Universität Zürich[UZH]

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Gutachten zur

Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS)

Prof. Dr. Rolf H. Weber / Prof. Dr. Florent Thouvenin

unter Mitarbeit von: Dr. Alfred Früh, RA, MLaw Damian George, RA und MLaw Kento Reutimann

Zürich, 22. Dezember 2017

INHALTSVERZEICHNIS

A. VORBEMERKUNGEN

Im Rahmen der Strategie „Digitale Schweiz" hat der Bundesrat das Ziel formuliert, eine kohärente und zukunftsorientierte Datenpolitik für die Schweiz zu schaffen und die Schweiz als attraktiven Standort für die Wertschöpfung durch Daten zu positionieren[1]. Zu diesem Zweck hat der Bundesrat an seiner Sitzung vom 22. März 2017 übergeordnete Ziele definiert und das Eidgenössische Justiz- und Polizeidepartement (EJPD) beauftragt, die Rechtslage für eine Weiterverwendung von Personendaten, Sachdaten und anonymisierten Daten zu analysieren.

Im Juli 2017 haben das Bundesamt für Justiz und das Bundesamt für Kommunikation dem Center for Information Technology, Society, and Law (ITSL), einem interdisziplinären Kompetenzzentrum der Universität Zürich, den Auftrag erteilt, für die Weiterverwendung von Personendaten zwei Fragestellungen im Rahmen eines Rechtsgutachtens näher zu untersuchen. Einerseits ist zu prüfen, ob der Gesetzgeber aktiv werden sollte, um die Wiederverwendung von Personendaten unter Kontrolle der betroffenen Personen zu fördern, insb. im Rahmen von sog. Personal Information Management Systems (PIMS). Andererseits ist zu untersuchen, ob die Datenportabilität (wie in der EU) auch im schweizerischen Recht geregelt werden sollte. Wie sich zeigen wird, sind die beiden Fragestellungen eng miteinander verknüpft. Namentlich kommt der Datenportabilität für das Funktionieren von PIMS eine zentrale Bedeutung zu.

Der Gutachtensauftrag umfasst zwölf spezifische Fragen: vier zu PIMS und acht zur Datenportabilität. Das Gutachten folgt im Wesentlichen den gestellten Fragen, wenn auch im Rahmen einer eigenständigen Struktur und teilweise in abgeänderter Reihenfolge. Namentlich beginnt der Teil zu den PIMS mit einer Übersicht zu den heutigen Entwicklungsformen und untersucht erst danach den rechtlichen Rahmen sowie die Frage nach möglichen Hindernissen und Fördermassnahmen. Bei der Datenportabilität erweist es sich als angebracht, die ausländischen Rechtsentwicklungen zu thematisieren, bevor auf die spezifischen Fragen eingegangen wird.

Um sicherzustellen, dass technische Expertise und die Sicht der betroffenen Kreise ins Gutachten einfliessen, haben die Gutachter – soweit erforderlich – das entsprechende Know-how innerhalb des ITSL beigezogen und eine Reihe von halb-strukturierten Interviews geführt. Als Interview-Partner standen Personen zur Verfügung, die massgeblich an der Entwicklung und Konzeption von PIMS beteiligt gewesen sind, und Personen aus Unternehmen, die von der Einführung eines Datenportabilitätsrechts betroffen wären. Die in den Interviews gewonnenen Erkenntnisse sind beim Verfassen dieses Gutachtens berücksichtigt worden, insbesondere bei den technischen Ausführungen.

Die Ausführungen in diesem Gutachten beziehen sich grundsätzlich auf das geltende Datenschutzgesetz (DSG), das derzeit eine Totalrevision erfährt. Soweit indessen nach dem heutigen Stand der

---

1 BUNDESRAT, Datenpolitik des Bundes.

Arbeiten damit zu rechnen ist, dass die Revision zu neuen Regelungen führen wird, die für PIMS oder die Einführung einer Datenportabilität relevant sind, wird auf diese Unterschiede hingewiesen. Grundlage ist dabei der Entwurf des DSG vom 15. September 2017 (E-DSG).

B. PERSONAL INFORMATION MANAGEMENT SYSTEMS (PIMS)

1. Ausgangslage

Mit Blick auf die weiterhin stark anwachsende Datenmenge ist es heute für die einzelne Person sehr schwierig, den Überblick oder gar die Kontrolle über sämtliche persönlichen Daten zu behalten. Eine Möglichkeit, diese Schwierigkeit zu überwinden, sind sog. *Personal Information Management Systems (PIMS)*.

Allgemein sind unter PIMS Systeme zur zentralen Sammlung und Verwaltung der eigenen Daten zu verstehen, die auf eine künftige Nutzung dieser Daten ausgerichtet sind. Eine spätere Nutzung kann beispielsweise darin bestehen, die Daten zu persönlichen Zwecken auszuwerten (bspw. um Rückschlüsse zur Verbesserung der eigenen Gesundheit zu ziehen) oder Daten der wissenschaftlichen Forschung oder kommerziellen Diensteanbietern zur Verfügung zu stellen. MyData-Dienste lassen sich entweder als Spielart von oder als Alternative zu PIMS verstehen. Bei MyData liegt der Fokus stärker auf dem gezielten Teilen der Daten mit Dritten, insbesondere zu Forschungszwecken. Eine klare Abgrenzung zwischen PIMS und MyData erscheint angesichts der vielfältigen Ausgestaltungen in der Praxis allerdings äusserst schwierig (siehe hinten Abschnitt B.3). Hinzu kommt, dass die Bezeichnung PIMS weder allgemein bekannt ist noch einheitlich verwendet wird. Stattdessen ist bisweilen auch von „Personal Data Storage“ oder „Personal Data Services“ (PDS) die Rede. Um Einheitlichkeit zu gewährleisten, wird in der Folge allein der Begriff „PIMS“ verwendet, unter Einschluss der MyData-Dienste und der als PDS bezeichneten Dienste.

Eine grundlegende Neuerung von PIMS besteht darin, dass die Daten eines Nutzers zentral gesammelt und verwaltet werden können und nicht mehr fragmentiert auf verschiedenen Plattformen kontrolliert werden müssen (siehe dazu die vereinfachte Darstellung in Abbildung 1; in der Realität ist nicht nur von zwei, sondern von einer Vielzahl von Diensteanbietern auszugehen). Diese Zentralisierung erleichtert es den Nutzern massgeblich, den Überblick über die eigenen Daten zu behalten oder sich diesen zu verschaffen und die Daten unter Umständen auch mithilfe der von PIMS zur Verfügung gestellten Analysemöglichkeiten für eigene Zwecke auszuwerten. Zudem können die Nutzer die Daten zentral aktualisieren und selbst entscheiden, ob und wem sie welche Daten zur Verfügung stellen. Das Funktionieren von PIMS steht in engem Zusammenhang mit der Datenportabilität (hinten Kap. C). Zum einen könnten die Nutzer von PIMS gestützt auf ein allfälliges Recht auf Datenportabilität ihre Daten mit vergleichsweise wenig Aufwand auf PIMS übertragen und Daten aus zahlreichen Quellen in einem PIMS zusammenführen. Zum andern könnte das gesammelte Knowhow beim PIMS-Anbieter die Sicherstellung der Kompatibilität verschiedener Datenformate vereinfachen, was auch die Diensteanbieter bei der Umsetzung des Rechts auf Datenportabilität entlasten würde.

PIMS haben das Potenzial, bei der Nutzung von persönlichen Daten einen eigentlichen Paradigmenwechsel herbeizuführen, indem nicht mehr nur die Diensteanbieter ihre Beziehungen zu ihren Kunden

steuern, sondern die Kunden ihrerseits ihre Beziehung zu verschiedenen Diensteanbietern verwalten können. Für die Nutzer sind PIMS auch deshalb von Interesse, weil sie es ermöglichen, dass Daten vereinfacht von den verschiedenen Diensteanbietern an die Nutzer zurückfliessen (bspw. Auswertungsergebnisse aus den zur Verfügung gestellten Daten).

Aus Sicht der Forschung haben PIMS enormes Potential, da Forschende (in Abbildung 1 als Datenanalysten bezeichnet) unter Umständen Zugang zu Daten erhalten, die bisher nicht zugänglich waren, namentlich nicht in diesen Mengen und allenfalls auch nicht in dieser Qualität.

Gewisse positive Aspekte könnten auch für (kommerzielle) Diensteanbieter entstehen, da die Daten von Personen stammen, die bewusst in die Bearbeitung einwilligen. Dadurch erhofft man sich eine bessere Datenqualität. Zudem liessen sich der Aufwand und die Kosten für die Compliance stark senken.

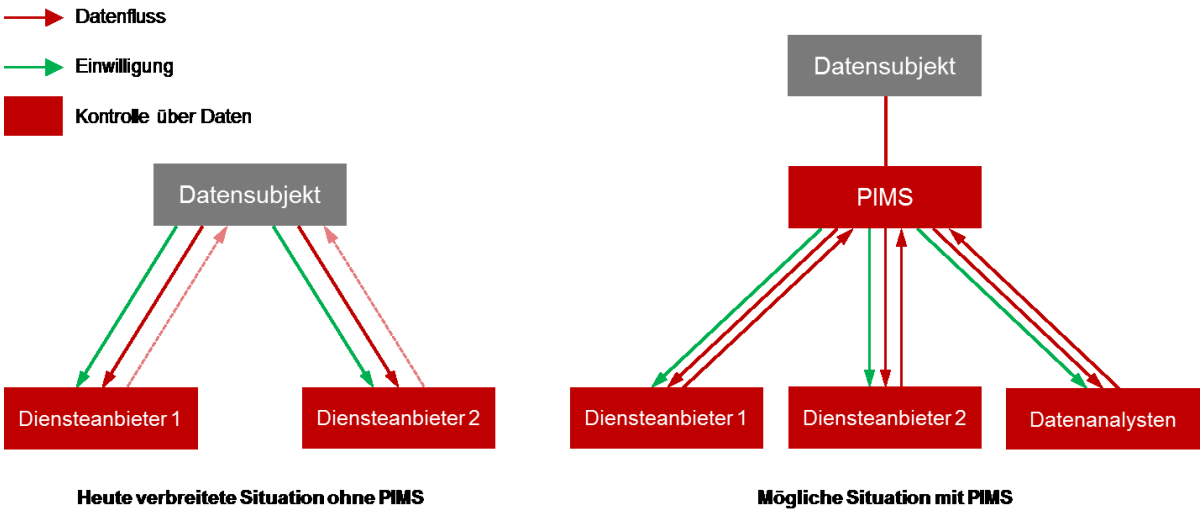

Abbildung 1: Datenfluss ohne/mit PIMS

Für die rechtliche Analyse von PIMS ist eine Orientierung am sog. Informationslebenszyklus hilfreich. Der Informationslebenszyklus beschreibt die Phasen, welche die Information typischerweise durchläuft[2]. Die Rechtsordnung orientiert sich verschiedentlich zumindest implizit an Informationslebenszyklen, um normative Konzepte der Informationshandhabung zu entwickeln und zu regeln[3]. Das konzeptionelle Erfassen von Information in Phasen strukturiert und erleichtert die rechtliche Beurteilung, da in den verschiedenen Phasen unterschiedliche Normen anzuwenden sind.

---

2 BEGLINGER/BURGWINKEL/LEHMANN/NEUENSCHWANDER/WILDHABER, 38 f.; siehe z.B. OFFICE OF MANAGEMENT AND BUDGET, 28, welches die Phasen als Erheben oder Kreation, Verarbeitung, Weiterverbreitung, Nutzung, Speicherung und Entäusserung durch Zerstörung oder Löschung beschreibt.

3 Siehe HARASGAMA, 225 f.

Der Informationslebenszyklus sieht bei PIMS wie folgt aus:

- **Erheben**: Die Daten werden von den Datensubjekten zur Verfügung gestellt. Je nach PIMS variieren Art und Umfang der Daten.
- **Speichern**: Die Daten werden lokal oder in einer Cloud gespeichert.
- **Verarbeiten und Instandhalten**: Die Daten werden analysiert, laufend ergänzt oder mit weiteren Daten kombiniert.
- **Kommunikation**: Die Daten oder die aus den Daten gezogenen Schlüsse werden dem Datensubjekt oder einem Diensteanbieter (Forschender, kommerzieller Nutzer) kommuniziert. Bei diesem Dritten beginnt ein neuer Informationslebenszyklus.
- **Nutzen**: Die Daten oder die Erkenntnisse werden für einen bestimmten Zweck verwendet.
- **Archivieren oder Löschen**: Die Daten werden archiviert und gegebenenfalls wiederverwertet oder sofort bzw. nach einer vorgegebenen Zeit gelöscht.

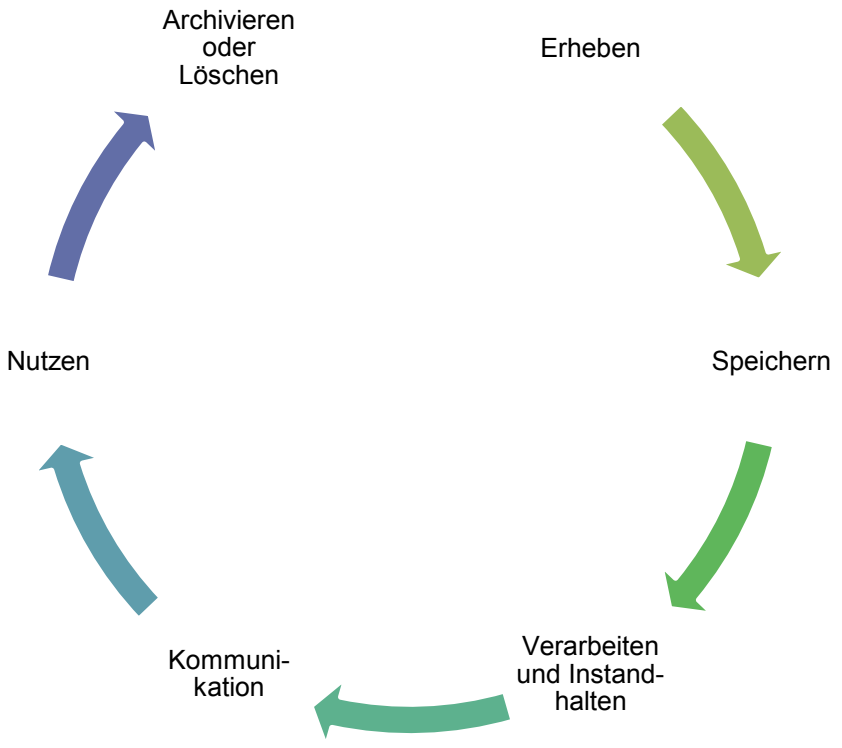

Abbildung 2: Informationslebenszyklus bei PIMS

Der Begriff Informationslebenszyklus darf nicht darüber hinwegtäuschen, dass Informationen diesen Zyklus nicht zwingend vollständig oder in der skizzierten Reihenfolge durchlaufen. Insbesondere ist der Begriff „Zyklus“ nicht wörtlich zu nehmen, weil dieser „Zyklus“ mit der Löschung der Daten endet, weshalb die Abbildung 2 (im Gegensatz zur gängigen Darstellung) keinen geschlossenen Kreis zeigt.

