesamt technikneutral und zielbeschreibend. Diese Ausgangssituation schafft derzeit einen Raum an Unsicherheit und Ungewissheiten, wie in der Praxis vorgegangen werden soll. Die Lösungsfindung für Anwender und Verantwortliche wird ein Prozess sein, der sich sowohl in der fortschreitenden technischen und gesellschaftspolitischen Entwicklung als auch in der ständigen Rechtsprechung fortentwickeln wird.

Um einen praxistauglichen Ansatz hierfür anzustoßen, wird sich diese Expertise mit den Rahmenbedingungen auseinandersetzen, die den gegenwärtigen Status Quo (Stand von Technik, Forschung und Rechtslage) widerspiegeln. Im vorliegenden Dokument werden die rechtlichen und technischen Anforderungen zur Datenportabilität nach der Datenschutzgrundverordnung (DSGVO) betrachtet, um einen Rahmen und mögliche Wege für eine praktikable, praxistaugliche Umsetzung des Rechts auf Datenportabilität zu validieren und aufzuzeigen. Der Schwerpunkt der Betrachtung soll dabei zeigen, auf welche Leitgedanken die Verantwortlichen abstellen und mit welchen Mitteln bzw. Techniken sie den gesetzlichen Erfordernissen nachkommen können.

2 Problemdarstellung und betroffene Ebenen aus Sicht der IT

Dienstanbieter werden durch das Recht auf Datenportabilität vor die Aufgabe gestellt, bestehende IT-Systeme insoweit anzupassen oder zu ergänzen, dass konkret definierte Datensätze (personenbezogene Daten) an die betroffene Person (nur natürliche Personen) oder an einen von ihr benannten anderen Dienstanbieter übermittelt werden können. Diese Daten müssen in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden.

Um eine praxistaugliche Lösung zur Umsetzung des Rechts auf Datenportabilität zu schaffen, sind im Wesentlichen fünf Ebenen (Hauptgestaltungsaspekte) zu betrachten und in der Struktur eines Umsetzungsprojektes abzuarbeiten:

- **Welche Daten sind betroffen**
- **Wo sind die Daten abgelegt**
- **In welchem Format sind die Daten zu exportieren**
- **Womit sind die Daten zu exportieren**
- **Wie sind die Daten zu übertragen**

Die Frage, **welche Daten** zu übermitteln sind, ist grundsätzlich eine rechtsdogmatische Problemstellung. Art. 20 Abs. 1 DSGVO benennt hierbei in der deutschen Übersetzung explizit solche personenbezogenen

Daten der betroffenen Person, die sie einem Verantwortlichen „bereitgestellt“ hat. Die englische Fassung verwendet den Begriff „provided“. Die Vorschrift kommt überall dort zur Anwendung, wo die Verarbeitungsprozesse auf einer Einwilligung oder auf einem Vertrag mit der betroffenen Person beruhen und auf automatisierten Verfahren basieren.

Als zentrale Frage zeichnet sich hier ab, wie genau der Begriff „bereitgestellt“ zu definieren ist. Eine Legaldefinition des Begriffs ist in der DSGVO nicht aufgeführt. Dennoch wird in den jeweiligen Anwendungsfällen eine klare Abgrenzung zu solchen Daten erforderlich sein, die der Anbieter für seine Zwecke aus den bereitgestellten Daten der betroffenen Person generiert bzw. ableitet (englisch: „inferred“, „derived“).

Eine allgemeingültige trennscharfe Unterscheidung ist schwierig zu formulieren. Zum einen deshalb, da hierbei verschiedenste Kategorien von Verarbeitungsprozessen in verschiedenen Branchen (Internetdienstleistungen, vernetztes KFZ, Energiebranche, Versicherungen, KMU Dienstleister mit Kundenportal, etc.) zu berücksichtigen sind. Zum anderen, weil die Bereitstellung für diese Verarbeitungsprozesse auf ganz verschiedene Art und Weise (händisch selbst eingetragen oder via IT-System an den Dienst übermittelt) oder in verschiedenen Zusammenhängen (Nutzer, Arbeitnehmer am Arbeitsplatz, …) geschehen kann. Zu denken ist hierbei insbesondere an Smarte Produkte der betroffenen Person, die Daten für den Dienst eines Anbieters an diesen übermittelt und damit in gewisser Weise auch „bereitstellt“.

Es ist notwendig, für die Anwendungsfälle eine solche trennscharfe Abgrenzung vorzunehmen, um klar definieren zu können, welche Datensätze zu exportieren sind, um dem Recht auf Datenportabilität nachzukommen.

Wo die Daten hinterlegt sind, umfasst die Problematik, dass die personenbezogenen Daten in einem Unternehmen mit automatisierten Verarbeitungsprozessen typischerweise auf verschiedenen technischen Ebenen mit unterschiedlichen Strukturen und technischen Beschaffenheiten abgelegt sind (mindestens Datenbanken, Mailsysteme, Dokumentenmanagement, ggf. Office-Daten). Häufig fehlen entsprechende Dokumentationen, auch wenn sie im Rahmen der zu erstellenden Verfahrensverzeichnisse vorhanden sein sollten.

Die Frage, **in welchem Format** die Daten zu übermitteln sind, betrifft technische, rechtliche und auch wirtschaftliche bzw. akzeptanzorientierte Aspekte. Die Besonderheit besteht darin, dass die Anforderungen an die technische Realisierung durch den Gesetzgeber nur vage formuliert sind und an keiner Stelle präzisiert werden.

Die Datenschutzgrundverordnung sieht allgemein vor, dass organisatorische und auch technische Maßnahmen und Verfahren zu schaffen sind, um die Ziele der Vorschriften effektiv umzusetzen. Dabei bleibt das Gesetz technikbeschreibend und technologieneutral. Ein bestimmtes Format oder ein Standard werden nicht postuliert. Vorgegeben wird nach dem Wortlaut nur die Verwendung eines strukturierten, gängigen und maschinenlesbaren Formats. Ferner wird zur Entwicklung von interoperablen Formaten aufgefordert (Erwägungsgrund 68), die die Weiterverarbeitung der Daten in anderen Systemen ermöglichen. Im Vorfeld der DSGVO zeigt sich hierbei in der Praxis eine verbreitete Unsicherheit, auf welches Format abgestellt werden soll.

Auch wenn einerseits eine Standardisierung effektiv sein kann, sind kartellrechtliche Fragen zu bedenken sowie Aufwände/Kosten der Umsetzung und die Anpassbarkeit an verschiedene, auch zukünftige Anforderungen (Generik) abzuschätzen.[1]

Womit die Daten zu exportieren sind, umfasst die Frage, über welche Technologie (Programmiersprache, Standardexportroutinen, ETL-Tools etc.) die relevanten Daten auszulesen sind. Von der rechtlichen

[1] Die Betrachtung dieser Aspekte ist nicht mehr Gegenstand dieser Stellungnahme.

Seite her gibt es hier keinerlei Beschränkungen. Die technisch zur Verfügung stehenden Möglichkeiten sind vielfältig.

Wie die Daten zu übertragen sind, wirft die Frage auf, wie die Daten zur betroffenen Person (Mail, Download, Datenträger per Post, ...) bzw. zum autorisierten Dienstanbieter (z.B. Web-servicebasierter Austausch zwischen Systemen) gelangen sollen. Hier ist auch zu bedenken, ob der zu transportierende Datenbestand archiviert werden sollte, um spätere Haftungsprobleme für den liefernden Dienstanbieter auszuschließen; ebenso sind alle Aspekte der Verschlüsselung, Authentifizierung, Autorisierung etc. zu beachten.

3 Rechtliche Betrachtungen und betroffene Ebenen

Die rechtlichen Anforderungen des Rechts auf Datenportabilität ergeben sich aus Art. 20 DSGVO und dem Erwägungsgrund 68. Funktional ist die Vorschrift als ein Betroffenenrecht zur Selbstbestimmung postuliert.[2] Andererseits verfolgt sie aber auch wettbewerbspolitische und allgemein verbraucherschützende Ziele.[3] Der für die Problemstellung relevante Wortlaut enthält folgende Regelungen:

DSGVO Vorschrift	Regelung
Art. 20 Abs. 1	Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln. Voraussetzung: 1.-Die Verarbeitung basiert auf einer Einwilligung oder einem Vertrag (Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a; Art. 6 Abs. 1 lit. b); 2.-Die Verarbeitung erfolgt mithilfe automatisierter Verfahren.
Art. 20 Abs. 2	Die Übermittlung nach Abs. 1 direkt von einem Verantwortlichen an einen anderen Verantwortlichen kann nur erwirkt werden, wenn dies technisch machbar ist.
Art. 20 Abs. 4	Das Recht nach Art. 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. [Anmerkung: redaktioneller Fehler! - gemeint ist ein Verweis auf Abs. 1]
Erwägungsgrund 68	Vorgaben: 1.-Die betroffene Person sollte berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt

[2] So Erwägungsgrund 68 S. 1; *Gola*, Datenschutzgrundverordnung (2017), Art. 20 RN 3; Art: 29 Datenschutzgruppe WP 196, 14 (16), WP 242, S.1 (Artikel-29-WP *Guidelines on the right to data portability. Adopted on 13 December 2016. As last Revised and adopted on 5 April 2017*. 2017. Article 29 Data Protection Working Party, WP 242, rev.01, http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (Abruf: 2017-09-27); ähnlich zu diesem Thema auch das *White House Office of Science and Technology Policy*. Request for Information Regarding Data Portability.
[3] *Kühling/Buchner*, Datenschutzgrundverordnung (2017), Art. 20 RN 4; (die Art. 29 Datenschutzgruppe betonte dies in der alten Fassung des WP 242, 1. gleichfalls; in der aktualisierten Fassung wurde dies allerdings relativiert).

	hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln, um bessere Kontrolle über die eigenen Daten zu haben. 2.-Die Verantwortlichen sollten dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. 3.-Das Recht der betroffenen Person zur Übermittlung der Daten sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten. 4.-Das Recht der Übermittlung der Daten an einen anderen Verantwortlichen sollte erwirkt werden können, soweit es technisch machbar ist.

Anhand dieser Regelungen sind die folgenden vorrangigen Problemstellungen zu lösen:

- Welche Daten sind vom Recht auf Datenportabilität betroffen
- In welcher Form sind die Daten zu exportieren

Sofern der Wortlaut keine eindeutigen Vorgaben postuliert, sind die Regelungen nach dem Sinn und Zweck der Norm, im Sinne des Betroffenenrechts zur Selbstbestimmung, auszulegen.

Welche Daten sind vom Recht auf Datenportabilität betroffen

Vom Recht auf Datenportabilität sind die Daten betroffen, die die Merkmale „… *die betroffene Person betreffend …"* und einem „… *Verantwortlichen von der betroffenen Person bereitgestellt* …" erfüllen.

Damit können ausschließlich personenbezogene Daten Gegenstand des Rechts sein. Alle anonymisierten Daten oder solche, die die Person nicht betreffen, fallen aus dem Anwendungsbereich der Vorschrift heraus. Bereits an dieser Stelle ist für den Verantwortlichen zu beachten, ob die zu exportierenden Daten der betroffenen Person selbst oder einem anderen Verantwortlichen zu übermitteln sind. Sofern die Übermittlung an einen anderen Verantwortlichen erfolgen soll, schränkt Art. 20 Abs. 4 DSGVO den Umfang der Daten dahingehend ein, dass nur solche Daten übertragen werden dürfen, die nicht mit Rechten oder Freiheiten anderer Personen in Verbindung stehen. Ausdrücklich betrifft dies Daten anderer Personen, die in den Datensätzen der antragstellenden betroffenen Person enthalten oder mit diesen verknüpft sind. Zu denken ist beispielsweise an Telefonrechnungen (in der Auflistung können Angaben zu anderen Telefonkunden enthalten sein), an Kontoauszüge (in den Auszügen können Angaben von Überweisenden oder Empfängern enthalten sein), an Chatverläufe oder an Verknüpfungen in Social Media Accounts (hier können Angaben zu Dritten enthalten sein) usw.

Für den Datenexport müssen deshalb Funktionen hinterlegt werden, die eine entsprechende Differenzierung ermöglichen. Solche Datensätze mit Angaben zu anderen Personen dürfen im Ergebnis grundsätzlich nicht an andere Verantwortliche, sondern nur an den Antragsteller selbst übermittelt werden. Eine Übertragung von Datensätzen mit Angaben anderer Personen an einen neuen Verantwortlichen ist unter Umständen dann möglich, wenn die antragstellende betroffene Person ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO) geltend machen kann und keine überwiegenden Interessen oder Rechte und Grundrechte eines betroffenen Dritten entgegenstehen. Die Übertragung von Datensätzen mit Angaben zu Dritten schafft ein rechtliches Risiko für den Verantwortlichen. Dabei ist im Detail zu prüfen, ob und wann eine Übertragung rechtlich zulässig ist.

Mit dem Merkmal „bereitgestellt“ wird generell der Umfang an Daten für den Export eingeschränkt. Als bereitgestellt gelten Daten immer dann, wenn die betroffene Person die Angaben wissentlich und aktiv an den Verantwortlichen übermittelt hat. Hierunter fallen beispielsweise solche Angaben, die die betroffene Person in eine Online-Maske eines Verantwortlichen (Onlineshop, Onlinedienst, Social Media Anbieter etc.) eingetragen hat.

Fraglich ist jedoch, inwieweit auch solche Daten als bereitgestellt anzusehen sind, die anhand der Nutzungsaktivitäten der betroffenen Person erzeugt und vom Verantwortlichen erhoben bzw. verarbeitet werden. Hierunter fallen denklogisch all diejenigen Daten, die bei der durch den Nutzer veranlassten Onlinenutzung entstehen oder durch den Einsatz eines Smart Service des Nutzers (Smart Service, Smart Product, Apps, IoT etc.) an den Verantwortlichen übertragen werden (beispielsweise: Wearables, Smarte Stromzähler, vernetzte Fahrzeuge, Browser- und Suchmaschinenhistorien, GPS-Lokalisation etc.).

Abzugrenzen sind diese Daten, die anhand von Nutzeraktivitäten entstehen, von solchen Informationen, die der Verantwortliche aus der Nutzung selbst ableitet und damit Rückschlüsse für seine eigenen Interessen bzw. Belange erzeugt. Ausdrücklich betroffen sind hiervon Bewertungen des Nutzers oder der Nutzungsaktivitäten, die für den Verantwortlichen von Interesse sind (um beispielsweise seinen Dienst zu verbessern oder zu monetarisieren).
Abgeleitete Daten sind nicht als von der betroffenen Person bereitgestellt anzusehen und stellen somit eine Datenkategorie dar, die nicht vom Recht auf Datenportabilität erfasst ist.

Eine eindeutige Abgrenzung der Datenkategorie in bereitgestellt und abgeleitet wird in der Praxis von einigen Seiten als problematisch betrachtet.

Die Artikel 29 Datenschutzgruppe, ein unabhängiges Beratungsgremium der Europäischen Kommission zu Fragen des Datenschutzes[4], hat in einer Stellungnahme zum Thema Recht auf Datenportabilität einige (nicht bindende) Leitlinien für die Auslegung des Begriffs „bereitstellen“ und damit für die Abgrenzung der Datenkategorien ausgearbeitet.[5] Das Gremium formuliert in seiner Empfehlung, wie die Datenkategorien abzugrenzen sind, dass „lediglich aus Rückschlüssen erzeugte Daten und abgeleitete Daten“ [algorithmische Ergebnisse] von dem Recht auf Datenportabilität ausgeschlossen sind. Im Umkehrschluss sind alle Informationen der Aktivität einer Person und der von ihr zugelassenen Beobachtung dieser Aktivität (Browserverlauf, Fahrverhalten im KFZ, Art und Umfang der Nutzung eines Dienstes etc.) als bereitgestellte Daten anzusehen, die dem Recht auf Datenportabilität unterliegen.

Diese weite Auslegung wird von verschiedenen Seiten kritisch betrachtet.[6] Wenn nach dieser Empfehlung auch Daten als bereitgestellt anzusehen sind, die das Ergebnis der Beobachtung eines Verhaltens darstellen (im Telekommunikationsbereich damit beispielsweise Logfiles, Verkehrs- und Standortdaten; im medizinischen Bereich betrifft dies u.a. Messungen bei Fitnessaktivitäten [Puls, Blutdruck, Körpergewicht etc.], im Mobilitätsbereich betrifft dies die Reaktionsgeschwindigkeit in Verbindung mit Fahrzeugfunktionen etc.), sehen die Verantwortlichen zum einen die Gefahr, dass hier für die betroffene Person ein nicht mehr sinnvoller oder brauchbarer Datensatz aus einer Unmenge von Informationen zu exportieren ist, der im Ergebnis nur geringen Nutzen für die betroffene Person hat und einen unverhältnismäßigen Aufwand für die Verantwortlichen bedeutet. Zum anderen sehen die Verantwortlichen das Problem, dass diese Daten in einem so engen Zusammenhang mit internen Prozessen des Verantwortlichen stehen, dass andere Verantwortliche ggf. aus diesen Informationen Rückschlüsse auf oder auch detaillierte Hintergrundinformationen zum Aufbau der verwendeten Algorithmen vom ursprünglichen Verant-

[4] Zu Funktion und Aufgaben des Gremiums: Art. 29 f RL 95/46/EG; Art.15, RL 2002/58/EG.
[5] WP 242 vom 13.12.2016; aktualisierte Fassung vom 05.04.2017.
[6] Im Detail: siehe Stellungnahmen von Wirtschaft und Verbänden aus der vorliegenden Studie der Stiftung Datenschutz.

wortlichen erhalten können. Hier besteht grundsätzlich die Gefahr, dass Unternehmensgrundlagen, geistiges Eigentum und Geschäfts- oder Forschungsgeheimnisse durch das Recht auf Datenportabilität beeinträchtigt werden können.

Neben Empfehlungen der Artikel 29 Datenschutzgruppe und den Standpunkten verschiedener Branchenteilnehmer ist zu betrachten, inwieweit die Rechtswissenschaft und auch die Rechtsprechung hierzu bereits Kriterien entwickelt hat.
Der gegenwärtige Stand der Rechtswissenschaft grenzt den Begriff des Bereitstellens zentral danach ein, dass die betroffene Person die personenbezogenen Daten dem Verantwortlichen selbst, aktiv und durch eine wissentliche Handlung übermittelt, verbreitet oder sonst bereitstellt.[7] Klare und gegebenenfalls branchen- oder prozessspezifische Abgrenzungskriterien sind in weiten Teilen noch nicht postuliert.
Eine Auslegung des Begriffs „bereitstellen" hat nach dem gegenwärtigen Stand im Sinne eines Betroffenenrechts zur Kontrolle und Selbstbestimmung über die Daten zu erfolgen.
Für die Ausübung des Selbstbestimmungsrechts und zur Kontrolle der personenbezogenen Daten wird es sinnvoll sein, den Umfang der Datensätze überschaubar zu halten und auf wesentliche Punkte zu konzentrieren.
Auch eine Gegenüberstellung dieses Rechts mit der Gefahr, dass interne Prozesse und damit Unternehmensgrundlagen offengelegt werden, wird zu berücksichtigen sein.
Ob die Rechtsprechung und gegebenenfalls auch die Rechtsfortentwicklung hierzu konkretere Abgrenzungskriterien entwickeln wird, bleibt abzuwarten. Ein Bedarf besteht in jedem Falle dort, wo geschützte Rechte und Rechtspositionen anderer betroffen sind, hier insbesondere Positionen der Verantwortlichen für die Verarbeitung.[8]
Bis dahin sind die Kriterien des aktiven, wissentlichen Übermittelns an einen Verantwortlichen auf der Basis einer Einwilligung oder eines Vertrages ausschlaggebend.

Zusammenfassend ist aus den rechtlichen Betrachtungen zum Begriff des „Bereitstellens" festzuhalten, dass der Gesetzeswortlaut und dessen Auslegung einen verhältnismäßig weit ausgedehnten Rahmen bieten, um ein Betroffenenrecht möglichst breit aufzustellen. Auf der Basis einer Einwilligung oder durch ein Vertragsverhältnis ermöglicht die betroffene Person dem Verantwortlichen, personenbezogene Daten zu verarbeiten, insbesondere diese Daten zu erheben. Sofern bei dieser Erhebung moderne Informationstechnologien (Smart Services in jeder Form) eingesetzt werden, sind die darüber direkt zur Verfügung gestellten Informationen denklogisch auch als von der betroffenen Person bereitgestellt anzusehen. Stellt die betroffene Person personenbezogene Daten händisch oder über automatisierte Dienste direkt in ein System ein, sind diese Daten im Sinne der Vorschrift bereitgestellt. Solange die Rechtsprechung oder Gesetzgebung keine präzisierenden Grundsätze oder neue Vorgaben entwickelt, kann dieses Kriterium vom Verantwortlichen zur Abgrenzung herangezogen werden, um möglichst rechtssicher zu handeln.

In welcher Form sind die Daten zu exportieren

Die Form, wie die Daten zu exportieren sind, wird in Art. 20 Abs. 1 DSGVO als ein „strukturiertes, gängiges und maschinenlesbares Format" vorgegeben. In Erwägungsgrund 68 wird darüber hinaus das Merk-

[7] *Ehmann/Selmayr*, DSGVO Kommentar (2017), Art. 20 RN 13; *Piltz,* K & R 2016, 634; *Gola,* DSGVO Kommentar (2017), Art. 20, RN 13 f; *Kühling/Buchner,* DSGVO Kommentar (2017)
[8] Beispielsweise die Gefahr, dass unternehmerische Geheimnisse durch die Datenportabilität offenbart werden, oder andere Rechte, die einen Anspruch auf Datenübermittlung schaffen, z.B. im Rahmen der PSD2 Richtlinie.

mal „interoperabel“ postuliert. Nach Art. 20 Abs. 2 DSGVO besteht die Verpflichtung für den Verantwortlichen, die Daten an einen anderen Verantwortlichen zu übermitteln, nur dann, soweit dies technisch machbar ist.

Nach der Systematik der DSGVO werden mit den rechtlichen Anforderungen die Ziele der Regelung beziehungsweise die geforderte Funktionalität der Technik beschrieben. Der Einsatz eines bestimmten Formats oder eine Standardisierung sind gerade nicht verlangt. Damit ist die Frage nach der Form, in der die Daten zu exportieren sind, im Wesentlichen eine technische Frage und eine Frage zur Schaffung von Technologie oder IT-Systemen, die den rechtlichen Anforderungen genügen.

Die geforderten Voraussetzungen sind insoweit auch funktionsbeschreibend formuliert. Was genau mit *strukturiert, gängig, maschinenlesbar* und *interoperabel* gemeint ist, wird in der DSGVO nicht geregelt. Wobei die Anforderung *interoperabel* auch nicht in der Norm des Art. 20 genannt ist, sondern nur in Erwägungsgrund 68 gefordert wird.

Deutlich wird, dass die Wahl des Formats für den Verantwortlichen nicht beliebig ist. Mit den genannten Voraussetzungen werden technologieneutral Mindestanforderungen an das Format beschrieben. Die betroffene Person soll im Ergebnis die Möglichkeit haben, ihre Daten ohne größeren Aufwand zu erhalten oder an einen anderen Verantwortlichen zu übermitteln. Dabei soll ein unzumutbarer Aufwand für eine Umstrukturierung oder sonstige Veränderung an den Daten vermieden werden.[9] Im Ergebnis sind die Daten in einem Format bereitzustellen, das eine Weiterverwendung der Daten möglich macht.[10]

Die einzelnen Anforderungen lassen sich dabei wie folgt konkretisieren: Die „Gängigkeit“ des Formats erfordert es, dass sich der Verantwortliche an den Praktiken und Gegebenheiten des Marktes orientiert[11] und sich auch den technischen Entwicklungen anpassen muss. Das Format darf nicht besonders oder speziell oder außergewöhnlich sein, sondern es muss sich vielmehr um ein auf dem Markt bekanntes Format handeln.[12]
Die Daten selbst sind in einer gewissen Struktur anzuordnen. Die Art dieser „Strukturiertheit“ wird nicht weiter konkretisiert. Vielmehr ist sie im Zusammenhang mit den Anforderungen der „Maschinenlesbarkeit“ und „Interoperabilität“ in Beziehung zu setzen. Allgemein ist ein Format dann maschinenlesbar, wenn es mittels eines informationstechnischen Systems (also Computer und Software) erkannt und ausgelesen werden kann.[13] Interoperabilität kann vorwiegend als die Fähigkeit zur Interaktion von verschiedenen Systemen und Technologien betrachtet werden, mit dem Ziel, Daten auf effiziente und verwertbare Art und Weise auszutauschen.

In Erwägungsgrund 68 wird klarstellend ausgeführt: „Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten.“ Darin wird deutlich, dass interoperable Systeme, nicht kompatible Systeme, zu schaffen sind.

---

[9] *Kühling/Buchner*, DSGVO Kommentar (2017), Art. 20 RN 20
[10] So auch Art. 29 Datenschutzgruppe, WP 242, V.
[11] *Gola*, DSGVO Kommentar (2017), Art. 20 RN 21.
[12] Ebd.
[13] Ebd.; *Kühling/Buchner*; DSGVO Kommentar (2017), Art. 20 RN 20;
Nach Erwägungsgrund 21 der Richtlinie 2013/37/EU17 gilt ein Dokument als „maschinenlesbar“,
wenn es in einem Dateiformat vorliegt, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten, einschließlich einzelner Sachverhaltsdarstellungen und deren interner Struktur, einfach identifizieren, erkennen und extrahieren können. In Dateien verschlüsselte Daten, die in maschinenlesbarem Format strukturiert sind, sind maschinenlesbare Daten. Maschinenlesbare Formate können offen oder geschützt sein; sie können einem formellen Standard entsprechen oder nicht. Dokumente, die in einem Dateiformat verschlüsselt sind, das eine automatische Verarbeitung einschränkt, weil die Daten nicht oder nicht ohne Weiteres aus ihnen extrahiert werden können, sollten nicht als maschinenlesbar gelten.

Die gesetzlichen Vorgaben bieten breite Möglichkeiten für die Wahl des Formats an. Voraussichtlich werden je nach Branche und nach Art der Prozesse unterschiedliche Formate zum Einsatz kommen. Welche technischen Aspekte dabei zu bedenken sind, wird im folgenden Kapitel behandelt.

Das Recht auf eine direkte Übermittlung kann nur dann beansprucht werden, wenn dies technisch machbar ist. Die „technische Machbarkeit" stellt sich als unbestimmter Rechtsbegriff dar, für dessen Konkretisierung wiederum Erwägungsgrund 68 heranzuziehen ist. Wenn hiernach der Verantwortliche nicht verpflichtet ist, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten, richtet sich die technische Machbarkeit grundsätzlich nach den beim Verantwortlichen schon vorhandenen technischen Möglichkeiten.[14]
Das Recht auf Datenportabilität normiert aber auch, dass die betroffene Person die Übermittlung der Daten „ohne Behinderung durch den für die Verarbeitung Verantwortlichen" verlangen darf. Die Vorschrift bietet an dieser Stelle keine klare Linie und scheint ambivalent.
Die Bundesnetzagentur führt in einer Betrachtung dieser Thematik aus, dass die technische Realisierbarkeit nach objektiven Kriterien zu bestimmen ist und nicht nach den informationstechnischen Systemen der verantwortlichen Stelle. Was die „technische Machbarkeit" betrifft, die nach Art. 20 Abs. 2 DSGVO Voraussetzung für die direkte Übermittlung von Daten von einem Verantwortlichen zum anderen ist, sollten sich die Anforderungen am Stand der Technik orientieren.[15]
Ziel des Rechts auf Datenportabilität ist es, dass die betroffene Person effizient Kontrolle über ihre Daten ausüben kann. Dieses Recht wird ins Leere laufen, wenn ein Verantwortlicher die Übermittlung dadurch verhindern kann, dass er überholte und nicht mehr gängige Datenverarbeitungsanlagen vorhält. Eine Orientierung am Stand der Technik wird deshalb sinnvoll sein. Ob die Rechtsprechung hierzu anzuwendende Kriterien entwickelt, bleibt abzuwarten.

4 Lösungsansätze für die technische Realisierung der Datenportabilität

Die Herausforderungen des Rechts auf Datenportabilität bestehen:

- In rechtlicher Hinsicht im Festlegen, welche Daten zu exportieren sind (Personenbezug)
- In technischer Sicht, wo diese technisch abgelegt sind
- In der Form der Bereitstellung, Festlegung des Datenformats
- Im Mitteleinsatz - mit welchen Techniken sie zu exportieren sind
- In der Art der Bereitstellung — wie die Daten an den Empfänger übermittelt werden
- Umsetzung und Test

Welche Daten sind zu exportieren: Identifizierung der betreffenden Daten

Basierend auf den relevanten Geschäftsprozessen muss zunächst die rechtliche Identifikation der relevanten Daten nach den im vorigen Abschnitt entwickelten Kriterien erfolgen.

[14] *Kühling/Buchner*; DSGVO Kommentar (2017), Art. 20 RN 27.
[15] Stellungnahme der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen zum Grünbuch „Digitale Plattformen" des Bundesministeriums für Wirtschaft und Energie, S. 130.

Auf eine betroffene Person bezogen ist also zu identifizieren, welche Daten sich auf die betreffende Person und dritte Personen beziehen (relevant für Art. 20 Abs. 4 DSGVO), und auf welche Art und Weise diese Informationen erhoben sind (aktiv und wissentlich übermittelt, beobachtetes Verhalten, abgeleitete Informationen und Rückschlüsse).

Zur Hilfestellung bieten sich hier generell die Verzeichnisse von Verarbeitungstätigkeiten an. Nach Art. 30 DSGVO werden zahlreiche Verantwortliche verpflichtet sein, entsprechende Verzeichnisse zu führen, und müssen damit die einzelnen Verarbeitungstätigkeiten ohnehin verwalten.

Zur Identifikation der relevanten Daten müssen in einem ersten Schritt alle Prozesse bzw. Verfahren betrachtet werden, deren Grundlage für die Datenverarbeitung eine Einwilligung oder ein Vertragsverhältnis bildet.
Im zweiten Schritt sind alle personenbezogenen Daten zu identifizieren, die der Verantwortliche von der betroffenen Person übermittelt bekommen oder auf deren Weisung von einem Dritten erhalten hat. Diese erhobenen oder erfassten personenbezogenen Daten werden regelmäßig als bereitgestellt anzusehen sein. Generell ist es hierbei unerheblich, ob diese Daten per Hand eingegeben sind oder über einen automatisierten Dienst in ein System übertragen werden (Smart Services jeglicher Art).
Sobald personenbezogene Daten durch die betroffene Person selbst und durch ein aktives, wissentliches, ihr zurechenbares Handeln in das System des Verantwortlichen gelangt sind, sind diese Daten relevant für das Recht auf Datenportabilität. Je nach Besonderheit der einzelnen Verfahren und Prozesse beim Verantwortlichen können noch weitere Informationen als bereitgestellt anzusehen sein. Gegebenenfalls ist dies im Einzelfall gesondert zu prüfen oder eine Routine zu erarbeiten.

In einem dritten Schritt ist zu prüfen, an wen die identifizierten Daten übermittelt werden sollen. Ist eine Übermittlung an die betroffene Person selbst verlangt, sind alle identifizierten personenbezogenen Daten zu exportieren. Wird hingegen die Übermittlung an einen anderen Verantwortlichen erwirkt, ist in einem folgenden Schritt zu prüfen, ob in den Datensätzen auch personenbezogene Informationen über Dritte zu identifizieren sind. In diesem Fall sind an den anderen Verantwortlichen nur die Datensätze oder Daten zu übermitteln, in denen keine personenbezogenen Daten Dritter enthalten sind.