2. Fragestellungen

Gemäss Auftrag sind in diesem Gutachten die folgenden Fragen zu beantworten:

Frage 1: Inwiefern sind PIMS-Projekte in der Schweiz bereits Realität?

Frage 2: In welchem Rahmen ermöglicht das schweizerische Recht die Realisierung von PIMS-Projekten? Was sind die allfälligen Hürden?

Frage 3: Welche konkreten Massnahmen können die Entwicklung derartiger Projekte fördern?

Frage 4: Welche Schwierigkeiten, Vorteile und Nachteile sind mit diesen Massnahmen verknüpft? Sind die Massnahmen kompatibel mit den internationalen Entwicklungen, insb. in der EU?

3. Stand der Entwicklung

Im Folgenden werden verschiedene PIMS-Projekte in der Schweiz dargestellt. Allgemein ist im Privatsektor ein massgeblicher Trend zu PIMS im Bereich Gesundheitsdaten erkennbar. Bei öffentlichen Projekten stand bisher die E-Identity im Vordergrund. Diese spielt nun aber auch bei privaten Projekten eine immer grössere Rolle.

3.1. Private Projekte

3.1.1. MIDATA.coop

Die MIDATA Genossenschaft[4] mit Sitz in Zürich bietet den Nutzern ihrer Plattform die Möglichkeit, ihre Daten zu speichern, zu verwalten und den Zugang dazu zu steuern. MIDATA legt den Fokus (zumindest vorerst) auf gesundheitsrelevante Daten. Die Nutzer sollen entscheiden können, welche Daten sie mit bestimmten Freunden oder Ärzten teilen oder der Forschung zur Verfügung stellen möchten. Den Nutzern werden zudem Tools zur Visualisierung und Analyse der eigenen Daten zur Verfügung gestellt, um Rückschlüsse auf die eigene Gesundheit ziehen zu können.

Es ist vorgesehen, dass sich die Nutzer genossenschaftlich organisieren, da diese Organisationsform nach Ansicht der Betreiber die bestmögliche Wahrung der Nutzerinteressen garantiert. Die Nutzer sollen sich in regionalen oder nationalen Genossenschaften zusammenschliessen. Die Mitgliedschaft in der Genossenschaft ist gemäss Statuten nicht Voraussetzung für die Eröffnung eines Daten-Kontos. Einkünfte der Genossenschaft sollen in die Plattform reinvestiert und zur Finanzierung von Forschungsprojekten verwendet werden, die dem Allgemeinwohl dienen.

---

4 <https://midata.coop>, zuletzt besucht am 20. Dezember 2017.

3.1.2. Healthbank

Healthbank[5] bietet ihren Nutzern eine zentrale Verwaltungsmöglichkeit für ihre gesundheitsrelevanten Daten. Die Plattform soll die Daten von Patientenakten, Wearables, E-Health Apps, Apotheken und Smart Medical Devices vereinen. Nutzer sollen selber entscheiden können, mit wem und wann sie die eigenen Daten teilen wollen. Die Einstellungen können jederzeit angepasst und die Einwilligung vollständig zurückgezogen werden.

Die Nutzer sollen profitieren, indem sie sich durch die Zusammenführung der Daten ein besseres Bild über ihre Gesundheit machen und eine angemessene „Belohnung" erhalten können. Auf Grundlage der Angaben der Anbieter ist allerdings nicht ganz klar, ob diese Belohnung finanzieller Natur ist.

Die Nutzer schliessen sich genossenschaftlich in der Société cooperative HealthBank zusammen. Die healthbank innovation AG übernimmt die Vermittlung zwischen der Genossenschaft und allfälligen Datenbearbeitern. Gemäss eigenen Angaben kontrolliert die Genossenschaft die healthbank innovation AG.

Die Basisnutzung wird den Nutzern kostenlos angeboten, der Genossenschaftsanteil kostet CHF 100.

3.1.3. BitsaboutMe

BitsaboutMe[6] bietet eine Importfunktion an, mit welcher Daten von grossen Plattformen wie Facebook, LinkedIn oder Google direkt in den persönlichen Speicher auf BitsaboutMe transferiert werden können. Dort abgelegte Daten lassen sich strukturiert einsehen. Das Angebot umfasst darüber hinaus einen Datenmarktplatz, auf dem die Nutzer Drittanbietern zu eigenen Konditionen ihre gespeicherten Daten zur Nutzung anbieten können. BitsaboutMe partizipiert bei diesen Transaktionen an den für den Nutzer generierten Erlösen.

BitsaboutMe ist als Aktiengesellschaft organisiert (Sitz in Bern). Im Unterschied zu MIDATA und Healthbank ist die Plattform mehr auf kommerzielle Nutzung als auf Forschung ausgerichtet.

3.1.4. Procivis

Die Procivis AG[7] mit Sitz in Zürich bietet eine E-ID-Lösung mit einer eigenen App („eID+") an, die Anfang Dezember 2017 in Zusammenarbeit mit dem Kanton Schaffhausen auf den Markt gebracht wurde[8]. eID+ soll einen sicheren Login per Zwei-Faktor-Authentifizierung sowie die digitale Signie-

---

5 <https://www.healthbank.coop>, zuletzt besucht am 20. Dezember 2017.

6 <https://bitsabout.me>, zuletzt besucht am 20. Dezember 2017.

7 <https://procivis.ch>, zuletzt besucht am 20. Dezember 2017.

8 Siehe hinten B.3.2.2.

rung und Speicherung von Dokumenten ermöglichen. Procivis arbeitet derzeit zudem mit der Universität Zürich an einem E-Voting-Projekt, das basierend auf der eigenen E-ID-Lösung funktioniert[9].

Kürzlich hat Procivis ein neues Non-Profit-Projekt namens „VALID" angekündigt[10]. VALID ermöglicht eine digitale Identität und bietet gleichzeitig eine Plattform zur Verwaltung und Monetarisierung von persönlichen Daten. Die Betreiberin selbst hat keinen Zugriff auf die Nutzerdaten und die Nutzer sollen ihre Daten auch in anonymisierter Form weitergeben können. Ein Marktplatz verbindet interessierte Datenbearbeiter mit den Nutzern. Diese sollen bei einem erfolgreichen Vertragsabschluss mit VALID-Tokens entschädigt werden. Nach aktuellem Stand ist ein Token Sale geplant. Die Plattform soll im Sommer 2019 starten und im Jahr 2021 an eine Stiftung übergeben werden[11].

3.1.5. uPort

Die Consensys AG mit Sitz in Zug entwickelt die uPort-Plattform, die auf der Blockchain (Ethereum) basiert und die Verwaltung eigener Daten inklusive Authentifizierung und Verifizierung ermöglicht[12]. uPort nutzt ein System aus verschiedenen Smart Contracts, um bekannten Sicherheitsrisiken entgegenzuwirken: Ein vorgelagerter Smart Contract reduziert das Risiko des Passwortverlusts, indem der Zugang mithilfe von vorbestimmten Drittpersonen (z.B. ein Quorum vorbestimmter Vertrauenspersonen) wieder hergestellt werden kann. Der Mechanismus ermöglicht zudem ein Eingreifen für den Fall, dass der Account gehackt wird und jemand die Kontrolle über die digitale Identität zu übernehmen versucht[13]. Die Daten der Nutzer werden nicht direkt auf der Blockchain, sondern *off-chain* gespeichert (Gerät des Nutzers oder bspw. IPFS[14]) und mittels Hash auf der Blockchain referenziert[15]. Die App ist momentan als Alpha-Version verfügbar[16].

3.2. Öffentliche Projekte

3.2.1. Stadt Zug

Die Stadt Zug bietet ihren Einwohnern seit September 2017 die Möglichkeit, eine digitale Identität basierend auf der Blockchain-Technologie (Ethereum) zu schaffen. An diesem Projekt ist auch die

---

9 <http://www.inside-it.ch/articles/48810>, zuletzt besucht am 20. Dezember 2017.

10 <https://valid.global>, zuletzt besucht am 20. Dezember 2017.

11 PROCIVIS.

12 LUNDKVIST/HECK/TORSTENSSON/MITTON/SENA, 2.

13 LUNDKVIST/HECK/TORSTENSSON/MITTON/SENA, 3 ff.

14 Das InterPlanetary File System (IPFS) ermöglicht eine dezentrale Speicherung von Daten (P2P). Die gespeicherten Daten können mittels eines unveränderlichen permanenten Links abgerufen werden, weshalb das System gerade im Bereich Blockchain grosses Potential hat.

15 LUNDKVIST/HECK/TORSTENSSON/MITTON/SENA, 2.

16 <https://www.uport.me/>, zuletzt besucht am 20. Dezember 2017.

ConsenSys AG beteiligt, welche die uPort-Plattform entwickelt[17]. Die Identität wird von der Einwohnerkontrolle der Stadt beglaubigt und es können weitere persönliche Informationen gespeichert werden. Sämtliche Informationen und Transaktionen sollen durch den Einsatz von Blockchain fälschungssicher sein[18].

3.2.2. Kanton Schaffhausen

Der Kanton Schaffhausen arbeitet zusammen mit der Procivis AG[19] an einem E-Government-Pilotprojekt. Die Bewohner des Kantons Schaffhausen sollen über eine mobile App Zugang zu ihrer offiziellen elektronischen Bürger-ID erhalten. Ermöglicht werden soll u.a. die Nutzung von darin verfügbaren Behördendienstleistungen wie Einwohnerkontrolldienste und Steuerservices. Die App eID+ wurde Anfang Dezember 2017 auf den Markt gebracht. Vorerst können die eingegebenen Daten (nur) bei der Einwohnerkontrolle der Stadt Schaffhausen verifiziert werden.

3.3. Forschungsprojekte

3.3.1. Universität Zürich: Data Purse – Data Management for Citizens

Im Rahmen des „Data Purse"-Projekts des Instituts für Informatik an der Universität Zürich wurde zusammen mit Partnern aus der Wirtschaft an PIMS-Lösungen geforscht. Von 2012 bis 2014 wurde untersucht, welche Vorteile aus Sicht der Nutzer durch die Nutzung von PIMS entstehen, wie PIMS technisch auszugestalten sind und was mögliche Geschäftsmodelle wären[20]. Der Fokus des Projekts lag auf elektronischen Dokumenten. Die Untersuchung war zudem mehr auf das Sammeln und Speichern von Daten und weniger auf das Teilen ausgerichtet[21]. Die Ergebnisse wurden in einer Reihe wissenschaftlicher Publikationen veröffentlicht[22].

3.3.2. MyData.org

Die EU Kommission und der Europäische Datenschutzbeauftragte (European Data Protection Supervisor, EDPS) haben angeregt, PIMS vertieft wissenschaftlich zu untersuchen[23]. Entsprechend sind PIMS denn auch Gegenstand verschiedener Forschungsaktivitäten. Zu erwähnen ist insbesondere das globale MyData-Netzwerk (https://mydata.org), das in den letzten Jahren verschiedene Konferen-

---

17 STADT ZUG.

18 Siehe vorne B.3.1.5.

19 Siehe dazu vorne B.3.1.4.

20 <http://www.ifi.uzh.ch/en/imrg/research/completed-projects/data-purse.html>, zuletzt besucht am 20. Dezember 2017.

21 Siehe zum Ganzen auch PFISTER, *passim*.

22 Eine Liste der Publikationen ist auf der Projektseite verfügbar, siehe <http://www.ifi.uzh.ch/en/imrg/research/completed-projects/data-purse.html>, zuletzt besucht am 20. Dezember 2017.

23 EUROPÄISCHE KOMMISSION, Personal information management services, 16; EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER, Stellungnahme, 17.

zen zum Thema organisiert hat, die nicht nur Forschende, sondern auch Unternehmen, Regierungsvertreter und NGO zusammengebracht haben. Ziel der diesjährigen interdisziplinären Konferenz war es, ein Netzwerk von Organisationen zu schaffen, die sich für eine Datenwirtschaft einsetzen, die den Menschen ins Zentrum stellt. Aus der Konferenz gingen verschiedene MyData-Hubs hervor[24], unter anderem die Swiss Data Alliance[25].

3.3.3. Internet Privacy Engineering Network

Das Internet Privacy Engineering Network (IPEN) ist eine vom EDPS im Jahre 2014 ins Leben gerufene Initiative. IPEN widmet sich der Integration des Datenschutzes und des Schutzes der Privatsphäre in allen Phasen des Entwicklungsprozesses neuer Technologien und bringt hierfür Entwickler mit Privacy Experten in einem jährlichen Workshop zusammen[26]. Der EDPS hat angekündigt, PIMS und ihre Rolle im europäischen Datenschutzrecht im Rahmen dieser Initiative weiter zu erforschen[27].

3.4. Elektronisches Patientendossier

Seit dem Inkrafttreten des Gesetzes über das elektronische Patientendossier am 15. April 2017 ist auf Bundesebene erstmals eine besondere Art von PIMS spezifisch gesetzlich geregelt. Das elektronische Patientendossier (EPD) soll Gesundheitsfachpersonen die Möglichkeit geben, auf behandlungsrelevante Daten von Patientinnen und Patienten zuzugreifen, die von anderen an der Behandlung beteiligten Gesundheitsfachpersonen erfasst wurden und dezentral gespeichert sind[28]. Patientinnen und Patienten sollen ihre eigenen Daten einsehen und den Zugriff auf diese mittels Zugangskontrolle selbst verwalten können. Es ist vorgesehen, dass die im EPD gespeicherten Daten ausschliesslich für die Behandlung der betreffenden Person genutzt werden. Eine Auswertung zu Forschungszwecken oder ein Zugriff durch Versicherungen sind beispielsweise ausgeschlossen. Die Nutzung des elektronischen Patientendossiers ist für Patientinnen und Patienten sowie ambulant tätige Gesundheitsfachpersonen freiwillig. Stationär tätige Gesundheitsfachpersonen haben ihren Patientinnen und Patienten hingegen die Nutzung eines elektronischen Patientendossiers anzubieten[29].

EPD-Anbieter müssen sich durch eine zugelassene Zertifizierungsstelle zertifizieren lassen (Art. 11 ff. EPDG). Die vorgegebenen Normen und Standards müssen erfüllt und organisatorische Vorgaben

---

24 <https://mydata.org/hubs/>, zuletzt besucht am 20. Dezember 2017.

25 Gemäss eigenen Angaben ein überparteilicher Zusammenschluss von Unternehmen, Wirtschaftsverbänden, zivilgesellschaftlichen Organisationen, Forschungsinstitutionen und Einzelpersonen mit dem Ziel, eine zukunftsorientierte Datenpolitik in der Schweiz zu etablieren, <https://www.swissdataalliance.ch>, zuletzt besucht am 20. Dezember 2017.

26 <https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_de>, zuletzt besucht am 20. Dezember 2017.

27 EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER, Stellungnahme, 14 f.

28 WIDMER B., AJP 2017, 770; BAUR/BLUM-SCHNEIDER/EGGER/MAIRE, Jusletter vom 28. August 2017, Rn. 9.

29 BAUR/BLUM-SCHNEIDER/EGGER/MAIRE, Jusletter vom 28. August 2017, Rn. 22; WIDMER B., AJP 2017, 773.

(vor allem in Bezug auf Datensicherheit und Datenschutz) eingehalten werden. Erwartet wird, dass erste EPD-Anbieter ihren Dienst ab Mitte 2018 aufnehmen werden[30].

Das vorgesehene EPD-System unterscheidet sich von der gängigen Vorstellung von PIMS in erster Linie dadurch, dass die Daten weiterhin in den sogenannten Primärsystemen der einzelnen Praxen und Kliniken verbleiben und lediglich im EPD referenziert werden[31]. Anerkannte Gesundheitsfachpersonen dürfen auf Dossiers zugreifen, sofern die Einwilligung der Patientin oder des Patienten vorliegt (Art. 9 Abs. 1 EPDG). Der Kreis der Personen, dem Zugang zu den Daten gewährt wird, ist grundsätzlich auf Gesundheitsfachpersonen beschränkt und kann von der Patientin oder dem Patienten nicht beliebig erweitert werden. Nicht vorgesehen ist bspw. die Möglichkeit, eigene Daten der Forschung zur Verfügung zu stellen[32].

Die Verordnungen enthalten spezifische Bestimmungen zu Datenschutz und Datensicherheit (insb. EPDV-EDI Anhang 2; siehe auch Art. 12, Art. 15 Abs. 2, Art. 31 Abs. 1 lit. d EPDV), welche die am EPD-System beteiligten Parteien für die Zertifizierung und den Betrieb einhalten müssen.

3.5. Charakterisierung von Personal Information Management Systems (PIMS)

Die rechtliche Erfassung von PIMS erfordert eine gewisse Charakterisierung des Phänomens. Die Herausforderung besteht dabei darin, dass PIMS eine relativ junge Erscheinung sind und sich bis jetzt weder einheitliche Geschäftsmodelle noch feste Begrifflichkeiten etabliert haben. Zudem besteht oft eine Diskrepanz zwischen den angestrebten und den heute bereits umsetzbaren oder gar umgesetzten Funktionalitäten. Hinzu kommt, dass schwer abschätzbar ist, welche Formen von PIMS künftig entwickelt und angeboten werden. Die nachfolgende Charakterisierung von PIMS erfolgt auf Grundlage der heute bestehenden und der bereits hinreichend erkennbaren künftigen Angebote. Diese Charakterisierung versteht sich als Analyseinstrument und kann nicht den Anspruch erheben, das Phänomen PIMS in allen seinen Facetten vollständig abzubilden.

PIMS sind in erster Linie als technische Infrastruktur zu betrachten. Sie bieten den Nutzern eine Plattform, um die eigenen Daten zentral zu sammeln, zu verwalten und weiterzugeben. Die Entscheidung, ob und wie die gespeicherten Daten genutzt werden, liegt beim Nutzer selbst. Die Kontrolle beschränkt sich dabei nicht auf einen Alles-oder-Nichts-Ansatz. Vielmehr können Einwilligung und Widerruf der Einwilligung granular erfolgen. Die primäre Aufgabe der PIMS-Anbieter liegt in der Sicherstellung der Datensicherheit und in der Gewährleistung der informationellen Selbstbestimmung der Nutzer. Der Anbieter hat dafür zu sorgen, dass die Daten gegen Verlust und Zugriff durch Dritte geschützt sind.

---

30 EHEALTH SUISSE.

31 Botschaft EPDG, BBl 2013 5321, 5333 f.

32 Botschaft EPDG, BBl 2013 5321, 5372; BAUR/BLUM-SCHNEIDER/EGGER/MAIRE, Jusletter vom 28. August 2017, Rn. 4.

Bei der konkreten Ausgestaltung zeigen sich verschiedene Unterschiede. Einige Anbieter gehen über diese Basisaufgabe hinaus und bieten beispielsweise auf ihrer Plattform Möglichkeiten zur Analyse der gespeicherten Daten an („*analytics as a service*“)[33]. Teilweise wird dem Nutzer die Möglichkeit eingeräumt, die eigenen Daten zu monetarisieren, wobei verschiedene Modelle angedacht sind[34]. Daten könnten direkt auf einem Marktplatz gegen Entgelt angeboten werden (z.B. BitsaboutMe). Möglich erscheint aber auch, dass die Auswertung der Daten beim PIMS-Anbieter erfolgt und an Dritte nur das Ergebnis herausgegeben wird, ohne dass diese Dritten selbst auf die Daten zugreifen können (z.B. VALID).

PIMS ermöglichen den Nutzern, eine bessere Übersicht über die eigenen Daten zu gewinnen und die Kontrolle über ihre Daten besser auszuüben. Je nach Angebot erhalten sie auch einen Zusatznutzen, z.B. eine finanzielle Entschädigung oder den Zugang zu konkreten Forschungsergebnissen (z.B. Empfehlungen zur Verbesserung der eigenen Gesundheit). Eine Rolle spielen aber auch altruistische Motive, namentlich die Förderung des Allgemeinwohls durch die Zurverfügungstellung der eigenen Daten für die Forschung.

3.6. Chancen und Risiken

a) Erweiterte Selbstbestimmung und Monetarisierung von Daten

Die Verwendung von PIMS eröffnet den betroffenen Datensubjekten eine breite Palette von Chancen, insbesondere mit Blick auf eine erweiterte informationelle Selbstbestimmung und die Monetarisierung von Daten.

Die zentrale Verwaltung der eigenen Daten führt zu einer höheren Bereitschaft der Nutzer, die Kontrolle über „ihre“ Daten auszuüben, und ermächtigt sie, (bessere) Erkenntnisse aus ihren eigenen Daten zu gewinnen. PIMS stärken somit die Stellung der betroffenen Personen. Insbesondere erweitern PIMS in genossenschaftlichen Organisationen die Partizipationschancen; überdies verbessern sich die Möglichkeiten von Rechtsdurchsetzung und Überwachung. Auch können die Modalitäten der Datenherausgabe einzelfallbezogen geordnet werden; denkbar wäre z.B. eine Vorsortierung durch den PIMS-Anbieter, damit der Datenbearbeiter keine Rückschlüsse auf die einzelnen Personen ziehen kann.

Mit PIMS lassen sich den betroffenen Personen für die Gewährung des Rechts zur Nutzung „ihrer“ Daten zudem gewisse Vorteile einräumen, z.B. eine Entschädigung in Form von Geld oder anderer finanzieller Anreize. Die Möglichkeit, die betroffenen Personen als Nutzniesser an den neuen Wertschöpfungen durch Daten zu beteiligen, wird oft unter dem Begriff „*Sharing the Wealth*“ diskutiert.

---

33 Z.B. MIDATA, siehe „Mission“, <www.midata.coop>, zuletzt besucht am 20. Dezember 2017.

34 Siehe dazu hinten B.3.6.

Nach diesem Konzept erfolgt eine Aufwertung der betroffenen Personen zu gleichberechtigten Wirtschaftsteilnehmern, die ebenfalls vom Wertzuwachs der Daten profitieren können. Die konkrete Nutzenzuteilung hängt von den Umständen der jeweiligen Datenbearbeitung und von der Ausgestaltung der PIMS ab.

b) Innovationstreiber für *Privacy Enhancing Technologies* (PET)

PIMS könnten einen massgeblichen Beitrag zur *Downstream*-Kontrolle über Daten leisten: Wenn ein Nutzer einem Datenbearbeiter heute Daten zur Verfügung stellt, vermag er nicht zu kontrollieren, was damit geschieht. So könnten Daten entgegen dem erwarteten Zweck bearbeitet, vervielfältigt oder an Dritte weitergegeben werden. Für dieses Problem werden derzeit vor allem vier Lösungsansätze diskutiert:

- *Data-Provenance*-Konzepte streben die Verknüpfung der Datenschutzinformationen mit den Daten an[35]. Die technische Entwicklung scheint jedoch noch nicht gewährleisten zu können, dass diese Verknüpfung nicht gelöscht werden kann.
- Elektronische Dokumente können durch *Digital-Rights-Management-Systeme* gegen Zugriffe von Dritten geschützt werden (sog. „*Information Rights Management*" oder „*Enterprise Digital Rights Management*")[36]. Diese Mittel werden bisher von grösseren Unternehmen eingesetzt, um sensitive Informationen zu schützen[37]. Möglich ist ein solcher Schutz derzeit aber nur für ganze Dokumente, nicht für einzelne Daten.
- Mithilfe *homomorpher Verschlüsselungen* können Computeroperationen an Daten durchgeführt werden, ohne dass der Bearbeiter die Daten sieht. Sobald die Daten entschlüsselt werden, ist das Resultat sichtbar. Derartige Verschlüsselungen stellen allerdings einen Kompromiss dar, weil sie generell schwächer als die gängigen kryptographischen Methoden und deshalb einfacher zu entschlüsseln sind. Zudem wird für die gleichen Computeroperationen viel mehr Rechnerleistung benötigt[38].
- *Data Flow Audits* können die Bearbeitung von Personendaten zu nicht vereinbarten Zwecken zwar nicht verhindern, aber nachvollziehbar machen. Dazu protokolliert der Datenbearbeiter den gesamten Umgang mit Personendaten von der Übernahme bis zur Löschung[39]. Dieses Protokoll

---

35 Primäres Ziel von *Data Provenance* ist ein Herkunftsnachweis. Der Datenbearbeiter kann damit aufzeigen, woher die Daten stammen, was Rückschlüsse auf die Datenqualität erlaubt. Das Konzept beruht auf der Annahme, dass Datenbearbeiter kein Interesse haben, die *Provenance*-Daten zu entfernen. Diese Daten sind deshalb grundsätzlich nicht technisch geschützt und können entsprechend leicht entfernt werden.

36 Siehe dazu REDDY/REDDY GOPU, *passim*.

37 BRANSCOMBE, *passim*.

38 Siehe dazu ausführlich ACAR/AKSU/ULUAGAC/CONTI, *passim*.

39 Siehe dazu PASQUIER/SINGH/POWLES/EYERS/SETZER/BACON, Personal and Ubiquitous Computing 2017, *passim*.

wäre dann von einem Dritten zu prüfen, was allerdings Aufwand und erhebliche Kosten zur Folge hätte.

PIMS könnten einen Beitrag zur Lösung dieser Probleme leisten, indem sie „*analytics as a service*“ und „*zero-knowledge proofs*“ ermöglichen:

- Bei „*analytics as a service*“ würden Diensteanbieter die Algorithmen liefern, die auf der Infrastruktur der PIMS-Anbieter ausgeführt werden. Der Diensteanbieter würde so nur die anonymen Resultate der Auswertung erhalten, ohne dass er je Einsicht in bzw. Kontrolle über die zugrundeliegenden Daten hätte[40]. Eine derartige Lösung wäre insbesondere für Forschung attraktiv, bei der ein Rückschluss auf das Individuum nicht erforderlich ist.
- Bei „*zero-knowledge proofs*“ kann ein Diensteanbieter eine Frage an den PIMS-Anbieter richten, die von diesem mit „wahr“ oder „falsch“ beantwortet wird. Der PIMS-Anbieter prüft also die Aussage und liefert eine Antwort, ohne dass die zugrundeliegenden Daten übermittelt werden. Beispielsweise könnte ein Casino-Betreiber überprüfen, ob ein Kunde volljährig ist, ohne dass ihm das Geburtsdatum mitgeteilt werden muss (so vorgesehen etwa bei eID+ von Procivis[41]).

c) Förderung des Gemeinwohls und Demokratisierung des Datenmarkts

Auch nicht-monetäre Anreize könnten zur Nutzung von PIMS motivieren, etwa die Förderung des Allgemeinwohls (z.B. durch den Fortschritt der Wissenschaft) oder die Verbesserung der eigenen Gesundheit aufgrund individualisierter Empfehlungen für das eigene Verhalten oder in Form konkreter, für die betroffene Person relevanter, Forschungsergebnisse.

d) Beitrag zum Setzen von Standards

Erlangen PIMS eine starke Marktposition, können sie einen Beitrag zum Setzen von Standards leisten und damit auch die Datenportabilität vereinfachen. Im derzeit noch eher hypothetisch erscheinenden Idealfall wäre es denkbar, dass PIMS sogar über ungleich mehr und qualitativ bessere Daten verfügen könnten als die heutigen grossen Player wie Google, Amazon, Facebook und Apple, weil die Nutzer PIMS bspw. auch ihre Gesundheitsdaten, die Daten über ihr Einkaufsverhalten (bspw. Cumulus-Karte), über ihre Finanztransaktionen und viele weitere zur Verfügung stellen. So betrachtet haben PIMS das Potential, den Datenmarkt umzuwälzen und dank der Verfügungsmacht der Individuen über „ihre“ Daten auch zu demokratisieren.