Diese Aufgabe ist in Zusammenarbeit von Business Process Owner, Wirtschaftsinformatikern und Juristen zu erbringen. Das Ergebnis muss eine inhaltliche Datenbeschreibung sein.

Wo sind die Daten technisch abgelegt

Die für die Exportierung in Frage kommenden Daten sind entsprechend der inhaltlichen Datenbeschreibung technisch zu lokalisieren — Datenbank, Tabelle, Feldname, valide Werte, Bezug zu anderen Feldern; aber auch Einbeziehung von Dokumentenablagen, ggf. Mailsystemen, Office-Dateien, Security-Systemen usw.

Eine technische Dokumentation ist zu erstellen, die den Entwicklern als Vorgabe für die Erstellung der Exportroutine dient. Dies kann grundsätzlich in Papierform erfolgen. Besser geeignet ist ein Verzeichnis in Form eines Repositorys. Mittels Software können so die jeweiligen Quellen angesprochen und es kann auf die relevanten Daten zugegriffen werden. Gleichzeitig ist damit eine technische Dokumentation erstellt, wodurch die fortlaufende Pflege bei Änderung qualitativ abgesichert und in einen geordneten Prozess eingebunden ist. Darauf zu achten ist, dass datenerzeugende/pflegende Programme im Repository z.B. beim Einfügen von Daten direkt entsprechende Tags (Kennzeichen) setzen müssen, damit diese in zukünftige Exporte einbezogen werden.

Das Verfahren ist aufwändig, sichert jedoch einen qualitativ hochwertigen Prozess ab.

In verschiedenen Dokumenten, die uns im Rahmen dieses Projektes zur Verfügung gestellt wurden, ist die Aussage zu lesen, dass die meisten Anbieter keine getrennten Datenbanken für die Rohdaten unterhalten, die *leicht (!) von den Algorithmen zur Kundenanalyse getrennt werden könnten*. Hierdurch würde Gefahr bestehen, dass mit einem Datentransfer zu einem anderen Anbieter in fast allen Fällen detaillierte Hintergrundinformationen über den technischen Aufbau, den verwendeten Algorithmen und damit Geschäftsgeheimnisse enthüllt würden.

Wir halten diese Gefahr für gering. Im Rahmen der Datendefinitionen (was ist zu exportieren) wird festgelegt, welche personenbezogenen Daten übertragen werden. Algorithmische Ergebnisse der Kundendaten werden zwar teilweise explizit gespeichert, sind aber in der Regel gängig, kryptisch und von der nach rechtlicher Definition zu exportierenden Datenmenge nicht betroffen. Darüber hinaus bestimmt der Anbieter mit dem Export den Datenumfang im Rahmen der rechtlichen Festlegungen.

Hier ist der Vollständigkeit halber nochmals darauf hinzuweisen, dass mit der Extrahierung ausdrücklich kein gleichzeitiger Grund besteht, die Daten zu löschen.

Form der Bereitstellung, Festlegung des Datenformats

Die Daten sind der betroffenen Person oder dem zukünftigen Verantwortlichen in einem geeigneten Format bereitzustellen.

Die rechtlichen Anforderungen an die Form bzw. das Format, in welches die Daten exportiert und im Sinne der betroffenen Person übermittelt werden sollen, geben einen relativ weiten Rahmen vor, wie geeignete Datenformate aussehen können. Es sind Kriterien herauszuarbeiten, welche technischen Formateigenschaften hier zweckmäßig sind und welche Anforderungen idealerweise zu berücksichtigen sind.

Die Zweckmäßigkeitsgesichtspunkte werden zentral bereits durch die Vorschrift des Art. 20 DSGVO vorgegeben. Weitere allgemein rechtliche und wirtschaftliche Zweckmäßigkeitsgesichtspunkte legen nahe, ein Format zu wählen, das eine Datenweitergabe auch branchenübergreifend ohne erheblichen Datenverlust ermöglicht, dessen Implementierungsaufwand gering ist, welches Verschlüsselungen nach dem Stand der Technik ermöglicht und revisionssicher ist.

Ein sektor- bzw. branchenübergreifender interoperabler Datenexport ist aus unserer Sicht nur theoretisch denkbar (z.B. können die Daten von einem Energieversorger an einen Social Media Dienst übermittelt werden). Die unterschiedlichen Datenstrukturen, die sich immer an den jeweiligen Geschäftsprozessen orientieren, können nur schwer in einer einheitlichen Lösung abgebildet werden.

Als am wahrscheinlichsten anzusehen, ist eine gewisse Standardisierung der Vorgehensweisen, technischen Formate und Verfahren.

<u>Architektur des Dateiformats</u>

Die Leitlinie der Art. 29 Datenschutzgruppe in der ursprünglichen Fassung, dass möglichst viele Metadaten unter dem bestmöglichen Granularitätslevel bereitzustellen sind, wurde in der korrigierten Fassung insoweit präzisiert, dass gängige und offene Formate zu verwenden sind, sofern in einer bestimmten Industrie oder einem Kontext kein Format gebräuchlich ist. Beispielhaft werden die Formate XML, JSON, CSV genannt.

Entscheidender als die Frage nach dem konkreten Format ist zunächst die Architektur bzw. allgemeine Eigenschaft eines „gängigen“ Formats.

Im Ergebnis sollten die Daten nach einem nachvollziehbaren Muster bzw. Bauplan in einer Datei angeordnet werden. Die Architektur muss Syntax und Semantik der Daten innerhalb der Datei abbilden. Während syntaktische Informationen festlegen, wie die Daten strukturiert und aufgebaut sind (Metadaten), werden die eigentlichen Inhalte auf der semantischen Ebene einheitlich festgelegt. Aus diesem Aufbau lässt sich ableiten, wie die Datei selbst (erkennen und behandeln) und auch wie die Daten in der Datei zu interpretieren sind; eine effiziente Maschinenlesbarkeit der enthaltenen personenbezogenen Daten ist so sichergestellt.[16] Auch eine funktionierende Interoperabilität ist hiermit realisierbar.

Geeignet kann hierbei beispielsweise der XML-basierte Standard für die Strukturierung von personenbezogenen Daten sein. Mit XML sind unterschiedliche Granularitätsstufen ohne weiteres möglich. Darüber hinaus sind die enthaltenen Informationen im XML-Schema nicht nur maschinenlesbar, sondern können über Standardsoftware von dem Betroffenen selbst gelesen werden. Diese Eigenschaft könnte neben dem Recht auf Datenübertragbarkeit auch die Wahrnehmung der Informationsrechte der betroffenen Person unterstützen.[17]

Die Mindestvoraussetzung für Datenportabilität bzw. Interoperabilität ist es, die Daten im einfachsten CSV-Format zu schreiben und eine einfache Beschreibung hinzuzufügen, wie die Daten in der Datei angeordnet sind. Zu beschreiben ist hierbei, an welcher Stelle in der Datei welche Dateninhalte zu finden sind (Name, Vorname, Geburtsdatum etc.) und was ggf. bestimmte Codierungen bedeuten.

Mitteleinsatz — mit welchen Techniken sie zu exportieren sind

Auf der Annahme beruhend, dass ein geeignetes Datenformat und die passenden Dateninhalte festgelegt sind, spielt es eine nachgeordnete Rolle, mit welchen Techniken die Dienstanbieter die Daten exportieren. Letztlich hängt es von den jeweils eingesetzten Ablagetechniken, zur Verfügung stehenden Ressourcen (Werkzeuge, Know-how, Zeit und Geld) des jeweiligen Unternehmens ab, was als Technik zum Einsatz kommt.

Denkbar sind individuell programmierte Export-Importroutinen, ETL-Tools, SQL-Abfragen, generische Standardexportroutinen der jeweiligen Anwendungssoftware usw.

Art der Bereitstellung — wie die Daten an den Empfänger übermittelt werden

Für die eigentliche Bereitstellung der extrahierten Daten gibt es unterschiedliche Varianten:

	Liefern	**Bereitstellen**
Betroffene Person	• Via Mail • Via Datenträger	• Download als Datei • Download aus einem Formular
Zukünftiger Dienstanbieter	• Via Datenträger	• Download als Datei

[16] So auch Stellungnahme *Drepper/Schlünder/Buckow*, Praktische Umsetzbarkeit der Datenportabilität im Bereich der medizinischen Forschung, Kap. VII. 2.
[17] Ebd.

	• Via Mail • Übertragen auf ein Ziel (z.B. FTP) • Aufruf eines Web-Service des zukünftigen Dienstanbieters (verbundene Systeme)	• Download aus einem Formular • Bereitstellung auf einem Server (z.B. FTP)

Gesetzlich gibt es hierzu keine verbindlichen Vorgaben.

Bei der Übertragung via Informationstechnologien (z.B. Internet) sind ausreichende Sicherheitsmaßnahmen, wie eine Ende-zu-Ende-Verschlüsselung der Daten während des Transports, nach dem Stand der Technik zu gewährleisten. Außerdem muss in jedem Fall die sichere Identifizierung und Authentifizierung des Betroffenen (LogIn-Verfahren, Double-Opt-In) sichergestellt sein.[18]

Die Notwendigkeit, die Daten zu verschlüsseln, ist unumgänglich und ein allgemeiner Grundsatz im Datenschutzrecht (u.a. Art. 5 Abs. 1 lit. f DSGVO). Davon ist auch die Integrität und Vertraulichkeit der Daten umfasst, die durch geeignete technische und organisatorische Maßnahmen abzusichern sind.

In diesem Sinne wird es sinnvoll sein, die betreffenden Daten auch revisionssicher oder signiert zu übermitteln. Dadurch kann im Zweifel nachgewiesen werden, dass der Verantwortliche richtige und unverfälschte Daten exportiert hat.
Allgemein besteht ansonsten die Gefahr der Manipulation von Daten im Rahmen der Übermittlung. Um sich hierbei haftungsrechtlich möglichst effektiv abzusichern, sind entsprechende Maßnahmen zu treffen.

Durchführung, Tests, Dokumentation

Abarbeitung/Realisierung der obigen Projektschritte – ohne weitere Ausführung an dieser Stelle.

5 Herausforderungen und Risiken

Die Herausforderungen der Umsetzung des Art. 20 Abs. 1, Datenportabilität, ist in der Praxis in noch relativ geringem Umfang angekommen. Nachfolgend beschreiben wir im Allgemeinen spezielle Herausforderungen und Risiken:

- Branchen/Marktsegmente
- Durchsetzbarkeit
- Industriestandards
- Notwendigkeit von Gremien

Branchen/Marktsegmente:

Branchenspezifische Prozesse erfordern spezifische Datenstrukturen und teilweise bei der Portierung von Personendaten nicht nur uni-, sondern bidirektionale Datenflüsse. Die Erarbeitung von derartigen

[18] So auch Artikel-29-WP 242 *Guidelines on the right to data portability. Adopted on 13 December 2016. As last Revised and adopted on 5 April 2017*. 2017. Article 29 Data Protection Working Party, WP 242, rev.01, http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (Abruf: 2017-07-31).

Datenaustauschverfahren sind aufwändig in der Erarbeitung, Entwicklung und Implementierung. Beispiele hierfür sind:

- Der medizinische Bereich (Krankenakten, Klinische Studien, Forschung, Abrechnung von Leistungen)
- Der Versicherungsbereich (Übertragung von Risikodeterminanten, Schadensverläufe etc.)
- Der Finanzbereich (Übertragung von Kontodaten, Depotdaten etc.)
- Der Energiebereich (Anbieterwechsel bei Strom und Gas)

Es wurden hier bereits die direkte Übertragung von prozessrelevanten Daten und damit auch personenbezogenen Daten umgesetzt. Die Spezifik der Anforderungen, die Notwendigkeit von umfangreichen technischen Entwicklungen und die Einigung/Standardisierung auf diesen Datenaustauch von allen relevanten Marktbeteiligten (z.B. Kliniken, Forschungseinrichtungen, Ärzte, MVZs, Krankenkassen etc.) erfordert Zeit, Aufwand, Kostenverteilung, Kostendeckung. Teilweise werden derartige Vorhaben durch staatliche Förderungen unterstützt (z.B. BMBF Förderung der Medizin-Informatik).

Für die Autoren ist es schwer vorstellbar, dass branchenübergreifende Standards zielführend sind, die Prozesse hinreichend bedienen können und dementsprechend auf Akzeptanz treffen. Lediglich die generelle Vorgehensweise kann von Bereich zu Bereich ggf. übertragen werden.

Durchsetzbarkeit

Die Durchsetzbarkeit der Datenportabilität hängt von mehreren Faktoren ab, darüber hinaus kann nur die Rechtsprechung in signifikanten Fällen für eine Durchsetzung sorgen (Urteile, Strafen, Sanktionen etc.). Folgende Faktoren sind vorrangig ausschlaggebend:

<u>Nutzen/Komfort</u>

Nur wenn Anbieter und Anwender überwiegend/mehrheitlich einen Nutzen darin sehen, Daten zu portieren, werden sich derartige Prozesse durchsetzen. Dabei spielen für den Anwender die Einfachheit der Anwendung und dass er beim neuen Anbieter weitgehend unterbrechungsfrei weiter bedient werden kann, eine große Rolle (die Frist von 3 Monaten ist zu lang). In diesem Sinne sollten die Daten auch auf einen wirklich notwendigen Umfang (Vertragserfüllung) beschränkt werden.

<u>Qualität</u>

Simpel ausgedrückt: Es muss funktionieren, darf nicht zu anschließenden Einbußen und Fehlern führen. Dies gilt auch für die Datenqualität als Teil der Qualitätsbetrachtungen. Angesichts unterschiedlicher Zeichensätze innerhalb des Geltungsbereichs der EU dürfte alleine hier eine ernstzunehmende Herausforderung bestehen.

<u>Kosten der Realisierung</u>

Sind die Umsetzungskosten für einen Anbieter höher als vermeintliche Strafen oder der Verlust eines Kunden in Einzelfällen, wird es nicht zu einer Umsetzung kommen; der Aufwand muss also verhältnismäßig sein. Hier sehen wir nicht nur die Kosten für den exportierenden Anbieter, der durch das Gesetz verpflichtet ist. In den Regelungen und entsprechenden Kommentaren fehlt die einlesende Seite. Werden Daten im Standardformat exportiert, aber nur wenige sind in der Lage, sie zu importieren, ist der Effekt nicht viel umfassender als bei der jetzt schon bestehenden Auskunftspflicht.

Abhilfe könnten hier einfache generische Standardfunktionen sein, die Systemanbieter/Web-Agenturen etc. in ihre Software integrieren können. An dieser Stelle besteht eine Marktchance für innovative Entwickler von Standards.

Industriestandards

In den Jahren hat sich eine Vielzahl von Industriestandards für den Datenaustausch entwickelt.

Einer der bekanntesten Vertreter für spezifischen Datenaustausch ist z.B. **EDIFact.** Über diese Standardkommunikation wird ein großer Teil des Datenaustausches in Industrie, Dienstleistung und Handel abgewickelt. Standardsysteme wie das ERP von SAP, aber auch weniger verbreitete kommerzielle Anwendungen verfügen über EDIFact-Schnittstellen für Export und Import.

Die Implementierung von neuen EDIFact-Schnittstellen erfordert relativ genaue Fachkenntnisse und auch einigen Aufwand. Lesbar im Sinne des Anwenders ist EDIFact kaum. Personenbezogene Daten werden z.B. im Rahmen des Wechsels von Energielieferanten mittels EDIFact ausgetauscht.[19]

Dasselbe gilt für **DATANORM**. Dieses Format wird zur Übermittlung von Artikelinformationen eingesetzt. DATANORM ist hoch generisch, entsprechend flexibel und mächtig. Aber auch hier gilt, dass dieser Standard für die breiten Anforderungen der Datenportabilität kaum geeignet ist.