---

40 So auch EUROPÄISCHE KOMMISSION, Personal information management services, 2. Im Rahmen des Data Mining wird dieses Modell beispielsweise bereits vom Internet Archive angeboten, siehe dazu MACDONALD/ LEETARU, *passim*.

41 Siehe KANTON SCHAFFHAUSEN.

e) Sicherheit und Marktoffenheit

PIMS sind mit gewissen Sicherheitsrisiken verbunden. Das gilt namentlich, wenn ein Nutzer alle oder sehr viele Daten ausschliesslich in einem PIMS speichert und Dritte nur über PIMS auf diese Daten zugreifen können. PIMS werden dann zu einem *single point of failure*. Die Risiken können zwar durch angemessene Massnahmen zur Gewährleistung der Datensicherheit reduziert, aber nicht ausgeschlossen werden[42].

Ein weiteres Risiko besteht darin, dass erfolgreiche PIMS kleineren Datenbearbeitern den Zugang zu Daten verwehren könnten, wenn PIMS-Anbieter diesen nicht vertrauen oder den Aufwand für das Gewähren von Zugang scheuen sollten. Dieses Problem könnte allerdings durch die Einführung von Zugangsrechten gelöst werden[43].

f) Wettbewerbsfähigkeit

Die Attraktivität von PIMS für Diensteanbieter wird massgeblich von Volumen und Qualität der Daten abhängen, die sie zur Verfügung stellen können. Solange Diensteanbieter Daten mit gleicher Reliabilität und zu vergleichbar günstigen Konditionen auch von anderen Plattformen beziehen können, besteht die Gefahr, dass der Nutzen von PIMS auf eine verbesserte Selbsterkenntnis der Nutzer beschränkt bleibt. Dies würde die Geschäftsmodelle von PIMS mittelfristig in Frage stellen.

Ein Grossteil der Bevölkerung beteuert zudem zwar, dass ihnen Privatsphäre wichtig ist, was den Schluss zulässt, dass es für die Privatsphäre fördernde Infrastrukturen einen Markt gibt. Allerdings verhalten sich Internetnutzer nicht immer ihren erklärten Präferenzen entsprechend und sind regelmässig bereit, für (vermeintlich unentgeltliche) Leistungen mit ihren Daten zu bezahlen (sog. *Privacy Paradox*)[44]. Der Einfluss dieses Effekts ist allerdings noch nicht abschliessend geklärt[45].

4. Heutiger Rechtsrahmen

4.1. Vorbemerkungen

Das Betreiben und Anbieten von PIMS ist in der Schweiz grundsätzlich erlaubt. Es bestehen namentlich keine allgemeinen oder konkreten Verbote für das Erbringen und Anbieten solcher Dienste[46].

Wie alle privaten Personen (Individuen und Unternehmen), die Personendaten bearbeiten, müssen auch PIMS die Vorgaben des Datenschutzgesetzes (DSG) einhalten. Zugleich sind die Regelungen

---

42 Siehe dazu hinten B.4.2.2.f).

43 Siehe dazu hinten C.2.1.

44 Statt vieler: HARGITTAI/MARWICK, International Journal of Communication 2016, 3737.

45 Siehe auch TSAI/EGELMAN/CRANOR/ACQUISTI, Information Systems Research 2011, *passim*.

46 Siehe auch GORDON, Jusletter IT Flash vom 11. Dezember 2017, Rn. 9 f.

des DSG eine zentrale Grundlage für das Funktionieren dieser Dienste, weil das DSG den betroffenen Personen ein Auskunftsrecht (Art. 8 DSG) gewährt und diesen damit erst ermöglicht, von Datenbearbeitern die Herausgabe ihrer eigenen Daten zu verlangen, um diese anschliessend auf PIMS zu übertragen[47].

Es besteht aber die Möglichkeit, dass ein PIMS-Anbieter gar nicht auf die bei ihm gespeicherten oder verwalteten Daten zugreifen kann (bspw. wegen Verschlüsselung)[48]. In diesem Fall mangelt es an einer rechtlich relevanten Datenbearbeitung, weshalb das DSG keine Anwendung findet[49].

Neben den allgemeinen Vorgaben des DSG haben Anbieter bestimmter Arten von PIMS auch spezialgesetzliche Regelungen zu beachten. Dies gilt namentlich für die Bearbeitung von „Gesundheitsdaten", die den Vorgaben des Humanforschungsgesetzes (HFG) untersteht. Unter Umständen können an Daten, die von Nutzern in PIMS gespeichert werden, auch Rechte Dritter bestehen, insb. Urheber- und Persönlichkeitsrechte. Für diese Fälle ist zu prüfen, ob diese Dritten gegen die Nutzung dieser Daten durch PIMS vorgehen können. Werden verbotene Inhalte gespeichert (bspw. harte Pornografie), könnte sich daraus zudem eine strafrechtliche Verantwortlichkeit des PIMS-Anbieters ergeben.

Die Entwicklung von PIMS im öffentlich-rechtlichen, teilweise aber auch im privat-rechtlichen Bereich[50] wäre mit den Arbeiten zum Bundesgesetz über elektronische Identifizierungsdienste (E-IDG) zu koordinieren. Das Ziel des E-IDG ist die Schaffung staatlich anerkannter elektronischer Identitäten zur Authentifizierung der Identität bei der Inanspruchnahme von E-Government-Dienstleistungen oder E-Commerce-Transaktionen[51]. Anbieter von Identitätsdienstleistungen, die sich nach dem E-IDG anerkennen lassen, sollen nach dem Vorentwurf allerdings keine umfassenden Exklusivrechte geniessen[52], so dass nicht anerkannte PIMS weiterhin am Wettbewerb teilnehmen könnten. Zurzeit werden die Vernehmlassungsergebnisse zum VE-E-IDG ausgewertet und es wird die Botschaft entworfen.

4.2. Datenschutzrecht

4.2.1. Grundsatz

Die Bearbeitung von Personendaten durch Private (Individuen und Unternehmen) ist nach schweizerischem Recht grundsätzlich zulässig[53]. Die Rechtmässigkeit der Datenbearbeitung hängt – anders

---

47 Siehe dazu hinten C.3.3.2.

48 Diesen Ansatz verfolgt z.B. PROCIVIS mit der VALID-Plattform. Siehe dazu vorne B.3.1.4.

49 Siehe zur (Mit-)Haftung für DSG Verletzungen hinten B.4.3.

50 Siehe dazu auch vorne B.3.

51 BUNDESAMT FÜR JUSTIZ, Erläuternder Bericht, 2.

52 BUNDESAMT FÜR JUSTIZ, Erläuternder Bericht, 38.

53 SHK-WERMELINGER, DSG 12 N 1; ROSENTHAL, DSG 12 N 2; THOUVENIN, Big Data, 46; NOUREDDINE, Rz. 3.105; MEIER, Rn. 1526.

als im europäischen Recht – nicht davon ab, dass eine besondere Bedingung für die Rechtmässigkeit erfüllt ist, bspw. eine Einwilligung der von einer Datenbearbeitung betroffenen Person vorliegt. Voraussetzung ist nach schweizerischem Recht allerdings, dass die Grundsätze der Datenbearbeitung (Art. 4, Art. 5 Abs. 1 und Art. 7 DSG) eingehalten werden. Ist dies nicht der Fall, ist die Bearbeitung von Personendaten unzulässig, sofern kein Rechtfertigungsgrund vorliegt (Art. 12 Abs. 1 und Art. 13 DSG). Ein Rechtfertigungsgrund ist gegeben, wenn die betroffene Person in die Bearbeitung ihrer Personendaten eingewilligt hat, ein überwiegendes privates oder öffentliches Interesse vorliegt oder eine gesetzliche Grundlage besteht (Art. 13 Abs. 1 DSG). An diesem Regelungskonzept soll mit dem E-DSG festgehalten werden[54].

Falls PIMS von Bund oder Kantonen angeboten werden, ist eine formell-gesetzliche Grundlage erforderlich (Art. 17 DSG)[55]. Die Behörden sind bereits verfassungsrechtlich an das Legalitäts- (Art. 5 Abs. 1 BV) und das Verhältnismässigkeitsprinzip (Art. 5 Abs. 2 BV) gebunden. Darüber hinaus bestehen für Bundesorgane weitergehende Informationspflichten (z.B. Art. 18a DSG) und Personendaten dürfen nur bekanntgegeben werden, wenn hierfür eine Rechtsgrundlage besteht (Art. 19 DSG).

Falls PIMS-Anbieter als Inhaber einer Datensammlung zu qualifizieren sind[56], treffen sie verschiedene Pflichten[57]. Gemäss Art. 3 lit. i DSG gilt als Inhaber, wer über den Zweck und den Inhalt der Datensammlung entscheidet. Nicht als Inhaber zu qualifizieren ist z.B. ein Rechenzentrum, das nur die technische Infrastruktur zur Verfügung stellt, damit ein Auftraggeber die Datenbearbeitung vornehmen kann[58]. Im Rahmen von PIMS entscheiden zwar üblicherweise die Nutzer selbst, welche Daten sie auf die Plattform hochladen und an wen die Daten herausgegeben werden. Der PIMS-Anbieter stellt aber meist nicht nur eine neutrale Infrastruktur zur Verfügung, sondern richtet die Plattform auf eine bestimmte Nutzungsform aus (z.B. Forschung oder Monetarisierung). PIMS-Anbieter müssen wohl deshalb in der Regel davon ausgehen, dass sie als Inhaber der Datensammlung qualifiziert werden.

Das E-DSG verwendet den Begriff „Inhaber einer Datensammlung“ nicht mehr. Vielmehr definiert es den „Verantwortlichen“ als private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über Zweck und Mittel der Bearbeitung entscheidet (Art. 4 lit. i DSG). Der Begriff „Verant-

---

54 Zum Vorentwurf, siehe ROSENTHAL, Jusletter vom 20. Februar 2017, Rn. 16.

55 Vgl. § 8 ZH-IDG; Art. 5 Abs. 1 BE-KDSG; § 9 BS-IDG; Art. 5 SG-DSG; § 8 i.V.m. § 2 Abs. 3 AG-IDAG.

56 Siehe dazu gerade vorstehend B.4.1.

57 Informationspflicht bei Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 7a DSG); Informationspflicht im Falle von Datenschutzgarantien und -regeln für die grenzüberschreitende Bekanntgabe von Personendaten (Art. 6 Abs. 3 DSG); Auskunftspflicht (Art. 8 DSG); Anmeldepflicht der Datensammlung (Art. 11a DSG); besondere Massnahmen im Bereich Datensicherheit (Art. 9 VDSG); Führung eines Bearbeitungsreglements (Art. 11 und 21 VDSG); Pflicht, im Rahmen einer Bekanntgabe an einen Dritten diesen über die Aktualität und Zuverlässigkeit der Daten zu informieren (Art. 12 VDSG).

58 Botschaft DSG 1988, BBl 1988 413, 448; BSK-BLECHTA, DSG 3 N 88; ROSENTHAL, DSG 3 N 110.

wortlicher“ entspricht dem in der EU verwendeten Begriff (Art. 4 Abs. 7 DSGVO); anders als in der DSGVO genügt aber die blosse Möglichkeit, über die Bearbeitung zu bestimmen, nicht, um als Verantwortlicher zu gelten[59]. Je nach Ausgestaltung dürften auch PIMS als Verantwortliche zu qualifizieren sein; als solche haben sie unter dem E-DSG andere Pflichten als die Inhaber von Datensammlungen unter geltendem Recht, worauf noch spezifisch einzugehen sein wird.

4.2.2. Grundsätze der Datenbearbeitung

Die Grundsätze der Datenbearbeitung sind abstrakt und äusserst breit gefasst. Entsprechend ist es für die Verantwortlichen oft schwierig, deren Einhaltung sicherzustellen. Dies gilt auch für PIMS. Allerdings bestehen relevante Unterschiede zwischen den einzelnen Grundsätzen.

a) Rechtmässigkeit

Rechtmässig ist eine Datenbearbeitung, wenn sie nicht gegen eine Norm der schweizerischen Rechtsordnung verstösst[60]. Bei einer unrechtmässigen Datenbeschaffung ist auch jede darauffolgende Datenbearbeitung grundsätzlich unrechtmässig[61].

b) Treu und Glauben sowie Verhältnismässigkeit

Nach Treu und Glauben erfolgt die Bearbeitung, wenn die Daten in einer Weise bearbeitet werden, die man von einem loyalen und vertrauenswürdigen Teilnehmer am Rechtsverkehr erwarten kann[62]. Die Bearbeitung nach Treu und Glauben dürfte für PIMS in aller Regel unproblematisch sein. Dasselbe gilt für die Verhältnismässigkeit. Dazu muss zunächst die Datenbearbeitung geeignet und erforderlich sein, um den verfolgten Zweck zu erreichen[63]. Darüber hinaus hat der Zweck im Verhältnis zu den Konsequenzen für die betroffene Person (insb. in Bezug auf das Persönlichkeitsrecht) angemessen zu sein. Aus dem Verhältnismässigkeitsgrundsatz werden der Grundsatz der Datenminimierung bzw. Datensparsamkeit sowie der Speicherbegrenzung abgeleitet[64]. Da der Zweck von PIMS

---

59 So schon zum Vorentwurf DSG, siehe ROSENTHAL, Jusletter vom 20. Februar 2017, Rn. 10; zur DSGVO, siehe KLABUNDE, DSGVO 4 N 25, der auf „Entscheidungsgewalt“ abstellt.