In der Medizin-Informatik hat sich analog der Standard HL7 durchgesetzt. Aber auch für ihn gelten obige Limitationen im Sinne einer branchenübergreifenden Portabilität.

Die drei Beispiele zeigen, wie sich anwendungs- bzw. branchenspezifisch Austauschstandards entwickelt haben.

Von allgemeinerer Bedeutung ist der **XML**-Standard (Extensible Markup Language).

- Industriestandard mit hoher Verbreitung
- Nutzung durch viele IT-Lösungen, plattformübergreifend, flexibel und einfach erweiterbar
- Grundlage für moderne Übertragungstechniken wie Web-Services
- Schnelle Reaktion auf Gesetzesanforderungen möglich
- Standardisierung verhindert individueller Lösungen
- Auch tief verschachtelte Ebenen lassen sich relativ leicht lesen
- XSLT steht für die Transformation in verschiedene Formate zur Verfügung

XML hat den Vorteil, dass diese Technik sowohl Daten selbst als auch die Metadaten für die Beschreibung der Daten, für Plausibilitäten und Weiterverarbeitung mitliefern kann; auf diese Weise wird die Datenbeschreibung im Austauschformat direkt mitgeliefert.

Darüber hinaus können Daten im XML-Format einfach, z.B. mittels MS-EXCEL oder einem beliebigen Editor, einfach lesbar angezeigt werden.

XML eignet sich in Verbindung mit Web-Services hervorragend zur Kommunikation zwischen unterschiedlichen Systemen.

Natürlich befreit diese Technik nicht von der Festlegung, welche Daten überhaupt übertragen werden – dies gilt für alle Austauschformate.

[19] So *Gutmann,* Stellungnahme der Energiewirtschaft zur Datenportabilität.

In jüngerer Zeit kommt immer mehr **JSON** (JavaScript Object Notation) zum Einsatz. Es ist relativ einfach, für den Menschen lesbar:

- Einfache, minimalistische Syntax
- Geringes Datenvolumen
- Eignet sich besser für AJAX-Applikationen
- Unterstützung einer Vielzahl von Programmiersprachen
- Weniger geeignet für Dokumente und mediale Daten

Ein neuer technischer Trend ist die **Block Chain**. Die Autoren gehen hier nicht weiter darauf ein. Datenaustausch und die Abbildung von Prozessen ist relativ komplex und aufwändig. Dieses Verfahren, das im Augenblick erst mit seiner Verbreitung beginnt, ist aus unserer Sicht auf dem aktuellen Stand der Technik zu rechenleistungs- und ressourcenintensiv für einfache Anwendungen und ist somit eher branchenspezifischen Anwendungen (vorerst) vorbehalten.

Generell stellen sowohl XML als auch JSON offene Schnittstellentechniken dar, die die Anforderung an die Interoperabilität sicherstellen.

Notwendigkeit von Gremien

Um die Datenportabilität voranzutreiben, ist es sinnvoll, geeignete Gremien zu bilden. Die Gremien sind abzuleiten aus der Orientierung an Branchen (z.B. Automobil, Handel, Mittelstand). Die Besetzung sollte sich zusammensetzen aus Juristen, Wirtschaftsinformatikern und Prozessspezialisten des jeweiligen Umfeldes. Hilfreich könnte auch die Entwicklung von jeweiligen Codes of Conduct sein.

Resultierende Ergebnisse aus den einzelnen Gremien können dann nach und nach in branchenübergreifende Austauschformate überführt werden. In welchem Maße branchenübergreifende „Verschränkungen“ bestimmter Dienste in gemeinsamen Formaten sinnhaft ist, kann derzeit noch nicht abschließend beurteilt werden.
Ggf. werden hier auch neue Geschäftskonzepte entstehen, die diese Anforderung vorantreiben.

Besonders interessant erscheint uns die Bildung eines Mittelstandsgremiums, da hier unterschiedliche Branchen abgedeckt werden und vor allem auf die Anforderungen von KMU eingegangen werden muss. Sie haben deutlich weniger Mittel und müssen trotzdem denselben gesetzlichen Vorgaben entsprechen wie die „Großen“.

6 Zusammengefasste Anforderungen an die Lösung

Es sind aus unserer Sicht branchenorientierte Gremien zu bilden. Dort zu entwickelnde Codes of Conduct können den Rahmen für Projekte zur Realisierung eines Standards stellen. Realisierungsprojekte durchlaufen nach Zusammenstellung der Projektbeteiligten und Klärung der Kosten folgende Schritte:

- Festlegung der relevanten Daten aus Sicht des Datenschutzes (was sind die personenbezogenen Daten? – rechtliche Betrachtung)
- Festlegung der konkreten Struktur
- Fixierung des Austauschformats
- Festlegung des Mitteleinsatzes (Systeme)
- Festlegung des Datentransports
- Umsetzung und Test

Im Rahmen des Projektes entstehen in Zusammenarbeit von Juristen, Wirtschaftsinformatikern und Prozessspezialisten des jeweiligen Bereichs Formatvorschläge und entsprechende Dokumentationen sowie Einführungshinweise für die Anbieter der Branche.

Auf die Technik reduziert kann für einfache Lösungen auf CSV [20] zurückgegriffen werden. Für umfangreichere Lösungen bieten sich XML oder JSON an. Beide Standards erfüllen die Anforderungen an die Maschinenlesbarkeit sowie Interoperabilität. Sie enthalten die Daten sowie die beschreibenden Metadaten und haben aufgrund ihrer Struktur die entsprechende Tiefe, um auch komplexe Datengerüste abzubilden.

PDFs können zwar die grundsätzlichen Anforderungen an die Datenportabilität erfüllen, sind jedoch im Sinne einer automatisierten Verarbeitung beim neuen Anbieter als aufwändig einzustufen.

Technologien wie Block Chain oder Portale als Austauschdrehscheiben, z.B. auf Basis eines PIMS, sind in der Kürze der Zeit nicht etablierbar, jedoch für die Zukunft eine Alternative.

Branchenspezifische Umsetzungen können ggf. auf etablierte Industriestandards wie EDIFact zurückgreifen.

[20] So auch Stellungnahme *Drepper/Schlünder/Buckow*, Praktische Umsetzbarkeit der Datenportabilität im Bereich der medizinischen Forschung, Kap. VII. 2.

7 Management Summary

Rechtliche Grundlage für die Vorgabe der Datenportabilität ist die EU-weite Datenschutzgrundverordnung, gültig ab 25. Mai 2018. Danach erhalten betroffene Personen nach Art. 20 Abs. 1 DSGVO das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder diese Daten an einen anderen Verantwortlichen übermitteln zu lassen.

Der Gesetzgeber schreibt keine konkreteren Anforderungen an die technische Realisierung vor.

Angesichts der zahlreichen verschiedenen Branchen und den kaum überschaubaren einzelnen Akteuren ist nicht davon auszugehen, dass kurzfristig breit unterstützte und tatsächlich interoperable Formate im inhaltlichen Sinne und Standards allgemeingültig zur Verfügung stehen werden. Es wird branchengetriebenen Gremien, neuen Lösungsanbietern bzw. etablierten Systemanbietern obliegen, die Entwicklung voranzutreiben.

Wir sehen dies nicht als technisches Problem, sondern als Herausforderung an die Einigung auf übergreifende Standards, die in Gremien für einzelne Bereiche entwickelt werden müssen. In verschiedenen Branchen existieren bereits Umsetzungen (Energiewirtschaft, Versicherungen …).

Realisierungsprojekte, eben idealerweise getrieben durch branchenorientierte Gremien, umfassen folgende wesentlichen technischen Schritte:

- Festlegung der relevanten Daten aus Sicht des Datenschutzes (was sind die personenbezogenen Daten? – rechtliche Betrachtung)
- Festlegung der konkreten Struktur
- Fixierung des Austauschformats
- Festlegung des Mitteleinsatzes (System)
- Festlegung des Datentransports
- Umsetzung und Test

Prädestinierte Formate sind XML und JSON in Abhängigkeit verfügbaren Ressourcen bzw. zu übertragenden Daten. Mit beiden sind unterschiedliche Granularitätsstufen möglich. Die enthaltenen Informationen sind nicht nur maschinenlesbar, sondern können über Standardsoftware von dem Betroffenen selbst gelesen werden. Diese Eigenschaft könnte neben dem Recht auf Datenübertragbarkeit auch die Wahrnehmung der Informationsrechte der betroffenen Person unterstützen.[21]

Die Mindestvoraussetzung für Datenportabilität bzw. Interoperabilität ist es, die Daten im einfachsten CSV-Format zu schreiben und eine einfache Beschreibung hinzuzufügen, wie die Daten in der Datei angeordnet sind.

Projektteams sollten sich aus Juristen, Wirtschaftsinformatikern und Prozessspezialisten der jeweiligen Anwendungsbereiche zusammensetzen (Business Process Owner).

8 Impressum

Projektleitung
Karl Schmid (karl.schmid@scrc-leipzig.de)
Phone: +49 (0) 172 7200 895

Fachliche Leitung
Dr. Gunnar Hempel (gunnar.hempel@scrc-leipzig.de)
Phone: +49 (0) 176 8062 9804

Social CRM Research Center
c/o Prof. Dr. Rainer Alt
Institut für Wirtschaftsinformatik
Universität Leipzig
Grimmaische Str. 12
04109 Leipzig

www.scrc-leipzig.de
facebook.com/SCRCLEIPZIG

Phone: +49 (0) 341 97 33600
Fax: +49 (0) 341 97 33 612
E-Mail: info@scrc-leipzig.de
Web: http://www.scrc-leipzig.de

Amtsgericht Leipzig, VR 5657
Vertreten durch den Vorstand: Rainer Alt, Karl Schmid, Olaf Reinhold
Steuernummer: 231/141/11813
Bankverbindung: Leipziger Volksbank eG
IBAN: DE41 860 956 04 03 07 20 64 98
BIC: GENODEF1LVB

III. Rechtliche Analyse zum Anwendungsbereich – Prof. Dr. Anne Riechert

1. Welche Daten sind vom Recht auf Datenübertragbarkeit umfasst?

Das Recht auf Datenübertragbarkeit ist in Artikel 20 Datenschutzgrundverordnung nicht derart konkret formuliert, dass aus dem Wortlaut klare Voraussetzungen hergeleitet werden könnten. Zudem müssen im Hinblick auf eine einheitliche Rechtsanwendung und europaweite Harmonisierung eventuelle Unterschiede in den Übersetzungen und im Wortsinn der einzelnen Mitgliedstaaten berücksichtigt und verglichen werden.[1] Es wird außerdem darauf verwiesen, dass zukünftig nach wie vor strittig bleiben wird, ob der Personenbezug relativ oder absolut zu bestimmen ist.[2]

Insgesamt ist gemäß Artikel 20 Datenschutzgrundverordnung erforderlich, dass die personenbezogenen Daten entweder auf Grund einer informierten Einwilligung des Betroffenen oder auf der Grundlage eines Vertrags verarbeitet werden und vom Betroffenen bereitgestellt wurden. In der Literatur wird angemerkt, dass in der Praxis oftmals der Verarbeitungsgrund nicht so klar sei und es sich in zahlreichen Fällen um vermischte Datensätze handele, die etwa auf Einwilligungen oder berechtigten Interessen basierten.[3] Da der Verantwortliche die Rechtmäßigkeit der Verarbeitung gemäß Artikel 5 Absatz 2 Datenschutzgrundverordnung jedoch nachweisen und unter den Voraussetzungen des Artikel 30 Absatz 5 Datenschutzgrundverordnung ein Verzeichnis der Verarbeitungstätigkeiten anlegen muss, sollte daher stets die Verarbeitungsgrundlage klar bzw. die Rechtsgrundlage in diesen Fällen gut dokumentiert sein.

1.1. Bereitgestellte Daten

(1) Vertragsdaten und/oder Nutzungsdaten der betroffenen Person

Die Artikel-29-Datenschutzgruppe hat in ihren Stellungnahmen vom 13.12.2016 und 05.04.2017 das wesentliche aber mangels Legaldefinition umstrittene Merkmal des Bereitstellens von Daten („the personal data concerning him or her, which he or she has provided to a controller“) weit ausgelegt.[4] Damit ist sie vielfach auf Kritik gestoßen, da ebenso die so genannten „observed data“ gemeint sind, also die Daten, die aufgrund der Inanspruchnahme eines Dienstes erzeugt werden, z.B. Nutzungsdaten, die Suchhistorie des Betroffenen oder Daten, die durch einen Fitness-Tracker aufgenommen worden sind. [5] Diese Meinung wird unter anderem mit dem Argument abgelehnt, dass die meisten Anbieter keine getrennten Datenbänke für die Rohdaten unterhielten, die leicht von den Algorithmen zur Kundenanalyse getrennt werden könnten.[6] Daher besteht von Unternehmensseite oftmals die Anforderung, Nutzungsdaten vom Anwendungsbereich der Regelung

[1] Strubel, ZD 8/2017, S. 358.
[2] Strubel, ZD 8/2017, S. 357.
[3] Siehe Moos, Datenportabilität: Eine Gefahr für datengetriebene Unternehmen?, März 2016, der darauf hinweist, dass es im Unternehmen ein durchaus übliches Szenario sei, dass die Verarbeitung personenbezogener Daten zugleich auf mehrere Rechtsgrundlagen gestützt werde.
[4] Artikel-29-Datenschutzgruppe, WP 242 Guidelines on the right to data portability vom 13.12.2016 und Artikel-29-Datenschutzgruppe, WP 242 Guidelines on the right to data portability vom 05.04.2017
[5] Artikel-29-Datenschutzgruppe, WP 242, S. 5; Benedikt, RDV 2017, S. 190; Jüllicher/Röttgen/v.Schönfeld, ZD 2016, S. 359, die ein aktives Tun als Voraussetzung ablehnen.
[6] Siehe Stellungnahme Deutsche Telekom AG. Dies würde dazu führen, dass bei einem Datentransfer zu einem anderen Anbieter detaillierte Hintergrundinformationen über den technischen Aufbau und der verwendeten Algorithmen verbunden seien und damit das Geschäftsmodell enthüllt sei, besonders in Bezug auf geistiges Eigentum und Geschäftsgeheimnisse, siehe hierzu: BitKom, Stellungnahme Datenportabilität, S. 8 und Stellungnahme Deutsche Telekom AG.

auszuschließen (ebenso Telekommunikations-/Verkehrsdaten sowie Standortdaten) und sich streng am Wortlaut zu orientieren.[7] Damit wären lediglich Daten erfasst, die die betroffene Person aktiv und bewusst zur Verfügung stellt, z.B. beim Ausfüllen eines Online-Anmeldeformulars, und die von ihr kontrolliert werden.[8]

Weitgehend Einigkeit besteht hingegen darüber, dass keine Daten erfasst sein sollen, die der Verantwortliche erst auf Grund der bereitgestellten Daten selbst ausgewertet und erzeugt hat („inferred data"), z.B. im Rahmen der Profilbildung und Scorewerte.[9]

Grundsätzlich muss also entschieden werden, ob ausschließlich Daten erfasst sein sollen, die zur Erfüllung eines Vertrages erforderlich sind und die die betroffene Person im Rahmen einer Direkterhebung bereitgestellt hat oder ob außerdem Nutzungsdaten unter den Anwendungsbereich fallen.[10] Darüber hinaus wird vorgeschlagen, das Merkmal des Bereitstellens service-spezifisch auszulegen und damit den Anspruch lediglich auf die Daten anzuwenden, die für die Nutzung eines vergleichbaren Dienstes relevant sind.[11]

(2) Schutzzweck des Gesetzes

Ursprünglich war das Recht auf Datenübertragbarkeit gemäß Erwägungsgrund 55 des Entwurfs einer Datenschutzgrundverordnung (2012)[12] als Verbesserung des Auskunftsrechts ausgestaltet und die betroffene Person hatte bei einer elektronischen Verarbeitung einen Anspruch darauf, die Daten, die Gegenstand einer Auskunft waren, als Kopie in einem gängigen elektronischen Format erhalten. Bei einer automatisierten Anwendung sollte die betroffene Person außerdem die Möglichkeit haben, die von ihr durch ausdrückliche Einwilligung oder im Zuge der Erfüllung eines Vertrages zur Verfügung gestellten Daten auf eine andere Anwendung zu übertragen. Korrespondierend dazu regelte Artikel 18 Absatz 1 des Entwurfs einer Datenschutzgrundverordnung (2012) den Anspruch auf Kopie „aller" (die Person betreffende) Daten und Absatz 2 den Anspruch auf Übertragung der vertragsrelevanten Daten bzw. der Daten, die mit Einwilligung der betroffenen Person zur Verfügung gestellt wurden. Bei der Datenübertragung auf eine andere Anwendung wurde der Fokus außerdem auf soziale Netzwerke gelegt.[13]

---

[7] Siehe BitKom, Stellungnahme Datenportabilität (Stellungnahme zum Recht auf Datenübertragbarkeit nach Art. 20 Datenschutzgrundverordnung) vom 14.03.2017, S. 7 sowie Stellungnahme Deutsche Telekom AG (Statement on the Guidelines on the right to data portability oft he Article 29 Data Protection Working Party).
[8] Siehe Strubel, ZD 8/2017, S. 357/358, der darlegt, dass ein „Geschehenlassen" nicht ausreichen soll und mit Bereitstellen die Direkterhebung gemeint sei. Siehe auch Stellungnahme Deutsche Telekom AG, die das Merkmal auf „nützliche" und vom Nutzer kontrollierte Daten begrenzt.
[9] Artikel-29-Datenschutzgruppe, WP 242, S.10.
[10] Im Gegensatz dazu gibt es sogar einzelne Meinungen, die aufgrund des zugrundeliegenden monetären Werts gleichermaßen nicht-personenbezogene Daten in den Anwendungsbereich einbeziehen möchten: Siehe Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries.
[11] Siehe Strubel, ZD 8/2017, S. 360, der danach trennt, ob die Daten notwendig sind, um einen vergleichbaren Service anzubieten zu können: Damit sollten bei einer Jogging-App sowohl die vom Nutzer eingegeben Daten wie Name, E-Mail, Gewicht erfasst sein, aber ebenso die aufgezeichneten Laufstrecken und Pulswerte, da diese Daten der Serviceerbringung immanent seien. Allerdings sollten davon keine werberelevanten Nutzungsdaten erfasst sein, wenn der Betroffene sich beispielsweise für eine in der App angezeigte Werbung interessiert habe.
[12] Siehe Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.01.2012, KOM(2012) 11 endgültig.
[13] Siehe hierzu die Nachweise unter Fußnote 64.

Hier ist zum einen zu beachten, dass auch die Übertragung ein Recht auf eine Kopie beinhaltet. Diese Kopie erfolgt allerdings direkt in ein anderes automatisiertes Verarbeitungssystem sowie in einem Format, welches die weitere Verwendung der Daten erlaubt. Zum anderen handelt es sich, sofern die Verarbeitung der personenbezogenen Daten auf einem Vertrag basiert (siehe Wortlaut des Artikel 18 Absatz 2 der ursprünglichen Fassung), um Daten, die für die Vertragserfüllung erforderlich sind, und damit nicht um Nutzungsdaten. Die betroffene Person ist aber dadurch nicht schlechter gestellt, da sie diese Daten auch nach derzeitiger Gesetzeslage im Wege ihres Auskunftsrechts erfragen kann und ihr diesbezüglich ein Anspruch auf Erhalt einer elektronischen Kopie zusteht.

Aus Artikel 18 Absatz 3 der ursprünglichen Fassung (2012) wird zudem deutlich, dass die Formate des Absatzes 1 und Absatzes 2 durchaus unterschiedlich sein können. Folgerichtig ist in Artikel 15 Absatz 3 Datenschutzgrundverordnung nunmehr auch ein gängiges, elektronisches Format verlangt und in Artikel 20 Datenschutzgrundverordnung ein maschinenlesbares Format.

Der Unterschied besteht also darin, dass die betroffene Person die Möglichkeit hat, Auskunft über „alle“ verarbeiteten Daten in einem elektronischen Format zu erhalten, während die weitere Verwendbarkeit der von ihr zur Verfügung oder bereitgestellten Daten in einem maschinenlesbaren Format erfolgen muss (siehe nun: Artikel 15 Absatz 3 und Artikel 20 Absatz 1 und Absatz 2 Datenschutzgrundverordnung). Ein gängiges elektronisches Format könnte auch eine E-Mail und ein pdf darstellen. Die Datenportabilität möchte jedoch eine weitere Erleichterung schaffen, nämlich die einfach auszuführende Weiterübertragung und Weiterverwendung der von der betroffenen Person bereitgestellten Daten in einem anderen System. Dazu ist die Maschinenlesbarkeit erforderlich.[14]

Insgesamt ist daher fraglich, ob im Laufe des Gesetzgebungs- und Verhandlungsprozesses tatsächlich eine Ausweitung dieser ursprünglichen Regelung angedacht war, wie sie nun -wie oben dargestellt- durch die Artikel-29-Datenschutzgruppe vorgenommen wurde. Daher gilt es zu entscheiden, ob die Intention des Entwurfs der Datenschutzgrundverordnung 2012 und der Schutzzweck tatsächlich geändert werden sollte oder ob die Umstellung der Formulierungen allein den langwierigen Verhandlungen geschuldet ist. So ist etwa auch zu berücksichtigen, dass das Recht auf den Erhalt einer Kopie zunächst im Rahmen der Datenportabilität in Artikel 18 Absatz 1 (2012) geregelt war und im Laufe der Verhandlungen als Regelung des Auskunftsanspruches in Artikel 15 Absatz 3 Datenschutzgrundverordnung verankert wurde.

1.2 Telekommunikationsdaten

Verkehrsdaten und Standortdaten werden nicht explizit vom Anwendungsbereich ausgenommen. Der Verband BitKom verweist aber darauf, dass auch Verkehrsdaten nicht erfasst sein dürfen, u.a. aus dem Grunde, da zum einen Schutzrechte von Dritten betroffen seien und zum anderen die Verkehrsdaten bei einem Kommunikationsvorgang stets und ohne Zutun der Betroffenen anfallen und damit nicht für die Vertragserfüllung erforderlich seien. [15]

[14] Siehe hierzu unter Punkt 2. Format. Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereit gestellt wurden, zu übermitteln, sofern die Verarbeitung auf einer Einwilligung beruht.

[15] Bitkom, Stellungnahme Datenportabilität, S. 10 mit dem Verweis unter anderem darauf, dass Verkehrs-und Standortdaten als Folge standardisierter Protokolle anfallen und nicht am Willen der Beteiligten hängen, sondern vom Kommunikationsvorgang initiiert werden.

Allerdings ist hier der Entwurf der E-Privacy-Verordnung zu beachten. [16] Dort wird der Begriff der Kommunikationsmetadaten unter Artikel 4 Absatz 3 c) definiert. Danach sind „elektronische Kommunikationsmetadaten“ Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden. Gemäß Artikel 6 Absatz 2c) der E-Privacy-Verordnung ist es möglich, dass solche Daten mit einer Einwilligung der Betroffenen verarbeitet werden, die den Vorgaben der Datenschutzgrundverordnung entsprechen muss. Erfolgt also eine Verarbeitung solcher Metadaten (Verkehrs- und Standortdaten) aufgrund einer Einwilligung der betroffenen Person, wäre vom Wortlaut des Artikels 20 Datenschutzgrundverordnung ein Anspruch auf Übertragung dieser Daten zu einem anderen Dienstleister umfasst.[17]

Hier sollte dennoch mit Blick auf die Vorratsdatenspeicherung berücksichtigt werden, dass in der Vergangenheit die Bundesnetzagentur sogar ein Auskunftsrecht gemäß § 34 BDSG aufgrund der möglichen Beeinträchtigung Dritter abgelehnt hat.[18] So werden Verkehrsdaten in Bezug auf einen bestimmten Anschluss gespeichert und berühren damit die Interessen des Anschlussinhabers sowie die Interessen von Mitbenutzern oder des Kommunikationspartners. Diese Wertung sollte ebenso bei der Datenportabilität gemäß Artikel 20 Datenschutzgrundverordnung beachtet werden.

Fraglich ist allenfalls, ob es praktikabel wäre, eine Bestätigung der betroffenen Person zu verlangen, dass keine Rechte Dritter betroffen sind. Der Anschlussinhaber ist für den Datenschutz der Mitbenutzer verantwortlich. Infolgedessen könnte ebenso eine entsprechende Bestätigung eingeholt werden, dass Mitbenutzer entweder ihre Einwilligung erteilt haben oder keine Mitbenutzer vorhanden sind.

1.3. Daten Dritter

Die Übertragung von Daten ist darüber hinaus daran zu messen, ob Rechte Dritter im Sinne von Artikel 20 Absatz 4 Datenschutzgrundverordnung betroffen sind. Ergänzend ist anzumerken, dass bereits die Übertragung zu einem anderen „ungewollten“ Anbieter einen Eingriff in das informationelle Selbstbestimmungsrecht des Dritten darstellen kann, auch wenn die Speicherung zu

[16] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017 (E-Privacy-Verordnung). Gemäß Artikel 95 der Datenschutzgrundverordnung werden natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen. Die E-Privacy-Verordnung ist die Nachfolgeregelung und präzisiert und ergänzt durch die Festlegung besonderer Vorschriften die Datenschutzgrundverordnung.

[17] Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung auf einer Einwilligung beruht.

[18] Das Auskunftsrecht besteht gemäß § 34 Abs. 4 i.V.m. § 33 Abs. 2 Satz 1 Nr. 3 BDSG nicht, wenn die Daten nach einer Rechtsvorschrift oder wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen.

privaten Zwecken erfolgt.[19] Die Datenschutzgrundverordnung beansprucht zwar unter natürlichen Personen „zu ausschließlich persönlichen oder familiären Zwecken“ keine Geltung. Dennoch ist zu beachten, ob Daten bei einem kommerziellen Anbieter gespeichert werden, den sich die betroffenen Dritten nicht bewusst und eigenständig ausgesucht haben. So ist es in der digitalisierten Welt etwas völlig anderes, beispielsweise Bilder und Daten von Dritter in seinem eigenen privaten Archiv zu speichern, als diese einem kommerziellen Anbieter mit Gewinnerzielungsabsicht zu übermitteln. Insbesondere ist zu berücksichtigen, dass gemäß der Datenschutzgrundverordnung sämtliche Verarbeitungstatbestände gleichberechtigt nebeneinanderstehen und sich diesbezüglich noch keine europaweit einheitliche Rechtsauffassung im Hinblick auf die Rechtmäßigkeit der Verarbeitung aufgrund berechtigter Interessen gemäß Artikel 6 Absatz 1f Datenschutzgrundverordnung oder einer möglichen Zweckänderung gemäß Artikel 6 Absatz 4 Datenschutzgrundverordnung herausbilden konnte. Die (jeweils) betroffene Person darf somit insgesamt nicht den Überblick über mögliche Verarbeitungstatbestände, Verantwortliche und ihr zustehende Löschungsansprüche verlieren.

Es wäre zum jetzigen Zeitpunkt demzufolge verfrüht, dem neuen Verantwortlichen die verantwortungsbewusste Löschung und Nichtnutzung von Daten Dritter zu übertragen, wie es die Artikel-29-Datenschutzgruppe fordert.[20] Diese Auffassung, dass auch Daten Dritter grundsätzlich übermittelt, aber nicht für eigene Zwecke der neuen Datenverantwortlichen genutzt werden dürfen, zieht nicht in Betracht, dass bereits in der Übertragung der Daten ein Verstoß gegen das informationelle Selbstbestimmungsrecht liegen kann.[21] Möglich wäre etwa, dass sich der Dritte bewusst gegen einen kommerziellen Anbieter entschieden hat. Der Vorschlag der Einführung von Tools, mit denen die betroffenen Personen Daten auswählen und ausschließen können[22], ist an dieser Stelle nur ausreichend, wenn die Drittbetroffenen damit zuvor ihr Einverständnis erklären können, dass ihre Daten zu einem weiteren kommerziellen Anbieter übertragen werden.[23] Dann müsste jedoch eine entsprechende Verpflichtung im Hinblick auf die Einführung solcher Tools etabliert werden und die Transparenz sichergestellt sein.

Etwas anderes könnte insgesamt gelten, wenn der Nutzer beispielsweise seine Kontaktliste oder facebook-Account auf sein eigenes, privates Gerät kopieren möchte,[24] da es sich in diesem Falle tatsächlich um eine „ausschließlich“ private Verarbeitung handelt.

1.4. Arbeitnehmerdaten

Gemäß Wortlaut des Artikel 20 Datenschutzgrundverordnung sind Arbeitnehmerdaten vom Recht auf Datenübertragbarkeit erfasst, die Anwendbarkeit der Regelung ist dennoch im Einzelnen strittig.

---

[19] Ansprüche können sich nach deutschem Recht aus §§ 1004, 823 BGB ergeben, wobei ein Schadensersatzanspruch wegen Verletzung des allgemeinen Persönlichkeitsrechts gemäß der Rechtsprechung nur bei schwerwiegenden Persönlichkeitsrechtsverletzungen in Betracht kommt.

[20] Dies bezieht sich auch auf Metadaten, die ggf. personenbezogene Daten von Dritten enthalten können (siehe hierzu die Ausführungen unter Punkt 2).

[21] Artikel-29-Datenschutzgruppe, WP 242, S. 11.

[22] Artikel-29-Datenschutzgruppe, WP 242, S. 12.

[23] In diesem Zusammenhang wird außerdem angemerkt, dass ein wirtschaftlich unverhältnismäßiger Aufwand entstünde, wenn die Betreiber Sozialer Netzwerke den Drittbezug manuell aussortieren müssten. Daher müssten entsprechende Algorithmen entwickelt werden. Siehe hierzu die Ausführungen von Jüllicher/Röttgen/v.Schönfeld, ZD 2016, S. 362, die gleichzeitig aber auch als „Gefahr“ ansehen, wenn nur Bestandsdaten übertragen werden sollten.

[24] Siehe etwa die Dienste „DigiMe“ oder „MyData“ (behandelt in der Studie der Stiftung Datenschutz zum Thema „Einwilligung und Transparenz“).