60 SHK-BAERISWYL, DSG 4 N 12 f.; BSK-MAURER-LAMBROU/STEINER, DSG 4 N 6; EPINEY, § 9 N 11, 13. Teilweise wird weiter differenziert: Nach ROSENTHAL, DSG 4 N 7, führt lediglich ein Verstoss gegen eine Norm, die dem Schutz der Persönlichkeit dient, zur Unrechtmässigkeit der Datenbearbeitung. Zudem weist ROSENTHAL darauf hin, dass Verhaltensweisen, die ausschliesslich gegen Bestimmungen des DSG verstossen, keine Unrechtmässigkeit im Sinne von Art. 4 Abs. 1 begründen, siehe dazu N 9. EPINEY, § 9 N 11, führt an, bei der Datenbearbeitung durch Private sei insbesondere zu prüfen, ob die Datenbearbeitung im Einklang mit Art. 28 ZGB erfolge.

61 EPINEY, § 9 N 12; implizit wohl auch ROSENTHAL, DSG 4 N 10, der weiter darauf hinweist, dass auch eine unrechtmässige Beschaffung oder Bearbeitung grundsätzlich gerechtfertigt werden könnte.

62 EPINEY, § 9 N 21; NOUREDDINE, Rz. 3.71; siehe auch: BVGer vom 27. Mai 2009, A-3144/2008, E.9.3.

63 ROSENTHAL, DSG 4 N 20; EPINEY, § 9 N 24 i.V.m. N 26; MEIER, Rn. 665; BSK-MAURER-LAMBROU/STEINER, DSG 4 N 9.

64 MEIER, Rn. 673; EPINEY/NÜESCH, N 3.79 Fn. 105; EPINEY, § 9 N 27; BSK-MAURER-LAMBROU/STEINER, DSG 4 N 9; HARASGAMA, 50 f.

in der Regel gerade darin besteht, alle Personendaten, die ihnen von den betroffenen Personen zur Verfügung gestellt werden, zu speichern und zur weiteren Nutzung bereit zu halten, ist die zeitlich und mengenmässig grundsätzlich unbegrenzte Speicherung der Personendaten und deren Nutzung und/oder Bereithaltung zum Abruf verhältnismässig.

Nach E-DSG muss der Verantwortliche durch „Voreinstellungen" sicherstellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist (Art. 6 Abs. 3 E-DSG). Diese sog. „*Privacy by default*" soll erreichen, dass der Nutzer keine Änderung der Einstellungen vornehmen muss, damit die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist. Diese Pflicht zur Voreinstellung gilt jedoch nur, „soweit die betroffene Person nicht etwas anderes bestimmt" (Art. 6 Abs. 3 E-DSG *in fine*). Datenschutzfreundliche Voreinstellungen betreffen den ganzen Lebenszyklus der Daten, deshalb sind die Erhebung der Daten, die Dauer ihrer Speicherung, die Bearbeitungsarten und die Zugänglichkeit für Dritte datensparsam einzustellen[65]. Damit wird letztlich die Erforderlichkeit konkretisiert[66]. Dies bedeutet im Umkehrschluss, dass auch besonders datenintensive Nutzungen zur Erreichung des Zwecks der Bearbeitung erforderlich sein und damit auch entsprechend voreingestellt werden können[67].

PIMS bezwecken, alle Personendaten, die ihnen die betroffenen Personen zur Verfügung stellen, zu speichern und zur weiteren Nutzung bereit zu halten. Eine zeitlich und mengenmässig grundsätzlich unbegrenzte Speicherung der Personendaten und deren Nutzung und/oder Bereithaltung für Dritte ist für die Erreichung dieses Zwecks erforderlich und damit auch mit dem Prinzip des Datenschutzes durch Voreinstellung grundsätzlich zu vereinbaren.

c) Erkennbarkeit

Besondere Bedeutung kommt bei PIMS den Grundsätzen der Erkennbarkeit (Art. 4 Abs. 4 DSG) und der Zweckbindung (Art. 4 Abs. 3 DSG) zu. Nach dem Grundsatz der Erkennbarkeit muss es für die betroffene Person erkennbar sein, ob und wann Daten beschafft werden. Weitgehend unproblematisch ist die Erkennbarkeit bei PIMS, weil die Personendaten von den betroffenen Personen in aller Regel selbst übermittelt werden oder die Übermittlung von ihnen veranlasst wird. Bei der anschliessenden Bearbeitung der Daten durch PIMS ist zentral, dass der Zweck der Bearbeitung für die betroffenen Personen vollständig erkennbar ist. Namentlich dürfen die Daten von PIMS weder zu Zwecken bearbeitet werden, die sie nicht offenlegen, noch ohne Information der Betroffenen an Dritte

---

65 Siehe zur DSGVO BAUMGARTNER, DSGVO 25 N 15.

66 BAUMGARTNER, DSGVO 25 N 14; PLATH, DSGVO 25 N 8. Da die Erforderlichkeit aus der Verhältnismässigkeit hergeleitet wird, wurden datenschutzfreundliche Voreinstellungen schon unter geltendem Recht verlangt. Siehe z.B. EDÖB, Internetprotokoll IPv6; BAUMGARTNER, DSGVO 25 N 17.

67 BAUMGARTNER, DSGVO 25 N 14; PLATH, DSGVO 25 N 11; siehe auch ROSENTHAL, Jusletter vom 27. November 2017, Rn. 43.

weitergegeben werden. Nach Literatur und Rechtsprechung sind die Anforderungen an die Erkennbarkeit im Verhältnis zur jeweiligen Bearbeitung zu beurteilen, insbesondere was den Detaillierungsgrad der Information anbelangt[68]: Bei einfachen Transaktionen kann die Information knapper sein oder unter Umständen sogar gänzlich unterbleiben, wenn die Bearbeitungszwecke bereits aufgrund der Umstände ersichtlich sind oder sich aus dem Gesetz ergeben[69].

Dies erscheint allerdings nicht unproblematisch. Anstatt allgemein einen nicht allzu tiefen Detaillierungsgrad zu verlangen, dürfte es dem Ziel der Erkennbarkeit besser gerecht werden, wenn von den Datenbearbeitern eine gestufte Information verlangt wird. PIMS sollten zum einen einfache und kurze Ausführungen (allenfalls auch in Form von Graphiken oder Kurzfilmen) zu Art, Zweck und Mittel der Datenbearbeitung zur Verfügung stellen, die es kaum an Details interessierten sowie eiligen Nutzern ermöglichen, sich rasch einen Überblick über die Datenbearbeitung zu verschaffen. Darüber hinaus sollten PIMS aber auch detaillierte Informationen bereithalten, die sich an besonders interessierte Nutzer richten. Diese detaillierten Informationen könnten auch auf der Website des jeweiligen PIMS erfolgen und dort aktualisiert werden[70]. Nur wenn sich Nutzer – je nach Bedarf – einfache oder genaue Kenntnis von der Datenbearbeitung zu verschaffen vermögen, ist dem Grundsatz der Erkennbarkeit effektiv Genüge getan. Bei PIMS dürften häufig besonders schützenswerte Daten oder Persönlichkeitsprofile vorliegen, weshalb darüber hinaus die Informationspflicht gemäss Art. 14 DSG zu beachten ist[71].

d) Zweckbindung

Der Grundsatz der Zweckbindung verlangt, dass Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG). Mit diesem Grundsatz wird klargestellt, dass PIMS die ihnen übermittelten Personendaten nur zu den Zwecken bearbeiten dürfen, die sie ihren Nutzern offen legen. So wäre der Grundsatz der Zweckbindung verletzt, falls der PIMS-Anbieter nach dem Zurverfügungstellen der Daten durch die Nutzer und ohne deren Einwilligung entscheiden würde, die Daten zu eigenen Zwecken auszuwerten oder der Forschung zur Verfügung zu stellen.

Nach Art. 5 Abs. 3 Satz 2 E-DSG dürfen Daten neu auch für mit dem ursprünglichen Zweck vereinbare Zwecke bearbeitet werden. Gemäss Botschaft bringt dies eine „terminologische Annäherung“ an die Europarats-Konvention 108, welche keine wesentlichen Änderungen mit sich bringe. Schon bisher gelte, dass keine Weiterbearbeitung zu berechtigterweise unerwarteten oder unange-

---

68 Siehe EDÖB, Erläuterungen, 3; MAURER-LAMBROU/STEINER, DSG 4 N 16c; BAERISWYL, DSG 4 N 47 ff.; EPINEY, § 9 N 39; ROSENTHAL, DSG 4 N 34 und 51; THOUVENIN, Grundprinzipien, 65.

69 EDÖB, Erläuterungen, 3.

70 Vgl. LOBSIGER; siehe auch Erwägungsgrund 58 DSGVO, aus dem nicht ganz klar wird, ob Kommunikation über eine Website nur für an die Öffentlichkeit gerichtete Information ausreichend ist.

71 Siehe dazu hinten B.4.2.5.

brachten Bearbeitungszwecken erfolgen dürfe[72]. Gemäss ROSENTHAL handelt es sich hierbei jedoch um eine Implementierung des Konzeptes der kompatiblen Bearbeitungszwecke, welches sich als eine der Voraussetzungen der Rechtmässigkeit auch in Art. 6 Abs. 4 Satz 2 DSGVO finde[73]. Kompatible Bearbeitungszwecke kommen in der EU als Rechtmässigkeitsgrundlage zur Anwendung, wenn der Verantwortliche Daten einem neuen Bearbeitungszweck zuführen will und sich weder auf eine Einwilligung noch auf eine Rechtsgrundlage zur Bearbeitung der Daten stützen kann[74]. Da eine Bearbeitung zu einem bei der Beschaffung angegebenen Zweck (DSG) nicht das Gleiche ist wie eine mit diesem Zweck vereinbare Datenbearbeitung (E-DSG), spricht eine grammatikalische Auslegung dafür, dass neu die Bearbeitung zu kompatiblen Bearbeitungszwecken möglich ist.

Kompatible Bearbeitungszwecke stehen mit dem Grundsatz der Erkennbarkeit im Zusammenhang[75]. Nach dem geltenden DSG bedarf eine Bearbeitung zu neuen Zwecken bereits deshalb der Rechtfertigung, weil sie mit einem Verstoss gegen den Grundsatz der Erkennbarkeit verbunden ist[76]. Da die Erkennbarkeit gemäss dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auch in gestufter Form erfolgen kann, scheint auch dieses Problem lösbar zu sein, indem die Bearbeitungszwecke bei der Beschaffung nicht abschliessend spezifiziert werden müssen und eine detaillierte Information zu den kompatiblen Zwecken nachträglich erfolgen kann. Die Einführung kompatibler Bearbeitungszwecke führt folglich in Kombination mit den gelockerten Anforderungen an die Erkennbarkeit dazu, dass die Anforderungen an den Detaillierungsgrad der ursprünglich bekanntgegebenen Information sinken. Diese Neuerung stellt eine Erleichterung für PIMS dar.

e) Datenrichtigkeit

Nach dem Grundsatz der Richtigkeit von Personendaten ist der Inhaber der Datensammlung verpflichtet, sich über die Korrektheit der bearbeiteten Personendaten zu vergewissern und angemessene Massnahmen zu treffen, um unrichtige Daten zu berichtigen oder zu löschen (Art. 5 Abs. 1 DSG). Bei PIMS dürften die Daten im Normalfall von der betroffenen Person selbst stammen oder die betroffene Person wird zumindest die Übertragung der Daten von einem Dritten selbst veranlasst haben. Falls die Daten nicht richtig sein sollten, ist zwar grundsätzlich von einer Verletzung dieses Grundsatzes auszugehen. Diese wird aber aufgrund einer konkludenten Einwilligung in aller Regel gerechtfertigt sein[77].

---

72 Botschaft DSG 2017, BBl 2017 6941, 7024 f.

73 ROSENTHAL, Jusletter vom 20. Februar 2017, Rn. 24. In der EU muss eine Relativierung der Rechtmässigkeit mit dem Grundsatz der Zweckbindung koordiniert werden, da eine Personendatenbearbeitung stets alle Grundsätze nach Art. 5 DSGVO einhalten muss und die Rechtsmässigkeit der Bearbeitung (Art. 5 Abs. 1 lit. a DSGVO) nur einer dieser Grundsätze ist (HEBERLEIN, DSGVO 5 N 46).

74 PLATH, DSGVO 6 N 32; HEBERLEIN, DSGVO 4 N 42 f.

75 HEBERLEIN, DSGVO 4 N 46.

76 BAERISWYL, DSG 4 N 43; siehe auch MEIER, Rn. 702; HEBERLEIN, DSGVO 5 N 21.

77 Siehe dazu hinten B.4.2.3.

f) Datensicherheit

Der Grundsatz der Datensicherheit erfordert, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSG). Dieser Grundsatz wird durch die Verordnung zum Bundesgesetz über den Datenschutz (VDSG) dahingehend konkretisiert, dass der Datenbearbeiter für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten sorgen muss (Art. 8 Abs. 1 VDSG).

Der Datenbearbeiter muss sicherstellen, dass einerseits Personendaten intern gesetzeskonform bearbeitet werden und andererseits Dritte die Personendaten nicht missbrauchen können[78]. Die erforderlichen Massnahmen beurteilen sich nach einem relativen Massstab. Zu beachten sind dabei das Risiko einer Persönlichkeitsverletzung bei der betroffenen Person, der Zweck der Datenbearbeitung, die Art der bearbeiteten Daten und der Umfang der Datenbearbeitung[79]. Eine absolute Sicherheit wird nicht vorausgesetzt[80]. Erforderlich ist eine Risikoanalyse anhand verschiedener Kriterien, namentlich Zweck, Art und Umfang der Bearbeitung, Risiken für betroffene Personen und Stand der Technik (Art. 8 Abs. 2 VDSG). Der Inhaber einer Datensammlung ist gemäss Art. 9 VDSG verpflichtet, besondere Kontrollmassnahmen zu treffen: Unbefugte Personen dürfen keinen Zugang zu Einrichtungen oder automatisierten Datenverarbeitungssystemen haben, in denen Personendaten bearbeitet werden, und auch keine Datenträger lesen, kopieren, verändern oder entfernen. Bei der Bekanntgabe von Personendaten ist ebenso unberechtigtes Lesen, Kopieren, Verändern oder Löschen der Daten zu verhindern. Berechtigte Personen dürfen zudem nur zu denjenigen Daten Zugang haben, die sie zur Aufgabenerfüllung benötigen. Aufgrund letztgenannter Verpflichtungen muss überprüfbar sein, wer welche Manipulationen an den Daten vorgenommen hat, die in einem automatisierten System gespeichert sind.