Während teilweise auf die Relevanz beim Arbeitgeberwechsel verwiesen wird, beziehen sich andere Auffassungen auf den ohnehin engen Anwendungsbereich für die Verarbeitungen aufgrund einer Einwilligung im Arbeitsverhältnis.[25] Die Artikel-29-Datenschutzgruppe regt für Arbeitnehmerdaten eine auf den Einzelfall bezogene Prüfung an.[26]

2. In welchem Format müssen die Daten übertragen werden?

Unklar ist außerdem, in welchem Format die Daten zukünftig übertragen werden sollen. Die Datenschutzgrundverordnung enthält keine Definition und die Artikel-29-Datenschutzgruppe verweist in ihrer Stellungnahme lediglich auf die notwendige Interoperabilität[27], ohne ein konkretes Format vorzugeben. Insgesamt wird betont, dass ein solches zukünftig entwickelt werden müsse und es wird zur Zusammenarbeit von Wirtschaftsunternehmen und Industrie aufgefordert.[28]

Hierbei ist strittig, ob ein Format gewählt werden sollte, welches Metadaten beibehält, [29] oder dies den Interessen des Datenschutzes gerade zuwiderläuft. [30] Die Artikel-29-Datenschutzgruppe führt aus, dass mit den personenbezogenen Daten möglichst viele Metadaten bereitgestellt werden sollten. [31] Dies deutet darauf hin, dass eine Unterscheidung seitens der Artikel-29-Datenschutzgruppe zwischen personenbezogenen Daten und Metadaten vorgenommen wird, was jedoch nicht näher konkretisiert wird. Eine gesetzliche Definition für Metadaten findet sich bislang im Entwurf der E-Privacy-Verordnung, welche personenbezogene Daten umfasst.[32] So sind gemäß Artikel 4 Absatz 3 c) des Entwurfs der E-Privacy-Verordnung „elektronische Kommunikationsmetadaten“ Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden,[33] also auch Verkehrs- und

[25] Hennemann, Ping 01.17, S. 5; BitKom, Stellungnahme Datenportabilität, S. 8.
[26] Artikel-29-Datenschutzgruppe, WP 242, S. 8/9.
[27] Artikel-29-Datenschutzgruppe, WP 242, S. 5, 16 ff.
[28] Artikel-29-Datenschutzgruppe, WP 242, S. 18. Siehe außerdem Schätzle, Ping 02.16, S. 74/75; Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries, wobei diese Autoren in ihrer Stellungnahme die allgemeinen Bedingungen für ein entsprechendes Datenübertragungsformat anhand von unterschiedlichen Szenarien beschreiben und in der Übertragbarkeit an sich keine technische Hürde sehen. Siehe auch Hennemann, Ping 01.17, S. 8, der darauf hinweist, dass die Interoperabilität von Artikel 20 Datenschutzgrundverordnung gerade nicht gefordert wird. Diese Voraussetzung ist lediglich in Erwägungsgrund 68 der Datenschutzgrundverordnung enthalten.
[29] Siehe Artikel-29-Datenschutzgruppe, WP 242, S.18, die Metadaten auf bester Granularitätsstufe vorschlägt und der Auffassung ist, dass ein Format gewählt werden sollte, welches sämtliche Metadaten beibehält, die für eine effektive erneute Verwendung der Daten relevant sind; Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries.
[30] Siehe Stellungnahme Deutsche Telekom AG, in der darauf verwiesen wird, dass die Übersendung eines vollständigen Datensatzes mit der anschließenden Prüfung, ob tatsächlich alle Daten benötigt werden, aus Sicht des Datenschutzes sehr beunruhigend sei.
[31] Artikel-29-Datenschutzgruppe, WP 242, S. 18.
[32] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017
[33] Siehe die Begriffsdefinition von Metadaten der elektronischen Kommunikation auf S. 13 sowie unter Artikel 4 Absatz 3 c) der Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-Verordnung). Hierzu zählen beispielsweise angerufene Nummern, besuchte Websites, der geografische Standort, Uhrzeit, Datum und Dauer eines von einer Person getätigten Anrufs gehören, aus denen sich präzise Schlussfolgerungen über das Privatleben der an der elektronischen Kommunikation beteiligten Personen ziehen lassen könnten, z. B. in Bezug auf ihre sozialen Beziehungen, Gewohnheiten und ihren Lebensalltag, ihre Interessen, ihren Geschmack

Standortdaten. Letztere werden jedoch von der Artikel-29-Datenschutzgruppe als „von der betroffenen Person bereitgestellte personenbezogene Daten“ eingeordnet, was wiederum -wie oben ausgeführt- von Unternehmensseite vollständig abgelehnt wird.[34] Aus technischer Sicht werden ebenfalls genügend Metadaten gefordert,[35] aber diese sind nicht unbedingt personenbezogen auszulegen. So können Metadaten zwar unter anderem ein Dokument genauer beschreiben und diese Beschreibung kann aus personenbezogenen Daten bestehen (z.B. Vorname und Name des Autors eines pdf-Dokuments). Aber Metadaten können gleichermaßen ein Attribut näher konkretisieren und beispielsweise Beschränkungen festlegen (z.B. das Attribut „Name“ darf nicht mehr als 100 Zeichen haben).[36]

Zu berücksichtigen ist bei der Suche nach einem geeigneten Format gleichermaßen die Forderung der Artikel-29-Datenschutzgruppe, E-Mail-Daten in einem Format bereitzustellen, in dem möglichst viele Metadaten beibehalten werden, um eine effektive Wiederverwendung der Daten zu ermöglichen, so dass die Bereitstellung von PDF-Versionen nicht ausreichend sei.[37] Dieses Beispiel ist aber vorrangig keine Frage der Anzahl der Metadaten, sondern eine Frage der Maschinenlesbarkeit, da ein pdf-Dokument aus Sicht der Informatik eher den Begriff der „Menschenlesbarkeit“ verdient. Bei einem maschinenlesbaren Format dagegen geht es vorrangig um die automatisierte Auslesbarkeit und Verarbeitbarkeit durch Software.[38]

Daher sollte eine begriffliche Abgrenzung und Definition vorgenommen und aus technischer Sicht die Frage beantwortet werden, ob es immer erforderlich ist, möglichst viele (auch personenbezogene) Metadaten zu übertragen, oder ob es andere definierbare Voraussetzungen im Hinblick auf ein Format gibt, welche eine sinnvolle Weiterverwendung der personenbezogenen Daten sicherstellen. Insbesondere sollte geprüft werden, inwieweit ein bestimmtes, maschinenlesbares Format die Übertragung von Metadaten „auf bester Granularitätsstufe“ obsolet machen könnte.[39] So könnte etwa ein pdf-Dokument zwar die Einordnung als gängiges, elektronisches Format zur Sicherstellung des Auskunftsrechts verdienen, aber könnte als maschinenlesbares Format bzw. als Format, mit dem die betroffene Person die Daten sinnvoll weiterverwenden kann, ausdrücklich ausgeschlossen werden.

Insgesamt ist daher zu prüfen, ob zwecks Bildung eines einheitlichen technischen und juristischen Verständnisses ein übereinstimmendes Verständnis zum Begriff der Metadaten sowie hinsichtlich eines maschinenlesbaren Formats besteht und inwieweit dieses bei der Entwicklung eines Standardformats zur Datenübertragung relevant ist.[40] Dies gilt auch, um entscheiden zu können, welche Metadaten aus technischer Sicht für eine erfolgreiche Umsetzung der Datenportabilität erforderlich und aus rechtlicher Sicht zulässig sind.

3. Welche Erwägungen sind bei der Interoperabilität des Formats zu beachten?

[34] Siehe Fußnote 15.
[35] Siehe Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries.
[36] Siehe Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries.
[37] Artikel-29-Datenschutzgruppe, WP 242, S. 18.
[38] Siehe zur Maschinenlesbarkeit auch BeckOK DatenSR/von Lewinski DS-GVO Art. 20 Rn. 74-75.
[39] Die Artikel-29-Datenschutzgruppe schließt ein pdf-Dokument bei einem E-Mail-Postfach zwar als Format aus, aber nicht generell. Ergänzend ist anzumerken, dass bei Zugrundlegung der weiten Auslegung der Artikel-29-Datenschutzgruppe, möglichst viele Metadaten zu übertragen, fraglich ist, inwiefern hier ebenso Daten Dritter betroffen sind (siehe Punkt 1.3).
[40] Siehe auch die Beschreibung von unterschiedlichen Szenarien im Rahmen der Datenübertragung bei Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries.

Festzuhalten ist zunächst, dass die Interoperabilität nicht im Gesetzestext selbst, sondern im Erwägungsgrund 68 erwähnt wird. Insgesamt ist außerdem die Uneinigkeit über Sinn und Zweck des Artikels 20 Datenschutzgrundverordnung zu beachten. Einerseits soll die Regelung das informationelle Selbstbestimmungsrecht stärken. Dennoch wird sie einschränkend dahin ausgelegt, dass (nur) die Datenübertragung von einem Dienstleister zum anderen erleichtert und Lock-In-Effekte vermieden werden sollen.[41]

Der Arbeit der wissenschaftlichen Dienste des Bundestags ist jedoch in diesem Zusammenhang zu entnehmen,[42] dass bei den so genannten OTT-I-Dienste ohnehin kein Lock-In-Effekt eintreten würde,[43] da die Nutzer diese Dienste regelmäßig parallel im so genannten Multi-Homing nutzten und von einem Dienst zum anderen flexibel sowie ohne Kosten wechseln könnten. [44] In Bezug auf Inhalte des E-Mailverkehrs sowie Adressbücher könnten die Nutzer eine lokale Kopie der Daten außerdem leicht selbst erstellen.[45] Weiter führen die wissenschaftlichen Dienste aus, dass die Interoperabilität zwar dazu beitragen könne, die Monopolbildung, namentlich bei marktbeherrschenden Unternehmen, zu vermeiden und so den Wettbewerb zu fördern.[46] Allerdings seien gerade die OTT-I-Dienste oftmals neue Produkte, die sich durch Produktdifferenzierung auszeichnen, so dass eine regulatorisch erzwungene Zusammenschaltung auch wettbewerbsdämpfend und einen erheblichen Eingriff in die unternehmerische Freiheit darstellen könne, der einer fundierten Begründung im Einzelfall bedarf.[47]

Weiterhin geht es bei der Interoperabilität ebenso um die „technische Machbarkeit“, die sowohl subjektiv als auch objektiv ausgelegt werden kann.[48] Eine objektive Auslegung könnte kleine und mittelständische Unternehmen belasten, sofern die individuelle Leistungsfähigkeit keine Rolle spielt. Daher könnte bei einer subjektiven Auslegung die Anregung, dass die Unternehmen ihre verwendeten Formate für den Import veröffentlichen sollten, dazu beitragen, die Datenübertragung in der Praxis zu unterstützen und zu erleichtern.[49]

Aus den gerade gemachten Ausführungen folgt, dass bei Bewertung der Interoperabilität aus wettbewerbsrechtlicher Sicht demnach der jeweilige Dienst entscheidend sowie ein

---

[41] Siehe hierzu Hennemann, Ping 01.17, S. 6 mit Verweis auf Erwägungsgrund 68 der Datenschutzgrundverordnung.
[42] Arbeit der wissenschaftliche Dienste des Bundestages zum Thema „Regulierung von Messengerdiensten, Datenportabilität und Interoperabilität“ ; Aktenzeichen: WD 10 – 3000 – 060/16; Fachbereich: WD 10 : Kultur, Medien und Sport.
[43] Arbeit der wissenschaftliche Dienste des Bundestages zum Thema „Regulierung von Messengerdiensten, Datenportabilität und Interoperabilität“ , S. 6 ff: OTT-I-Dienste werden als Dienste definiert, denen kein inhaltliches Angebot zugrunde liegt, sondern die Individual- oder Gruppenkommunikation unter Einsatz des IP-Protokolls (Internet-Protokolls) ermöglichen. Hierunter fallen damit auch Messengerdienste wie WhatsApp.
[44] Arbeit der wissenschaftliche Dienste des Bundestages zum Thema „Regulierung von Messengerdiensten, Datenportabilität und Interoperabilität“, S. 13.
[45] Arbeit der wissenschaftliche Dienste des Bundestages zum Thema „Regulierung von Messengerdiensten, Datenportabilität und Interoperabilität“, S. 13.
[46] Arbeit der wissenschaftliche Dienste des Bundestages zum Thema „Regulierung von Messengerdiensten, Datenportabilität und Interoperabilität“, S. 18.
[47] Arbeit der wissenschaftliche Dienste des Bundestages zum Thema „Regulierung von Messengerdiensten, Datenportabilität und Interoperabilität“, S. 18, auch unter Verweis auf die Auffassung des Bundeskartellamts. Siehe außerdem Hennemann, Ping 01.17, S.6, der auf den wettbewerblichen Ansatz sowie auf das Gesetzgebungsverfahren hinweist, in welchem angeregt wurde, dieses Recht nicht im Zuge der Verordnung zu regeln.
[48] Hennemann, Ping 01.17, S. 8.
[49] Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries.

Wettbewerbsnachteil kleiner und mittelständischer Unternehmen zu berücksichtigen ist. Dies hat ebenso Auswirkung auf die Frage, ob die gemäß Verordnung geforderte „technische Machbarkeit“ objektiv oder subjektiv zu bewerten ist. Außerdem muss aus wettbewerbsrechtlicher bzw. kartellrechtlicher Sicht im Einzelfall unterschieden werden, bei welchen Diensten tatsächlich Lock-In-Effekte eintreten.

Im Hinblick auf das Wettbewerbsrecht im engeren Sinne kann die Möglichkeit nicht außer Acht gelassen werden, dass die Verletzung einer Marktverhaltensregel zu Abmahnungen durch Mitbewerber und Verbraucherzentralen führen kann (UWG). Außerdem sollte ergänzend geklärt werden, ob es ebenso eine wettbewerbsrechtliche Relevanz haben könnte, wenn der neue Datenverantwortliche sich weigert, die Daten zu importieren.

4. Relevanz des Wettbewerbsrechts für die datenschutzrechtliche Bewertung?

Wettbewerbsrecht (Gesetz gegen den unlauteren Wettbewerb - UWG) und Datenschutzrecht (Bundesdatenschutzgesetz - BDSG) stehen gleichberechtigt nebeneinander. So sind beide Gesetze etwa bei Werbemaßnahmen zu beachten. Dies gilt auch zukünftig im Hinblick auf die Datenschutzgrundverordnung, wobei darüber hinaus die europarechtliche Harmonisierung zu berücksichtigen ist.

In der deutschen Rechtsprechung ist umstritten, inwieweit datenschutzrechtliche Regelungen gleichzeitig Marktverhaltensregeln im Sinne des UWG darstellen.[50] Grundsätzlich könnte bei Nichteinhaltung der Interoperabilität und in der fehlenden Bereitstellung einer mühelosen Übertragungsmöglichkeit der Daten ein Verstoß gegen § 3a UWG[51] (Rechtsbruch) und § 4 Nr. 4 UWG[52] (gezielte Behinderung der Mitbewerber) in Betracht kommen.

Das OLG Hamburg wertet etwa einen Verstoß gegen die datenschutzrechtlichen Informationspflichten des § 13 TMG als Wettbewerbsverstoß.[53] Das OLG Hamburg beruft sich in seiner Argumentation auf die Erwägungsgründe der Datenschutzrichtlinie 96/46/EG, in denen gleichermaßen auf den europäischen Wettbewerb sowie das notwendige einheitliche Schutzniveau für das Funktionieren von Wirtschaftstätigkeiten auf Gemeinschaftsebene Bezug genommen

[50] Verneinend etwa OLG München, Urteil vom 12. Januar 2012, Az. 29 U 3926/11:
Das Datenschutzrecht sei Ausfluss des Persönlichkeitsrechts und schütze ganz allgemein diese Individualrechtsposition und es gehe dabei nicht konkret um den Schutz in der Rolle als Marktteilnehmer. Die Bestimmungen des Bundesdatenschutzgesetzes stellten ungeachtet dessen, dass sich ihre Verletzung im Geschäftsleben durchaus auswirken kann, grundsätzlich keine Marktverhaltensregelungen dar (unter Verweis auf die Ausnahme des § 28 Absatz 4 Satz 2 BDSG). Siehe außerdem OLG Köln, Urteil vom 19. November 2010, Az. 6 U 73/10; Kammergericht Berlin, Beschluss vom 29. April 2011, Az. 5 W 88/11; OLG Stuttgart, Urteil vom 22. Juli 2007, Az. 2 U 132/06. Andererseits OLG Karlsruhe, Urteil vom 09. Mai 2011, Az. 6 U 38/11, welches §§ 4, 28 BDSG als Marktverhaltensregeln einstufen, soweit sie die Datenverarbeitung für Werbezwecke regeln.
[51] § 3a UWG regelt den Rechtsbruch. Danach handelt unlauter, wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln, und der Verstoß geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen.
[52] § 4 UWG regelt den Mitbewerberschutz. Danach handelt unlauter, wer Mitbewerber gezielt behindert.
[53] OLG Hamburg, Urteil vom 27. Juni 2013 · Az. 3 U 26/12 mit dem Argument, dass es sich bei § 13 TMG (Informationspflichten) um eine im Sinne des § 4 Nr. 11 UWG das Marktverhalten regelnde Norm handele (nun § 3a UWG) und nicht nur als eine Missachtung einer allein überindividuelle Belange des freien Wettbewerbs regelnden Vorschrift. Ebenso OLG Köln, Urteil vom 11.März 2016, Az. 6 U 121/15.

werde.[54] Die Vorschrift diene daher auch dem Schutz der Interessen der Mitbewerber und sei damit eine Regelung, die dazu bestimmt ist, das Marktverhalten im Interesse der Marktteilnehmer zu regeln.

Unter diesen Gesichtspunkten könnten ebenfalls die Regelungen der Datenschutzgrundverordnung Marktverhaltensregeln beinhalten, da deren Erwägungsgründe ähnliche wettbewerbsbezogene Aspekte beinhalten.[55]
Im Sinne einer solchen Auslegung würde ein Verstoß gegen Artikel 20 Datenschutzgrundverordnung zugleich ein unlauteres Verhalten darstellen, welches geeignet ist, die Interessen von Verbrauchern und Mitbewerbern spürbar zu beeinträchtigen. Unter Berücksichtigung der unter Punkt 1.3 dargestellten wettbewerbsrechtlichen Erwägungen ist allerdings fraglich, ob es interessensgerecht ist, stets ein objektiv rechtswidriges (wettbewerbswidriges) Verhalten zu unterstellen, sofern Unternehmen, unter Zugrundelegung der Auslegungskriterien der Artikel-29-Datenschutzgruppe, keine Lösungen zur „pauschalen" Datenportabilität bereitstellen. Diese Frage stellt sich auch unter der Annahme, dass Artikel 20 Datenschutzgrundverordnung systemfremd als wettbewerbsrechtliche Regelung in der Datenschutzgrundverordnung verankert ist.[56]

Im Hinblick auf die wettbewerbsrechtliche Bewertung der oben erwähnten „gezielten Behinderung" hat der Bundesgerichtshof etwa entschieden, dass eine Beeinträchtigung im Allgemeinen dann unlauter sei, wenn gezielt der Zweck verfolgt werde, Mitbewerber an ihrer Entfaltung zu hindern und sie dadurch zu verdrängen, *oder* wenn die Behinderung dazu führt, dass die beeinträchtigten Mitbewerber ihre Leistung am Markt durch eigene Anstrengung nicht mehr in angemessener Weise zur Geltung bringen können.[57] Ob diese Voraussetzungen erfüllt sind, lasse sich nur aufgrund einer Gesamtwürdigung der Umstände des Einzelfalls unter Berücksichtigung der Interessen der Mitbewerber, Verbraucher und sonstiger Marktteilnehmer sowie der Allgemeinheit beurteilen,[58]

---

[54] Das OLG Hamburg ist der Auffassung, dass durch die Schaffung gleicher Wettbewerbsbedingungen auch die wettbewerbliche Entfaltung des Mitbewerbers geschützt werden soll Das OLG Hamburg führt weiter hierzu aus, dass diese Vorschrift u.a. Art. 10 der Datenschutzrichtlinie 95/46/EG umsetze, die nicht nur datenbezogene Grundrechte gewährleisten (Erwägungsgrund 1), sondern auch den grenzüberschreitenden Verkehr personenbezogener Daten auf ein einheitliches Schutzniveau heben solle (Erwägungsgründe 6 und 7), weil ein unterschiedliches Schutzniveau ein Hemmnis für die Ausübung von Wirtschaftstätigkeiten auf Gemeinschaftsebene darstelle und den Wettbewerb verfälschen könne (Erwägungsgrund 7 Satz 2). Die Regelungen der Richtlinie dienten deshalb auch der Beseitigung solcher Hemmnisse, um einen grenzüberschreitenden Fluss personenbezogener Daten kohärent in allen Mitgliedsstaaten und in Übereinstimmung mit dem Ziel des Binnenmarktes zu regeln (Erwägungsgrund 8).
[55] Siehe Erwägungsgründe 2, 9, 10, 13 der Datenschutzgrundverordnung: So etwa Erwägungsgrund 2 (*Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen*) und Erwägungsgrund 9 (*…Unterschiede beim Schutzniveau für die Rechte und Freiheiten von natürlichen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, können den unionsweiten freien Verkehr solcher Daten behindern. Diese Unterschiede im Schutzniveau können daher ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern.*).
[56] Siehe Hennemann, Ping 01.17, S.6, der auf den wettbewerblichen Ansatz sowie auf das Gesetzgebungsverfahren hinweist, in welchem angeregt wurde, dieses Recht nicht im Zuge der Verordnung zu regeln.
[57] BGH, Urteil vom 22. Januar 2014 – I ZR 164/12.
[58] BGH, Urteil vom 22. Januar 2014 – I ZR 164/12 sowie BGH, Urteil vom 24. Juni 2004 – I ZR 26/02: Die Frage, ob in einem beanstandeten Wettbewerbsverhalten eine unzulässige allgemeine Marktbehinderung zu sehen

wobei keine Behinderungsabsicht erforderlich sei.[59] Dabei sei auch den kollidierenden Grundrechtspositionen Rechnung zu tragen.[60] Weiterhin muss das Vorliegen eines konkreten Wettbewerbsverhältnisses berücksichtigt werden. Dieses liege immer dann vor, wenn beide Parteien gleichartige Waren oder gewerbliche Leistungen innerhalb desselben Endverbraucherkreises abzusetzen versuchen und das Wettbewerbsverhalten des einen daher den anderen beeinträchtigen, d.h. im Absatz behindern oder stören kann.[61] Es müsse aber keine Branchengleichheit vorliegen. [62]

Mit dieser wettbewerbsrechtlichen Sichtweise ist damit unter anderem die Frage nach der Gleichartigkeit der Leistungen verbunden sowie eine Gesamtwürdigung aller Umstände unter Abwägung der Interessen der Mitbewerber, der Verbraucher und der Allgemeinheit relevant. Fraglich ist, ob ein ähnlicher Bewertungsmaßstab bei der Auslegung von Artikel 20 Datenschutzgrundverordnung und Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Datenschutzgrundverordnung mit einfließen könnte. Denn durch eine fehlende „Datenübertragungsmöglichkeit mit einem Klick“ könnten auch Mitbewerber in der Ausgestaltung ihrer Geschäftsmodelle behindert werden.[63] Zu berücksichtigen ist in diesem Kontext besonders, dass die Idee der Datenübertragbarkeit ihren Ursprung gerade in wettbewerblichen Erwägungen hatte und auf soziale Medien fokussiert war.[64] So hatte der europäische Gesetzgeber ursprünglich geplant, die Monopolstellung von sozialen Netzwerken durch Netzwerkeffekte aufzuweichen und den Wechsel zu datenschutzfreundlichen Technologien zu ermöglichen.[65] Damit entsprechen die ursprüngliche Gesetzesintention sowie der Schutzzweck von Artikel 20 Datenschutzgrundverordnung, den Anbieterwechsel zu erleichtern, dem wettbewerbsrechtlichen Merkmal der Vergleichbarkeit der Dienstleistungen.

Erörterungswürdig ist demzufolge, ob entweder eine einheitliche Sichtweise von Wettbewerbsrecht und des Datenschutzrecht möglich wäre und welche Kriterien hierfür gelten müssten oder inwieweit beide Rechtsgebiete weiterhin getrennt und unabhängig voneinander beurteilt werden müssen.[66]

Für ein differenziertes Ergebnis könnten insgesamt Bedingungen formuliert werden. So wäre etwa in einer Gesamtabwägung der Interessen der Betroffenen eine Prüfung dahingehend möglich,

---

ist, könne nur aufgrund einer Gesamtwürdigung aller Umstände des jeweiligen Einzelfalls unter Abwägung der Interessen der Mitbewerber und der Allgemeinheit beurteilt werden. Siehe hierzu auch BGH, Urteil vom 7. Oktober 2009 - I ZR 150/07.

[59] Siehe BGH, Urteil vom 11. Januar 2007 – I ZR 96/04; BGH, Urteil vom 19. Februar 2009 – I ZR 135/06; BGH, Urteil vom 22. Januar 2014 – I ZR 164/12.

[60] BGH, Urteil vom 24. Juni 2004 – I ZR 26/02.

[61] BGH, Urteil vom 24. Juni 2004 – I ZR 26/02.

[62] BGH, Urteil vom 24. Juni 2004 – I ZR 26/02.

[63] Insbesondere ist keine Behinderungsabsicht verlangt, siehe oben Fußnote 59.

[64] Jüllicher/Röttgen/v.Schönfeld, ZD 2016, S.360/362; Hennemann, Ping 01.17., S. 6; Strubel, ZD 8/2017, S. 359 mit dem Hinweis, dass ursprünglich angedacht war, das Recht auf Datenübertragbarkeit auf die Angebote Sozialer Medien zu begrenzen; Schätzle, Ping 02.16, S. 74 mit dem Hinweis auf die Kritik, dass es bei dem Recht auf Datenübertragbarkeit nicht um den Schutz der Privatsphäre gehe, sondern es sich vielmehr um ein wettbewerbspolitisches Instrument handele.

[65] Hennemann, Ping 01.17., S. 6 mit Verweis auf den wettbewerblichen Ansatz sowie auf die Aussage von Jan Albrecht (Berichterstatter des Europäischen Parlaments zur Datenschutzgrundverordnung), der in Artikel 20 einen Katalysator eines Wettbewerbs um datenschutzfreundliche Technologien sieht.

[66] Ergänzend ist zu wiederholen, dass bei Einordnung von Artikel 20 Datenschutzgrundverordnung als eine Marktverhaltensregel, dennoch ein abmahnfähiges unlauteres Verhalten vorliegen würde, siehe hierzu oben S. 10. Dies bedeutet, dass in diesem Zusammenhang eine unmittelbare wettbewerbsrechtliche Konsequenz vorliegen würde.

inwieweit nach Datenarten unterschieden werden könnte. So könnte bei der eingangs dargestellten Streitfrage, ob sowohl Vertragsdaten als auch Nutzungsdaten vom Anwendungsbereich umfasst sind, bei der Bewertung mit einfließen, ob es im Hinblick auf *sämtliche* Nutzungsdaten immer einen Mehrwert für die informationelle Selbstbestimmung darstellt, diese nicht nur in einem elektronischen Format gemäß Artikel 15 Absatz Datenschutzgrundverordnung, sondern ebenso in maschinenlesbarer Form gemäß Artikel 20 Datenschutzgrundverordnung zu erhalten. Zu berücksichtigen ist, dass Nutzungsdaten verstärkt den neuen Anbieter interessieren, für den diese ein wertvolles Gut darstellen. Die informationelle Selbstbestimmung in ihrem Kern wird aber eher dadurch gestärkt, sofern auf einfache Art und Weise Auskunftsrechte und im Anschluss entsprechende Löschungsrechte geltend gemacht werden können. Sowohl bei der informationellen Selbstbestimmung nach Artikel 1 Absatz 1, Artikel 2 Absatz 1 als auch nach Artikel 8 Grundrechte-Charta geht es um den Schutz der personenbezogenen Daten. Ein direkter Übertragungs- und Verwertungsanspruch von *sämtlichen* Nutzungsdaten zur Verbesserung der Schutz- und Kontrollrechte der Betroffenen könnte gelten, wenn zum jetzigen Zeitpunkt bereits der Wert der Daten bekannt wäre und ein florierender Datenhandel durch die Betroffenen forciert werden soll. Die Nutzer wissen jedoch nicht, ob sie bereits durch ihr Nutzungsverhalten Millionäre sind. Hier spielt außerdem eine Rolle, inwieweit Artikel 20 Datenschutzgrundverordnung einen wirtschaftlichen Vorteil des informationellen Selbstbestimmungsrechts umfassen und diesen schützen soll.[67] Somit stellt sich die zusätzliche Frage nach der Kommerzialisierung von Daten und ob den betroffenen Personen eine wirtschaftliche Verwertungsbefugnis zusteht,[68] aber gleichwohl, ob sie diese überhaupt selbstbestimmt ausüben können, wenn der Wert der Daten nicht bezifferbar ist. Der Nutzer müsste also ab Mai 2018 wissender und kompetenter Verhandlungspartner sein, dem der Wert seiner Daten bewusst und bekannt ist, insbesondere seiner gesamten Nutzungsdaten.

Der weitere wesentliche Aspekt bezieht sich daher auf die Verbesserung der Betroffenenrechte sowie der Erleichterung einer Datenübertragung. Im Hinblick auf die Interoperabilität des Formats ist demzufolge die Frage zu stellen, ob es einen Vorteil für die Betroffenen darstellt, wenn eine branchenübergreifende Portabilität sowie direkte Übertragbarkeit und „Datenkopie“ zwischen den Verantwortlichen ausnahmslos gelten würde. Die Einbeziehung des Merkmals „Branche“ könnte hier im Gegensatz zum Wettbewerbsrecht bei der Bewertung der Betroffenenrechte eine Rolle spielen. Mit Verweis auf die ursprüngliche Intention der Europäischen Kommission, dass der Umzug eines Online-Profils von einem sozialen Netzwerk zu einem anderen mit einem einzigen Klick möglich sein sollte, wird in diesem Zusammenhang das Beispiel einer Datenübermittlung zwischen einem

[67] Auf die klärungsbedürftige Frage nach dem Dateneigentum verweisen unter anderem Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries.

[68] Siehe etwa Lindhorst, Sanktionsdefizite im Datenschutzrecht (2009), S. 66 ff. zur informationellen Selbstbestimmung als Vermögensrecht; Unseld, Die Kommerzialisierung personenbezogener Daten (2010), S. 14 mit der Anmerkung, dass nur die zugrundeliegenden Datenträger kommerzialisiert werden, nicht aber die Person. Bezüglich dieser Daten (und Datenträger) müssten Rechte eingeräumt werden. Siehe auch Klüber, Persönlichkeitsschutz und Kommerzialisierung: die juristisch-ökonomischen Grundlagen des Schutzes der vermögenswerten Bestandteile des allgemeinen Persönlichkeitsrechts (2007), S. 82: Es werde erst im Rahmen einer rechtlichen Wertung entschieden, ob die Persönlichkeitsdetails der Allgemeinheit zugewiesen sind und damit öffentliche Güter darstellen oder ob der der Einzelne ein uneingeschränktes Verwertungsrecht an der eigenen Persönlichkeit hat. Weiter weist Klüber (aaO) auf die Rechtsprechung hin, nach welcher die vermögensrechtliche Seite des allgemeinen Persönlichkeitsrechts zwar anerkannt werde, ein kommerzieller Zuweisungsgehalt aber davon abhänge, dass zum einen die Erlaubnis zur Verwertung üblicherweise nur gegen Zahlung eines Entgelts erfolge und zum anderen die betroffene Person auch nutzungsbereit gewesen sei.

Fitnessportal und einer Krankenversicherung genannt.[69] Würde es tatsächlich eine Verbesserung der Kontrolle und des Auskunftsrechts der Betroffenen darstellen, wenn unter Zugrundelegung der Definition der Artikel-29-Datenschutzgruppe sowohl Vertrags- als auch *sämtliche* Nutzungsdaten vom Fitnessportal zu einer Krankenversicherung übertragen werden müssten und sogar umgekehrt? Oder haben dadurch eher die Verantwortlichen einen Mehrwert? Insbesondere kann, wie oben unter Punkt 1.3. dargestellt, Berücksichtigung finden, dass noch keine einheitliche, europaweit geltende Rechtsauslegung zu den Regelungen des Artikel 6 Absatz 1f Datenschutzgrundverordnung (berechtigte Interessen) sowie der Möglichkeit einer Zweckänderung (§ 6 Absatz 4 Datenschutzgrundverordnung) besteht. Es würde unter Umständen eine große Datenmenge zu einem weiteren Verantwortlichen übertragen werden, die dieser eigenverantwortlich rechtlich bewerten könnte. In diesem Falle könnte im Übrigen und im Hinblick auf die Kommerzialisierung personenbezogener Daten in die Überlegung einbezogen werden, ob die weitere Verarbeitung „gewinnbringend" seitens des neuen Verantwortlichen auf berechtigte Interessen gestützt werden kann.[70] Außerdem stellt in diesem Zusammenhang die Sicherstellung von ausreichender Transparenz eine weitere wesentliche Anforderung dar, da der betroffenen Person alle Informationen, die sich auf die Verarbeitung durch den alten und neuen Verantwortlichen beziehen, bekannt sein müssen.