Technische Massnahmen hängen direkt mit dem Informationssystem zusammen[81] und umfassen beispielsweise die Verschlüsselung (sowohl Speicherung als auch Übertragung), Zugriffsverwaltung, Protokollierung und Back-ups[82]. Weder das DSG noch die VDSG schreiben jedoch spezifische technische Lösungen vor[83]. Bei PIMS dürften technische Massnahmen im Vordergrund stehen. Organisa-

---

78 SHK-BAERISWYL, DSG 7 N 13; EPINEY, § 9 N 51; MEIER, Rn. 786; sinngemäss auch BSK-STAMM-PFISTER, DSG 7 N 7 f.; ROSENTHAL, DSG 7 N 7.

79 SHK-BAERISWYL, DSG 7 N 23; EPINEY, § 9 N 53; BSK-STAMM-PFISTER, DSG 7 N 9; BUNDESAMT FÜR JUSTIZ, Kommentar, Abs. 6.1.1.

80 SHK-BAERISWYL DSG 7 N 22; BSK-STAMM-PFISTER, DSG 7 N 9; EPINEY, § 9 N 53; BUNDESAMT FÜR JUSTIZ, Kommentar, Abs. 6.1.1.

81 EDÖB, Leitfaden Massnahmen, 5; BSK-STAMM-PFISTER, DSG 7 N 11; BAERISWYL, DSG 7 N 19.

82 SHK-BAERISWYL DSG 7 N 19; EPINEY, § 9 N 56; ROSENTHAL, DSG 7 N 8; EDÖB, Leitfaden Massnahmen, *passim*.

83 BUNDESAMT FÜR JUSTIZ, Kommentar, Abs. 6.1.1; Lediglich subsidiär, wenn präventive Massnahmen keinen genügenden Schutz versprechen, schreibt Art. 10 VDSG die Protokollierung der beim Inhaber der Datensammlung vorgenommenen automatisierten Datenbearbeitung vor.

torische Massnahmen, also Organisationstruktur und Prozesse des Bearbeiters[84], sind dennoch nicht zu vernachlässigen. Als Orientierungshilfe wird teilweise auf internationale Standards verwiesen (z.B. ISO 27001, ISO 27002, COBIT, BSI 100-1, BSI 100-2, BSI 100-3 und BSI 100-4)[85].

Im E-DSG wird die bestehende Regelung zur Datensicherheit weitgehend übernommen. Im Vergleich zum VE-DSG findet sich die Ergänzung, dass die ergriffenen Massnahmen es ermöglichen müssen, Verletzungen der Datensicherheit zu vermeiden (Art. 7 Abs. 2 E-DSG). Es dürfte sich hierbei um die Präzisierung einer Selbstverständlichkeit handeln. Neu ist hingegen das Konzept des Datenschutzes durch Technik („Privacy by Design"). Der Verantwortliche, nicht jedoch der Auftragsdatenbearbeiter[86], hat schon in der Planung die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften, insbesondere die Grundsätze der Datenbearbeitung, eingehalten werden (Art. 6 E-DSG).

Dem Grundsatz der Datensicherheit kommt für PIMS aus mehreren Gründen eine zentrale Bedeutung zu. Zum einen speichern die Kunden von PIMS bei diesen regelmässig sehr grosse Mengen an Personendaten, im Idealfall gar alle sie betreffenden Personendaten. Entsprechend ist die Sicherheit dieser Dienste für die betroffenen Personen fundamental. Zum andern sind PIMS aufgrund der verfügbaren Datenmengen (zumindest bei einer relevanten Durchsetzung von PIMS in der Praxis) ein attraktives Ziel für Hacker.

Diesem Risiko kann einerseits durch die Art der Datenspeicherung begegnet werden. Die zentrale Speicherung ist heute weit verbreitet. Alleine in den letzten Monaten hat sich jedoch in einer Vielzahl von Fällen gezeigt, dass dieses Modell grosse Gefahren birgt (z.B. Equifax[87], Adult Friend Finder[88]). Zentrale Speicher sind ein bei Hackern beliebter Angriffspunkt, da in diesem Fall nur ein Ziel gehackt werden muss, um Zugriff auf den gesamten Datenpool zu erhalten. Bei einer dezentralen Speicherung müssten hingegen verschiedene Ziele separat angegriffen werden, was für Hacker weniger attraktiv ist. Allerdings ist anzumerken, dass eine dezentrale Speicherung technisch anspruchsvoller ist[89].

---

84 SHK-BAERISWYL, DSG 7 N 20; BSK-STAMM-PFISTER, DSG 7 N 11; EPINEY, § 9 N 56; siehe auch EDÖB, Leitfaden Massnahmen, *passim*.

85 SHK-BAERISWYL, DSG 7 N 37; BSK-STAMM-PFISTER, DSG 7 N 21.

86 So schon Art. 18 VE-DSG; ROSENTHAL, Jusletter vom 20. Februar 2017, Rn. 11.

87 Anfang September 2017 wurde bekannt, dass beim US-Finanzdienstleister Equifax Daten von 143 Millionen US-Kunden gestohlen wurden, darunter auch sensitive Daten wie Sozialversicherungsnummern. Siehe dazu GRESSIN.

88 Im Jahr 2016 wurden bei einem Angriff auf Adult Friend Finder Daten und Passwörter von über 400 Millionen Nutzerkonten entwendet. Die Passwörter waren in diesem Fall mit einem leicht zu entschlüsselnden Algorithmus verschlüsselt. Siehe dazu WHITTAKER, AdultFriendFinder network hack exposes 412 million accounts.

89 Zudem sind bei dezentraler Speicherung z.B. Analysen des gesamten Datenpools komplizierter.

Im Zentrum der Massnahmen zur Gewährleistung der Datensicherheit dürften bei PIMS insbesondere die Verschlüsselung der Daten und die sichere Verwahrung der Schlüssel stehen. Dabei stehen verschiedene Verschlüsselungsalgorithmen zur Verfügung, die heute einen angemessenen Schutz garantieren. Entscheidend dürfte daher sein, dass die Schlüssel sicher und getrennt von den verschlüsselten Daten aufbewahrt werden. Die optimale Lösung wäre, wenn nur der Nutzer die Schlüssel hätte und diese selbst lokal aufbewahren würde. In diesem Fall könnte jedoch der PIMS-Anbieter nicht mehr auf die Daten zugreifen. Zudem wäre es dem Nutzer überlassen, sich um die Aufbewahrung der Schlüssel zu kümmern, was technisch nicht versierten Nutzern nur bedingt zuzumuten ist.

Weiter ist auch der Einsatz zusätzlicher Schutzmassnahmen wie Firewalls oder Proxy Servern wichtig, um einen angemessenen Schutz sicherzustellen. Hackerattacken können mit diesen Mitteln weiter erschwert werden. Sofern API[90] eingerichtet werden, sind auch die entsprechenden Schnittstellen angemessen zu schützen.

4.2.3. Rechtfertigung durch Einwilligung

a) Grundsatz

An sich kann davon ausgegangen werden, dass Anbieter von PIMS bemüht sein werden, die Grundsätze der Datenbearbeitung einzuhalten. Gelingt dies vollumfänglich, ist ihre Tätigkeit nach Massgabe des DSG ohne weiteres zulässig. Zumindest grundsätzlich wäre es also denkbar, dass PIMS Personendaten ohne Einwilligung der betroffenen Personen bearbeiten könnten, sofern es sich nicht um besonders schützenswerte Personendaten[91] oder Persönlichkeitsprofile handelt, die nicht ohne Rechtfertigungsgrund bekanntgegeben werden dürfen (Art. 12 Abs. 2 lit. c DSG). In der Realität wird die Bearbeitung von Personendaten durch PIMS aber wohl immer auf der Einwilligung der Nutzer beruhen.

Eine Verletzung der Datenbearbeitungsgrundsätze kann durch Einwilligung des Verletzten, durch überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt werden (Art. 13 DSG). Während das Bundesgericht früher betonte, dass eine Rechtfertigung grundsätzlich nur sehr zurückhaltend anzunehmen sei[92], was zumindest einem Teil der Lehre widersprach[93], fehlen solche

---

90 Application program interface, bzw. Programmierschnittstelle; Fungiert als Bindeglied unterschiedlicher Soft- oder Hardware-Komponenten. Im Internet dienen APIs häufig der Verbindung unterschiedlicher Webanwendungen (sog. Mashups).

91 Dies sind nach Art. 3 lit. c DSG Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Informationen über Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen.

92 BGE 136 II 508, E. 5.2.4; BGE 138 II 346, E. 7.2.

93 Siehe ROSENTHAL, DSG 12 N 23, der eine Rechtfertigung als immer möglich bezeichnet; zum Ganzen auch SCHÄFER/DORDI, medialex 2011, 146 f.

pauschalen Feststellungen in jüngeren Entscheiden[94]. Eine ausdrückliche Praxisänderung ist aber nicht erfolgt. Sinnvoll erschiene, nach den verletzten Bearbeitungsgrundsätzen zu differenzieren[95]. Insbesondere eine Verletzung des Grundsatzes der Datensicherheit lässt sich wohl nur in Ausnahmefällen rechtfertigen, weil ohne Gewährleistung der Datensicherheit die Wirksamkeit des Datenschutzes insgesamt in Frage gestellt wäre. Ein anderer Ansatz bestünde darin, nach den Rechtfertigungsgründen zu differenzieren. Gerade wenn man bedenkt, dass das DSG die informationelle Selbstbestimmung schützen will, muss die Einwilligung als Ausdruck einer selbstbestimmten Entscheidung jede Bearbeitung zu rechtfertigen vermögen[96]. Liegt eine gültige Einwilligung vor, ist die hierauf gestützte Datenbearbeitung folglich zulässig[97].

Da PIMS die Personendaten in den meisten Fällen von den betroffenen Personen selbst oder zumindest mit deren Zustimmung übermittelt erhalten, kann sich ihre Tätigkeit in aller Regel auf eine ausdrückliche oder zumindest konkludente Einwilligung stützen. Voraussetzung ist allerdings, dass eine gültige Einwilligung vorliegt.

Die Einwilligung ist gültig, wenn sie freiwillig erfolgt und die betroffene Person vorgängig angemessen über die Bearbeitung informiert wurde (sog. *informed consent*, Art. 4 Abs. 5 DSG). Eine freiwillige Einwilligung liegt vor, wenn sie ohne Druck abgegeben wird[98].

b) Form

Die Einwilligung lässt sich grundsätzlich formfrei erteilen. In der Übermittlung der Daten an PIMS kann wohl eine konkludente Einwilligung zur Bearbeitung dieser Daten gesehen werden. Namentlich ist die Übermittlung der eigenen persönlichen Daten auf ein PIMS auch dahingehend zu verstehen, dass der PIMS-Anbieter die Richtigkeit dieser Daten nicht sicherstellen muss[99]. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen, die im Bereich von PIMS oft vorliegen dürften, muss die Einwilligung jedoch ausdrücklich erfolgen (Art. 4 Abs. 5 DSG). In Lehre und Rechtsprechung ist umstritten, ob sich „ausdrücklich" auf die Form der Kundgabe der Einwilligung oder auf das Informieren der betroffenen Person bezieht[100]. Folgt man der zweiten Ansicht, ist der einwilligenden Person der in Frage stehende Datenbearbeitungsvorgang klar darzu-

---

94 Siehe z.B. BGE 142 III 263, E.2.2, wo bemerkenswerterweise eine Persönlichkeitsverletzung bejaht wurde; anders jedoch BVGer vom 18. April 2017, A-4232/2015, E. 5.4.2.1.

95 Siehe aber BUNDESAMT FÜR JUSTIZ, Auslegungshilfe, 2, wonach eine solche Differenzierung im Ständerat vorgeschlagen, aber verworfen wurde.

96 Ebenso: ROSENTHAL, DSG 12 N 19; BSK-RAMPINI, DSG 13 N 3.

97 Ebenso: ROSENTHAL, DSG 12 N 19; BSK-RAMPINI, DSG 13 N 3; siehe auch BUNDESAMT FÜR JUSTIZ, Auslegungshilfe, 2.

98 EPINEY, § 9 N 18; FASNACHT, Rn. 274; AEBI-MÜLLER, Rn. 765; BSK-MAURER-LAMBROU/STEINER, DSG 4 N 16f.

99 Ebenso ROSENTHAL, DSG 5 N 11; BSK-MAURER-LAMBROU/SCHÖNBÄCHLER, DSG 5 N 12.

100 FASNACHT, Rn. 303; VASELLA, Jusletter vom 16. November 2015, Rn. 26 f.; ROSENTHAL, Jusletter vom 20. Februar 2017, Rn. 30 ff.; BVGer vom 18. April 2017, A-4232/2015, E. 5.4.1, verlangt eine „explizite" Einwilligung.

legen, sie kann dann aber einwilligen, ohne auf diesen Datenverarbeitungsvorgang ausdrücklich Bezug zu nehmen. In der Praxis wird dieses Erfordernis kaum ein Problem darstellen, da der Wille in der Regel ausdrücklich kundgegeben wird, insbesondere durch das Anwählen von Boxen oder das Anklicken von Buttons.

c) Angemessene Information (*informed consent*)

Gemäss Rechtsprechung und Lehre ist die Information angemessen, wenn die betroffene Person gestützt darauf die Konsequenzen ihrer Einwilligung abzuschätzen vermag[101]. Die Information kann sich aus verschiedenen Elementen zusammensetzen, so u.a. aus Gegenstand, Zweck und Umfang der beabsichtigten Datenbearbeitung, Datenbearbeiter und allfälligen besonderen Risiken[102]. Die Einwilligung muss sich dabei nicht auf eine konkrete Persönlichkeitsverletzung beziehen, sondern es kann auch in die Inkaufnahme eines Risikos eingewilligt werden[103]. Welche Informationen erforderlich sind und in welchem Detaillierungsgrad diese vorliegen müssen, lässt sich nur im Einzelfall beantworten.