Im Sinne des informationellen Selbstbestimmungsrechts könnte ein interessengerechtes Ergebnis gegebenenfalls dadurch erreicht werden, sofern bei der Einstufung von Daten als vertragsrelevante Daten gemäß Artikel 20 Absatz 1a) i.V.m. Artikel 6 Absatz 1b Datenschutzgrundverordnung im jeweiligen Einzelfall bzw. im Hinblick auf den zugrundeliegenden Dienst der Servicegedanke mit einfließt. So könnten beispielsweise die Aufzeichnung der Werte einer Fitness-App, nicht als „observed data", sondern als „zur Vertragserfüllung erforderlich" und damit (im Gegensatz zu *sämtlichen* durch die Inanspruchnahme des Dienstes erzeugten Nutzungsdaten) als sinnvolles Kundeninteresse bei der Datenportierung gewertet werden.[71] Es sollte daher im Einzelfall entschieden werden können, unter welchen Umständen die direkte Übertragung von „welchen" Nutzungsdaten („observed data") zu einem anderen Dienstleister tatsächlich zur Verbesserung der Kontrollrechte der betroffenen Person beiträgt.

Dementsprechend wäre eine einzelfallbezogene bzw. dienstespezifische Betrachtungsweise denkbar, wobei auf der Basis der oben getätigten Ausführungen die nachfolgenden Fragestellungen und Wertungen mit einbezogen werden könnten. So könnte geprüft werden, welche Daten „mit einem Klick" und „zwischen" welchen Diensten übertragen werden müssen, da ansonsten ein Eingriff in das informationelle Selbstbestimmungsrecht vorliegt .[72] Die Frage ist demzufolge auch, welchen

[69] Siehe Jüllicher/Röttgen/v.Schönfeld, ZD 2016, S. 360.

[70] Fraglich ist: Ist das Recht auf informationelle Selbstbestimmung der betroffenen Personen im Einzelfall besser gewährleistet, wenn das Kontrollrecht bei sämtlichen Nutzungsdaten durch Übersendung einer elektronischen Kopie erfolgt, aber nicht, wenn Unternehmen animiert werden, Geschäftsmodelle zu entwickeln, ohne dass zum jetzigen Zeitpunkt der Wert der Daten vollumfänglich klar wäre? Auch hier spielt daher erneut die Frage nach der wirtschaftlichen Verwertungsbefugnis, aber auch der individuellen Verwertungskompetenz, eine wichtige Rolle.

[71] Siehe hierzu auch Taeger in: Taeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, § 28 BDSG Rn. 53, der darauf verweist, dass in bestimmten Vertragskonstellationen, bei denen der Servicegedanke eine außerordentlich große Rolle spielt, auch das Anlegen eines Kundenprofils als zur Vertragserfüllung erforderlich ableiten ließe. Siehe außerdem Strubel, Fußnote 11.

[72] Hier könnte auch entschieden werden, inwieweit bei einzelnen Diensten ein Wettbewerbsnachteil kleiner Unternehmen oder ein fehlender Lock-In-Effekt relevant ist. Auch wenn letzteres die damit zusammenhängende Monopolstellung und damit den Wettbewerb im weiteren Sinne, die kartellrechtliche Komponente, betrifft.

Datenportabilitätsansprüchen der Betroffenen ein „tatsächlicher“ Anbieterwechsel im Sinne eines Wechsels zu einem vergleichbaren Dienstleistungsangebot zugrunde liegt, der entweder eine Übertragung der Vertragsdaten und sämtlicher Nutzungsdaten oder nur eines beschränkten Satzes an Nutzungsdaten erforderlich macht. Bei einem solchen Anbieterwechsel könnte gegebenenfalls auch ein Wettbewerbsnachteil kleiner Unternehmen vorliegen oder ein Netzwerkeffekt fehlen, so dass die Interoperabilität und die technische Machbarkeit ebenfalls in den Fokus geraten.
Ist das Rechtsbegehren dagegen auf eine Kopie der Daten in ein anderes System gerichtet, ohne dass die Ursprungsdaten beim Verantwortlichen gelöscht werden, kann es sich beispielsweise um die Übertragung von Vertrags- und Nutzungsdaten zur Bereitstellung einer weiteren Dienstleistung durch einen anderen Anbieter handeln. Hier müssen einerseits die bereits oben aufgeworfenen Problemstellungen im Hinblick auf die Kommerzialisierung personenbezogener Daten und wirtschaftlicher Verwertungskompetenz im Rahmen des informationellen Selbstbestimmungsrechts erörtert werden. Andererseits könnte relevant sein, ob ein Anspruch der Allgemeinheit oder des anderen Dienstleisters auf „pauschale“ Datenübertragung und Bereitstellung einer „Datenkopie mit einem Klick“ besteht oder aber die damit geforderte Interoperabilität der Formate einen Eingriff in die unternehmerische Freiheit des Verantwortlichen darstellt. Dennoch gilt es insgesamt zu entscheiden, inwiefern bei Nichtumsetzung der Interoperabilität ein Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen vorliegt, der höher zu bewerten ist. Diese Ausführungen umfassen eine Gesamtwürdigung aller Umstände des jeweiligen Einzelfalls.

Im Ergebnis liefe dies auf eine Interessenabwägung hinaus, die in Artikel 20 Datenschutzgrundverordnung vom Wortlaut nicht vorgesehen ist, sondern nur korrigierend durch die Einbeziehung des Wettbewerbsrechts und des Schutzzwecks der Norm (den Anbieterwechsel zu erleichtern) erfolgt. Insgesamt muss dementsprechend entschieden werden, inwieweit Wettbewerbsrecht und Datenschutzrecht sich gegenseitig beeinflussen oder im Sinne eines gleichberechtigten Nebeneinanders unabhängige Sanktionsmöglichkeiten bestehen. Dies wäre grundsätzlich nichts neues, da nicht jeder Verstoß gegen das Datenschutzrecht gleichzeitig als wettbewerbswidrig eingestuft wird. Zu bedenken ist aber nun in diesem Fall, dass die Sanktionsmöglichkeiten der Datenschutzaufsichtsbehörden durch Erhöhung der Bußgelder empfindliche Konsequenzen haben und dem Recht auf Datenübertragbarkeit eine wettbewerbsrechtliche Komponente innewohnt. Bei der Auslegung der Norm und der Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Datenschutzgrundverordnung sollte hierauf und im Sinne einer europaweiten Vereinheitlichung besonders geachtet werden.

Fazit und Zusammenfassung

Das Recht auf informationelle Selbstbestimmung wird insgesamt dadurch gestärkt und verbessert, sofern betroffene Personen die von Ihnen in Anspruch genommenen Dienste leicht wechseln können. Zu prüfen ist jedoch, ob dies unterschiedslos bei jedem Dienst auch für *sämtliche* **Nutzungsdaten** gelten kann. Ursprünglich wollte der europäische Gesetzgeber im Rahmen des Rechts auf Datenübertragbarkeit lediglich ein Recht auf Kopie sicherstellen und das Recht der Weitergabe auf vertragsrelevante Daten beschränken.[73]

Zu bedenken ist, dass (auch) bei **Nutzungsdaten** stets ein Recht auf Erhalt einer gängigen, elektronischen Kopie nach Artikel 15 Absatz 3 Datenschutzgrundverordnung besteht. Damit erhält

[73] Siehe die obigen Ausführungen unter Punkt 1.2. sowie Artikel 18 des Entwurfs der Datenschutzgrundverordnung von 2012.

die betroffene Person ein wertvolles und verbessertes Kontrollinstrument.[74] Daher ist zu prüfen, inwieweit die darüber hinaus gehende direkte Übertragungsmöglichkeit im Sinne eines Verfügungsrechts über *sämtliche* Nutzungsdaten im Einzelfall tatsächlich einen Mehrwert für das informationelle Selbstbestimmungsrecht der Betroffenen darstellt. Dies ist auch in Bezug auf die Kommerzialisierung von personenbezogenen Daten sowie einer wirtschaftlichen Verwertungsbefugnis, aber auch Verwertungskompetenz zu betrachten. Letztendlich stellt es eine Entscheidung dahingehend dar, ob die betroffenen Personen tatsächlich für eine vollumfängliche Datensouveränität bereit sind.[75]

In diesem Zusammenhang ist die Sicherstellung von ausreichender **Transparenz** als weitere wesentliche Anforderung zu berücksichtigen, da der betroffenen Person alle Informationen bekannt sein müssen, die sich auf die Verarbeitung durch den alten und neuen Verantwortlichen beziehen. Dies gilt insbesondere, da mit dem Recht auf Datenübertragbarkeit nicht automatisch Löschungsansprüche gemäß Artikel 17 Datenschutzgrundverordnung verbunden sind.

Ein interessengerechtes Ergebnis in Bezug auf den **Anwendungsbereich** könnte auch dadurch erreicht werden, wenn bei der Abgrenzung von vertragsrelevanten Daten und Nutzungsdaten („observed data“) der Servicegedanke des jeweiligen konkreten Dienstes in die Bewertung mit einfließt. So könnte dienstespezifisch bzw. einzelfallbezogen geprüft werden, welche durch die Inanspruchnahme des Dienstes erzeugten Daten zugleich als „zur Vertragserfüllung erforderlich“ und damit ebenfalls als sinnvolles Kundeninteresse rechtlich eingeordnet werden könnten.[76]

In Bezug auf die **Daten Dritter** sind deren Schutzrechte zu berücksichtigen. Die Auffassung der Artikel-29-Datenschutzgruppe, dass einem „neuen“ Verantwortlichen zwar Daten Dritter übermittelt werden dürfen, er diese aber nicht für seine eigenen Zwecke verwenden darf, [77] ist differenziert zu betrachten. Zum einen könnten sich die Dritten bewusst gegen einen bestimmten kommerziellen Anbieter entschieden haben. Zum anderen ist die Nichtverwendung in der Praxis auch entsprechend sicherzustellen und zu vermeiden, dass Daten bei immer mehr Verantwortlichen aufgrund berechtigter Interessen und zulässiger Zweckänderung verarbeitet werden.[78] Hierfür müssen noch einheitliche, europaweit geltende Maßstäbe gebildet werden.

Für **Arbeitnehmerdaten** gibt es noch keine klare Tendenz, so dass hier klare Kriterien zu entwickeln sind, unter welchen Voraussetzungen ein Anspruch auf Datenübertragbarkeit besteht.

Hinsichtlich des **Datenformats** und der geforderten **Interoperabilität** ist das Wettbewerbsrecht ergänzend zu berücksichtigen. Wettbewerbsrecht und Datenschutzrecht stehen gleichberechtigt nebeneinander. Mit Blick auf den wettbewerbsrechtlichen Ansatz von Artikel 20 Datenschutzgrundverordnung sowie dem Schutzbereich dieser Norm, einen Anbieterwechsel zu erleichtern, könnten sich Wettbewerbsrecht und Datenschutzrecht dennoch gegenseitig

[74] Siehe hierzu auch die Ausführungen unter Punkt 1.2, insbesondere den ursprünglichen Erwägungsgrund 55 zum Recht auf Datenübertragbarkeit (in der Fassung der Datenschutzgrundverordnung von 2012), der auf die Verbesserung des Auskunftsrechts abstellte.
[75] Siehe hierzu die Ausführungen auf S. 11 ff.
[76] Z.B. die Werte einer Fitness-App, siehe oben S. 13. Dann kann aber wiederum der kommerzielle Wert der Daten für alle Beteiligten eine Rolle spielen.
[77] Siehe hierzu die Ausführungen unter Punkt 1.3.
[78] Zu beachten ist ergänzend, dass selbst ursprünglich anonymisierte Daten (etwa im Rahmen einer weiteren Datenverarbeitung) nach gewisser Zeit ihre Anonymität verlieren könnten.

beeinflussen. Aus diesem Grunde könnte geprüft werden, ob Kriterien entwickelt werden sollten, um eine harmonisierte Sichtweise zu schaffen.[79]

Des Weiteren ist hinsichtlich des Begriffs der **Metadaten** eine einheitliche technische und juristische Definition zu verwenden und zu prüfen, welche Metadaten aus technischer Sicht im Rahmen der Entwicklung eines Standard-Formats zur Datenportabilität unbedingt erforderlich und aus rechtlicher Sicht zulässig sind.[80]

Ebenso ist eine Abgrenzung zum **Auskunftsrecht** vorzunehmen und darüber hinaus zu prüfen, was von dem Begriff „Kategorien von Daten" gemäß Artikel 15 Absatz 3 Datenschutzgrundverordnung erfasst ist.[81]

Insgesamt gilt, dass der wirkungsvolle Schutz personenbezogener Daten und das Recht auf informationelle Selbstbestimmung wirtschaftlichen Interessen stets vorgehen müssen. Dennoch ist zu entscheiden, inwieweit das informationelle Selbstbestimmungsrecht der betroffenen Person bei Nichtbereitstellung einer „Datenübertragung mit einem Klick" ausnahmslos tangiert ist und auch einen abmahnfähigen Wettbewerbsverstoß nach sich zieht. Damit ist die Frage verbunden, ob ein „pauschales" Recht auf Datenübertragbarkeit unterschiedslos für *sämtliche* Nutzungsdaten sowie „zwischen" jeden Dienstleistungen gilt und im Rahmen einer fortwährenden praxisgerechten Prüfung eine Gesamtwürdigung der Interessen einfließen könnte. Dies muss insgesamt im europäischen Harmonisierungskontext betrachtet und bei der Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Datenschutzgrundverordnung berücksichtigt werden.

[79] Siehe hierzu die Ausführungen unter Punkt 4., unter anderem auch die Bewertungen zur Vergleichbarkeit von Dienstleistungen und der „Datenkopie" zu einem weiteren Dienstleister, S. 13 und S. 14.
[80] Siehe die Ausführungen unter Punkt 2. Es könnte ebenso aus technischer Sicht geprüft werden, ob ein bestimmtes, maschinenlesbares Format die von der Artikel-29-Datenschutzgruppe geforderte Übertragung von möglichst vielen Metadaten auf bester Granularitätsstufe obsolet machen könnte. Geprüft werden könnte dabei auch, ob ein pdf-Dokument eher als gängiges, elektronisches Format zur Sicherstellung des Auskunftsrechts dient, aber als maschinenlesbares Format im Rahmen der Umsetzung der Datenportabilität grundsätzlich auszuschließen ist.
[81] Das Auskunftsrecht bezieht sich nun anders als noch in § 34 BDSG geregelt, nicht mehr auf „die zur Person gespeicherten Daten", sondern auf „Kategorien von Daten". Daher muss entschieden werden, inwieweit die Erwägungsgründe (39) sowie (62) der Datenschutzgrundverordnung zu berücksichtigen sind, die diese Einschränkung nicht vornehmen, sondern die Auskunft weiterhin hinsichtlich der „die Person betreffenden verarbeiteten personenbezogene Daten" regeln. Fraglich ist auch, inwieweit damit eine Änderung der bisherigen Rechtspraxis verbunden sein könnte und weniger Information als bisher verlangt ist und ob etwa die Angabe „Telekommunikationsmetadaten" mit Aufzählung der Beispiele aus dem Verordnungstext der E-Privacy-Verordnung als Auskunft ausreichen könnte.

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

ISBN 978-3-00-058336-0