Bei der Nutzung von PIMS dürfte die Zustimmung der betroffenen Person in den meisten Fällen sämtliche Prozesse der Datenbearbeitung abdecken. Dies ist insbesondere dann der Fall, wenn die betroffene Person selbst über die gespeicherten Daten bestimmt und selbst entscheidet, mit welchen Diensteanbietern sie diese zu welchem Zweck teilt. In einem solchen Fall ist es Sache des jeweiligen Datenbearbeiters, die Bearbeitungsgrundsätze einzuhalten und insbesondere über den Zweck aufzuklären.

Gerade für die Forschung wäre es hingegen interessant, wenn betroffene Personen gewisse Daten im Voraus für spezifische Nutzungen freigeben könnten, ohne dass eine konkrete Bearbeitung vorgesehen ist. In diesem Fall würde der Nutzer die Rahmenbedingungen für die Datenbearbeitung im Voraus definieren, ohne im Moment der Zustimmung zu wissen, wer die Daten später tatsächlich nutzt. Naheliegend wäre in diesem Fall, dass der PIMS-Anbieter die Absichten des Datenbearbeiters und den Zweck der Datenbearbeitung überprüft. Heute wird ein solcher Generalkonsens zum Teil als ungültig qualifiziert[104], da die Folgen für die betroffene Person nicht abschätzbar seien. Nach anderer Ansicht genügt es aber, wenn die Einwilligung „in der einen oder anderen Weise“ bezüglich Person

---

101 BVGer vom 30. März 2011, A-7040/2009, E. 10.5.1; BSK-RAMPINI, DSG 13 N 4; NOUREDDINE, Rz. 3.103–3.134, Rz. 3.128; EPINEY, § 9 N 17; ROSENTHAL, DSG 4 N 72; SHK-BAERISWYL, DSG 4 N 59; eingehend FASNACHT, Rn. 255.

102 Siehe BVGer vom 30. März 2011, A-7040/2009, E. 10.5.1; BSK-MAURER-LAMBROU/STEINER, DSG 4 N 16f; BSK-RAMPINI, DSG 13 N 4; NOUREDDINE, Rz. 3.103–3.134, Rz. 3.128; EPINEY, § 9 N 17; ROSENTHAL, DSG 4 N 72 ff.

103 AEBI-MÜLLER, Rn. 228, mit dem Beispiel der Einwilligung in das Risiko einer leichten Körperverletzung im Zusammenhang mit einer sportlichen Betätigung.

104 BSK-MAURER-LAMBROU/STEINER, DSG 4 N 16f; BSK-RAMPINI, DSG 13 N 5; FASNACHT, Rn. 324.

des Bearbeiters, Art der Daten, Zweck der Bearbeitung oder Bearbeitungsform begrenzt ist[105]. Berücksichtigt man, dass Forschungsergebnisse kaum direkte Konsequenzen für die betroffene Person haben und die Einwilligung jederzeit widerrufen werden kann[106], sollte es zulässig sein, Personendaten allgemein zum Zweck der Forschung zur Verfügung zu stellen[107].

d) Widerruf

Eine einmal gültig erteilte Einwilligung ist jederzeit frei und grundsätzlich ohne Begründung[108] widerrufbar. Der Widerruf bewirkt, dass die laufenden und zukünftigen Datenbearbeitungen nicht mehr durch die Einwilligung gerechtfertigt werden können. Die vor dem Widerruf durchgeführten Datenbearbeitungen bleiben vom Widerruf aber unberührt[109]. Da Personendaten Persönlichkeitsgüter sind, die nicht zum Kernbereich der menschlichen Existenz gehören, können sie grundsätzlich Gegenstand unwiderruflicher vertraglicher Bindungen sein, sofern die wirtschaftlichen Interessen des Datensubjekts im Vordergrund stehen[110]. Ob bei bestehender vertraglicher Bindung ein Widerruf der Einwilligung zulässig bzw. die vertragliche Bindung übermässig i.S.v. Art. 27 ZGB ist, muss anhand der Umstände des Einzelfalls beurteilt werden. Zu berücksichtigen sind die betroffenen Personendaten, die Dauer der Bindung sowie allfällige finanzielle Entgelte[111]. Erfolgt der Widerruf zu Unzeit, können dem Datenbearbeiter aber Schadenersatzansprüche geschuldet sein[112].

Bei PIMS ist davon auszugehen, dass die Einwilligung jederzeit widerrufen werden kann. Zwar wäre an sich denkbar, dass PIMS den Widerruf der Einwilligung ihrer Nutzer in den Nutzungsbedingungen ausschliessen. Eine solche Vereinbarung ist aber kaum zu erwarten, weil sie dem Grundgedanken von PIMS, der Stärkung der informationellen Selbstbestimmung, widersprechen würde. Überdies erscheint fraglich, ob ein Ausschluss des Widerrufs gültig wäre, weil die Dauer der Nutzung der Daten durch PIMS in der Regel zeitlich nicht beschränkt ist und PIMS meist auch keine eigenen finanziellen Interessen verfolgen.

4.2.4. Auskunftsrecht

Das Auskunftsrecht vermittelt jeder Person das Recht, vom Inhaber einer Datensammlung Auskunft darüber zu erhalten, ob Daten über sie bearbeitet werden (Art. 8 Abs. 1 DSG). Verpflichtet ist nicht

---

105 ROSENTHAL, DSG 13 N 4.

106 BSK-RAMPINI, DSG 13 N 14; SHK-WERMELINGER, DSG 13 N 7; ROSENTHAL, DSG 4 N 104; FASNACHT, Rn. 323.

107 THOUVENIN, Big Data, 47.

108 AEBI-MÜLLER, Rn. 214 Fn. 554.

109 ROSENTHAL, DSG 4 N 104; SHK-WERMELINGER, DSG 13 N 7; FASNACHT, Rn. 326; AEBI-MÜLLER, Rn. 214.

110 BGE 136 III 401, E. 5.2.2; BSK-RAMPINI, DSG 13 N 14.

111 Siehe BSK-RAMPINI, DSG 13 N 14.

112 ROSENTHAL, DSG 4 N 105, m.H. auf Art. 404 Abs. 2 OR; AEBI-MÜLLER, Rn. 214 Fn. 555, gemäss der das negative Interesse zu ersetzen sei.

jeder Bearbeiter der Daten, sondern nur der Inhaber der entsprechenden Datensammlung[113]. Führen mehrere Inhaber gemeinsam eine Datensammlung, kann das Auskunftsbegehren gegenüber jedem Inhaber geltend gemacht werden (Art. 1 Abs. 2 VDSG). Der Inhaber der Datensammlung muss der betroffenen Person dabei nicht nur den Zweck und die Rechtsgrundlage des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger bekannt geben (Art. 8 Abs. 2 lit. b DSG), sondern auch – und dies vor allem – die in der Datensammlung über diese Person vorhandenen Daten (Art. 8 Abs. 2 lit. a DSG). Dies bedeutet, dass die betroffene Person gegenüber dem Inhaber der Datensammlung in der Regel einen Anspruch auf Herausgabe der sie betreffenden Daten – konkret: einer Kopie der Daten – hat (Art. 8 Abs. 5 DSG)[114]. Eine mündliche Auskunft soll gemäss Art. 1 Abs. 3 VDSG nur mit Einwilligung des Datensubjekts möglich sein. Die Auskunft hat in der Regel kostenlos zu erfolgen (Art. 8 Abs. 5 DSG).

Dem Auskunftsrecht kommt für PIMS eine doppelte Bedeutung zu. Zum einen müssen PIMS in der Lage sein, dem Auskunftsrecht zu genügen, ihren Kunden also auf Anfrage alle erforderlichen Angaben zu machen und eine Kopie ihrer Daten herauszugeben. Zum andern – und dies vor allem – ist das Bestehen des Auskunftsrechts Voraussetzung für das Funktionieren von PIMS, weil die Kunden von PIMS ihre Daten regelmässig mithilfe des Auskunftsrechts von anderen Datenbearbeitern beziehen und in einem PIMS zusammenführen werden. Dem Auskunftsrecht kommt für PIMS damit eine zentrale Bedeutung zu. Je nach Ausgestaltung und Auslegung dieses Rechts lässt sich das Betreiben von PIMS massgeblich erleichtern oder erschweren. Wird das Auskunftsrecht etwa so verstanden, dass es dem Berechtigten nur einen Anspruch auf eine Fotokopie, nicht aber auf Herausgabe einer elektronischen Version seiner Daten vermittelt[115], wird dieser kaum in der Lage sein, die bei einem bestimmten Diensteanbieter gespeicherten Personendaten auf ein PIMS zu übertragen. Durch eine weite Auslegung des Auskunftsrechts, die etwa auch das Zurverfügungstellen der Daten in einem standardisierten Format oder über ein API umfassen würde, könnte das Betreiben von PIMS dagegen massgeblich vereinfacht werden.

Das Auskunftsrecht gemäss Art. 23 E-DSG knüpft nicht an die Inhaberschaft einer Datensammlung an, sondern verpflichtet jeden Verantwortlichen im Sinne von Art. 4 lit. i DSG[116]. Der Verantwortliche hat über alle Informationen Auskunft zu geben, die zur Geltendmachung von Rechten nach dem E-

---

113 WIDMER M., Datensubjekte, Rz. 5.11.

114 BGE 123 III 534, E. 3; BGE 141 III 119, E. 6.2; GRAMIGNA/MAURER-LAMBROU, DSG 8 N 48; EPINEY/FASNACHT § 11 N 35; GNEHM, 93 ff.; WIDMER M., Datensubjekte, Rz. 5.24; RUDIN, DSG 8 N 49; zurückhaltend ROSENTHAL, DSG 8 N 25, der einen Ausdruck in Textform genügen lässt und einen Anspruch auf Herausgabe einer elektronischen Kopie nur bejaht, wenn nicht ausdruckbare Metadaten ebenfalls vom Auskunftsanspruch erfasst sind. Diese Unterscheidung ist im digitalen Kontext allerdings problematisch, weil Personendaten hier ohne einen Bezugspunkt in Form von Metadaten meistens unverständlich sind. Siehe dazu auch vorne B.4.2.4.

115 Siehe dazu hinten C.3.3.2.c).

116 Entgegen der Botschaft DSG handelt es sich nicht nur um eine redaktionelle Anpassung, da der Kreis der Verpflichteten neu gezogen wird, BBl 2017 6941, 7066.

DSG erforderlich sind und eine transparente Datenbearbeitung gewährleisten (Art. 23 Abs. 2 E-DSG). Es werden mindestens folgende Informationen mitgeteilt: Identität und Kontaktdaten des Verantwortlichen, bearbeitete Personendaten, Zweck der Bearbeitung, Aufbewahrungsdauer, verfügbare Angaben über Herkunft der Daten, falls diese nicht von der verantwortlichen Person erhoben wurden, automatisierte Einzelentscheidungen und deren Logik, Empfänger und Kategorien von Empfängern, denen Personendaten bekanntgeben werden. Der Grundsatz, dass die Auskunft in der Regel schriftlich in Form eines Ausdrucks zu erteilen ist, wurde bereits im VE-DSG gestrichen.

4.2.5. Melde- und Informationspflichten

Das Datenschutzgesetz sieht eine ausdrückliche Informationspflicht bei der Beschaffung von Personendaten für Private nur dann vor, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile betroffen sind (Art. 14 Abs. 1 DSG). Diese Pflicht trifft nur den Inhaber einer Datensammlung nach Art. 3 lit. g DSG, wenn er Daten in diese aufnehmen will[117], wobei die Qualifikation von PIMS als Datensammlung im Einzelfall vorzunehmen wäre[118]. Bundesorgane trifft dagegen bei der Beschaffung sämtlicher Personendaten eine Informationspflicht (Art. 18a Abs. 1 DSG). Es muss über Inhaber der Datensammlung, Zweck des Bearbeitens und die Kategorien der Datenempfänger informiert werden, sofern eine Datenbekanntgabe vorgesehen ist (Art. 14 Abs. 2 und Art. 18a Abs. 2 lit. a, b und c DSG).

Bundesorgane müssen auf das Auskunftsrecht nach Art. 8 DSG und auf die Folgen einer Weigerung der Bekanntgabe hinweisen, wenn die betroffene Person zur Bekanntgabe verpflichtet sein sollte (Art. 18a Abs. 2 lit. d und e DSG). Für das Bestehen einer Informationspflicht ist sowohl bei Privaten als auch bei Bundesorganen grundsätzlich irrelevant, ob die Daten beim Datensubjekt selbst oder bei Dritten beschafft werden (Art. 14 Abs. 1 und Art. 18a Abs. 1 DSG *in fine*). Die Informationspflicht besteht aber nicht bei jeder erneuten Beschaffung. Wenn das Datensubjekt bereits früher informiert wurde, ist eine erneute Information nur nötig, wenn sich inzwischen Inhaber der Datensammlung, Zweck oder Kategorien der Datenempfänger geändert haben[119]. Die Verletzung dieser Informationspflichten ist für Private strafbewehrt (Art. 34 Abs. 1 DSG i.V.m. Art. 14 Abs. 1 und 2 DSG).

Da PIMS die Daten in der Regel beim Datensubjekt erheben, können sie dieses schon beim Beschaffen der Daten informieren. Eine erneute Information wird nur nötig, wenn die Daten im PIMS neuen Empfängern oder den bisherigen Empfängern zu anderen Zwecken bekanntgegeben werden. Letztere Konstellationen werden im Verlaufe des Informationslebenszyklus der bei PIMS gespeicher-

---

117 WIDMER M., Personendaten, Rz. 4.12; BSK-RAMPINI/FUCHS, DSG 14 N 4; SHK-WERMELINGER, DSG 14 N 4.

118 Siehe dazu vorne B.4.2.1.

119 WIDMER M., Personendaten, Rz. 4.25, Rz. 4.40; EPINEY/FASNACHT, § 11 N 9; SHK-WERMELINGER, DSG 14 N 10; BSK-RAMPINI/FUCHS, DSG 14 N 16, N 18.

ten Daten häufig vorkommen. Diesen Informationspflichten sollte aber mit vernünftigem Aufwand Genüge getan werden können, gerade wenn PIMS über eine App mit dem Datensubjekt interagieren.

Gemäss Art. 11a Abs. 2 und 3 DSG führt der EDÖB ein Register von sämtlichen durch Bundesorgane geführten Datensammlungen sowie denjenigen Datensammlungen Privater, die Persönlichkeitsprofile oder besonders schützenswerte Personendaten enthalten oder aus denen regelmässig Personendaten bekanntgegeben werden. Die entsprechenden Datensammlungen sind dem EDÖB zu melden, bevor sie eröffnet werden (Art. 11a Abs. 4 DSG). Allerdings gibt es zahlreiche Ausnahmen von der Meldepflicht, die in Art. 11 Abs. 5 DSG sowie Art. 4 VDSG für Private und Art. 18 VDSG für Bundesorgane geregelt sind. Nennenswert sind das Entfallen der Meldepflicht bei der Ernennung eines unabhängigen Datenschutzbeauftragten, der die Einhaltung des DSG überwacht und ein Verzeichnis der Datensammlungen führt (Art. 11a Abs. 5 lit. e DSG), sowie bei der Zertifizierung durch eine unabhängige Zertifizierungsstelle (Art. 11a Abs. 5 lit. f DSG). Der EDÖB muss dann aber über die Ernennung des Datenschutzbeauftragten bzw. das Ergebnis der Zertifizierung informiert werden[120].

Da PIMS, selbst wenn sie keine Persönlichkeitsprofile oder besonders schützenswerten Daten bearbeiten, regelmässig Personendaten an Dritte bekanntgeben, müssen PIMS ihre Datensammlungen beim EDÖB registrieren, sofern sie sich nicht zertifizieren lassen oder einen unabhängigen Datenschutzbeauftragten bestellen.

Eine allgemeine Informationspflicht bei der Bearbeitung von Personendaten ist im DSG nicht explizit vorgesehen. Eine solche allgemeine Informationspflicht wird aber z.T. aus dem Grundsatz der Datenbearbeitung nach Treu und Glauben (Art. 4 Abs. 2 DSG) hergeleitet. Das Datensubjekt ist gemäss dieser Ansicht daher über eine Datenbearbeitung zu informieren, wenn dies von einem loyalen und vertrauenswürdigen Datenbearbeiter erwartet werden dürfte[121]. Eine solche Pflicht wird vor allem bei Datenpannen bejaht, bei denen eine „*Data Breach Notification*“ an die betroffenen Datensubjekte sowie an betroffene Dritte zu erfolgen habe[122].

Diese aus Treu und Glauben hergeleitete Informationspflicht bei Datenpannen gilt auch für PIMS. Bei PIMS könnte zudem eine schwere Datenpanne bei Diensteanbietern die berechtigte Erwartung wecken, dass der PIMS-Anbieter als loyaler Datenbearbeiter die betroffenen Datensubjekte über die Panne informiert. Der PIMS-Anbieter müsste in einer solchen Konstellation vertraglich sicherstellen, dass er vom Diensteanbieter eine entsprechende „*Data Breach Notifcation*“ erhält. Diese Problematik könnte umgangen werden, wenn der Diensteanbieter die Daten nur auf der PIMS-Infrastruktur zu nicht personenbezogenen Zwecken analysieren darf. Die Datenpanne beim Diensteanbieter wäre

---

120 WIDMER M., Personendaten, Rz. 4.110 f.; BSK-EHRENSPERGER/BELSER, DSG 11a N 16a, N 16i.

121 EPINEY/NÜESCH, N 3.73; NOUREDDINE, Rz. 3.71; siehe auch: BVGer vom 27. Mai 2009, A-3144/2008, E.9.3.

122 KLEINER/STOCKER, digma 2015, 90; vgl. SHK-BAERISWYL, DSG 4 N 18.

dann für die im PIMS gespeicherten Daten ohne Folge, da keine Personendaten der Datensubjekte betroffen wären.

Die Informations- und Meldepflichten werden in Art. 17-22 E-DSG deutlich erweitert. Insbesondere wird eine Meldepflicht für Verletzungen der Datensicherheit in Art. 22 E-DSG ausdrücklich geregelt[123]. Die Auftragsdatenbearbeiter haben dem Verantwortlichen jegliche Verletzungen der Datensicherheit zu melden (Art. 22 Abs. 3 E-DSG). Der Verantwortliche hat eine solche Verletzung wiederum dem EDÖB zu melden (Art. 22 Abs. 1 E-DSG). Eine Information der betroffenen Person erfolgt grundsätzlich nur auf Veranlassung des EDÖB oder wenn es zum Schutz der betroffenen Person notwendig sein sollte (Art. 22 Abs. 4 E-DSG)[124]. Eine Meldung an Dritte ist nicht vorgesehen.

Nach Art. 17 E-DSG müssen den Datensubjekten diejenigen Informationen mitgeteilt werden, die erforderlich sind, damit sie Rechte nach dem E-DSG geltend machen können und eine transparente Datenbearbeitung gewährleistet ist. Informiert werden muss dabei namentlich über Identität und Kontaktdaten des Verantwortlichen, Bearbeitungszweck, Empfänger bzw. Kategorien von Empfängern und Staaten, in welche die Daten bekanntgegeben werden. Die Information erfolgt direkt bei der Beschaffung oder, wenn die Daten bei Dritten beschafft wurden, innert eines Monats seit Empfang der Daten. Zudem ist in bestimmten Konstellationen eine Pflicht zur Meldung an den EDÖB vorgesehen, wenn Personendaten ohne Einwilligung des Datensubjekts in ein Land bekannt gegeben werden, das keinen angemessen Datenschutz gewährleistet (Art. 14. Abs. 2 E-DSG)[125]. Diese Informationspflichten werden kritisiert, weil sie – anders als in Art. 14 DSGVO – nicht abschliessend aufgezählt sind[126].

Die datenschutzrechtlichen Informationspflichten treffen PIMS nur, wenn sie als Datenbearbeiter zu qualifizieren sind. Werden PIMS als rein technische Infrastruktur ausgestaltet und fallen sie damit nicht in den Anwendungsbereich des DSG, werden nicht die PIMS, wohl aber die Diensteanbieter, welche die in PIMS gespeicherten Daten nutzen, regelmässig zur Information verpflichtet sein. Da Diensteanbieter von dieser Pflicht befreit werden, wenn die betroffenen Personen bereits über die erforderlichen Informationen verfügen (Art. 18 Abs. 1 lit. a E-DSG), ist denkbar, dass Diensteanbieter auf eine vertragliche Regelung hinwirken werden, welche die PIMS zur Übermittlung der Informationen verpflichtet.

---

123 Zu den Meldepflichten gemäss Vorentwurf: BERANEK ZANON, Jusletter vom 2. Oktober 2017, *passim*.

124 Zum Vorentwurf KLEINER, digma 2017, 172; VASELLA/SIEVERS, digma 2017, 46 f.

125 Bei einer Bekanntgabe ins Ausland sind besondere Bestimmungen zu beachten. Je nach Konstellation stellen sich unterschiedliche Fragen, auf die hier jedoch nicht einzugehen ist. Arbeiten PIMS mit ausländischen Diensteanbietern oder sonstigen ausländischen Dienstleistern (z.B. Cloud Service Providern) zusammen, ist diesen Bestimmungen Rechnung zu tragen.

126 ROSENTHAL, Jusletter vom 27. November 2017, Rn. 99.

4.3. Haftungsrecht

PIMS-Anbieter unterstehen gewissen Haftungsrisiken, die sich aus dem Umstand ergeben, dass Dritte, hier also die Nutzer von PIMS, Daten auf ihrer Infrastruktur speichern. In aller Regel ist dieser Vorgang zwar unproblematisch. Es ist aber denkbar, dass Inhalte gespeichert werden, die gegen objektives Recht verstossen oder Rechte Dritter verletzen. In diesem Fall stellt sich die Frage, ob und gegebenenfalls inwiefern die PIMS-Anbieter für solche Rechtsverletzungen einstehen müssen. Diese Frage wird meist unter dem Titel der „Provider-Haftung" diskutiert[127].

Die Frage der Provider-Haftung ist in der Schweiz – anders als in den Mitgliedstaaten der EU[128] – nicht gesetzlich geregelt und entsprechend umstritten. Das Bundesgericht hat mit seiner Rechtsprechung bisher nur beschränkt zur Klärung beitragen können[129] und in einem jüngeren Entscheid ausdrücklich darauf hingewiesen, dass der Gesetzgeber gefordert sei[130]. Der Bundesrat ist in seinem Bericht vom 11. Dezember 2015 über die zivilrechtliche Verantwortlichkeit von Providern allerdings zum Schluss gekommen, dass eine allgemeine gesetzliche Regelung der Provider-Haftung nicht angezeigt sei[131]. Die Rechtslage ist deshalb weiterhin recht unklar, was für die PIMS-Anbieter – je nach Art des PIMS – zu gewissen Haftungsrisiken führen kann.

Ein Verstoss gegen objektives Recht ist bei PIMS vor allem denkbar, wenn die Nutzer von PIMS auf deren Infrastruktur Daten speichern, die gegen die Vorgaben des Strafrechts verstossen. Zu denken ist etwa an pornografische Inhalte im Sinn von Art. 197 Abs. 4 StGB (sog. harte Pornografie) oder, sofern der PIMS-Anbieter davon weiss oder es annehmen muss, an Daten, die unbefugt beschafft wurden, wie z.B. abgehörte oder aufgenommene Gespräche (Art. 179bis und Art. 179ter StGB) oder aufgenommene Inhalte aus dem Geheim- oder Privatbereich (Art. 179^{quater} StGB). Das Risiko, dass derartige Daten tatsächlich auf PIMS gespeichert werden, erscheint allerdings als gering.

Ein Verstoss gegen Rechte Dritter kann namentlich vorliegen, wenn die von den Kunden von PIMS gespeicherten Daten Persönlichkeits- und Urheberrechte verletzen. Bei den Persönlichkeitsverletzungen dürfte das Recht am eigenen Bild im Vordergrund stehen. Dieses ist verletzt, wenn eine Person ohne ihre Zustimmung abgebildet wird oder das Bild ohne Zustimmung der abgebildeten Person oder

---

127 Zur sog. Provider-Haftung siehe namentlich: RIGAMONTI, sic! 2016, 117–134; ROSENTHAL, Haftung, 150–206; DERS., sic! 2006, 511–519; SCHOCH/SCHÜEPP, Jusletter vom 13. Mai 2013; KERNEN, Jusletter vom 4. März 2013; HÜRLIMANN, *passim*; FRECH, *passim*; ROHN, *passim*; SCHMIDT-GABAIN, sic! 2017, 451–467.

128 Siehe dazu: Art. 12 ff. Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, („Richtlinie über den elektronischen Geschäftsverkehr"), sog. E-Commerce-RL.

129 BGE 141 III 513, E. 5.3; BGer vom 14. Januar 2013, 5A_792/2011, E. 6.2 f.; ferner: BGer, sic! 2015, 571 ff., E. 4. Zur strafrechtlichen Haftung siehe auch: BGer vom 2. Mai 2008, 6B_645/2007 und 6B_650/2007, E. 7.3.4.4.2.

130 BGer vom 14. Januar 2013, 5A_792/2011, E. 6.3.

131 BUNDESRAT, Bericht zivilrechtliche Verantwortlichkeit von Providern, 4.

in einem anderen Kontext, als dem welchem die abgebildete Person zugestimmt hat, veröffentlicht wird[132]. Denkbar wäre zudem, dass die Persönlichkeitsrechte Dritter verletzende Informationen auf PIMS gespeichert werden, namentlich Informationen aus deren Geheim-, Intim- oder Privatsphäre wie etwa Gendaten oder Angaben über die Gesundheit. Soweit die Handlungen allerdings nicht über das blosse Speichern von Informationen auf einem PIMS hinausgehen, dürfte es in aller Regel an einer Persönlichkeitsverletzung fehlen. Dieser Grundsatz gilt auch für Informationen aus der Geheim-, Intim- oder Privatsphäre[133]. Ein Haftungsrisiko wird für PIMS deshalb nur bestehen, wenn Dritte Zugriff auf diese Informationen erhalten. In solchen Fällen steht es der in ihrer Persönlichkeit verletzten Person offen, gegen jeden vorzugehen, der an der Verletzung mitwirkt (Art. 28 Abs. 1 ZGB)[134], also auch gegen den PIMS-Anbieter.

Im Gegensatz zum Persönlichkeitsrecht reicht bei urheberrechtlich geschützten Inhalten das blosse Speichern auf einem PIMS für das Vorliegen einer Verletzung aus, weil es sich dabei um eine Vervielfältigung im Sinn von Art. 10 Abs. 2 lit. a URG handelt. Im Vordergrund steht auch hier das Speichern von Bildern, an denen Urheberrechte Dritter bestehen. Dies dürfte nach dem E-URG regelmässig der Fall sein, da neu alle Fotografien dreidimensionaler Objekte urheberrechtlich geschützt sein sollen, selbst wenn sie keinen individuellen Charakter haben (Art. 2 Abs. 3bis E-URG). Das blosse Speichern von Bildern durch einen Kunden auf einem PIMS kann zwar wohl regelmässig als Privatgebrauch unter Beizug eines Dritten (Art. 19 Abs. 1 lit. a i.V.m. Art. 19 Abs. 2 URG) qualifiziert werden. Diese Schranke greift aber nicht mehr, wenn die urheberrechtlich geschützten Inhalte durch ein PIMS in urheberrechtlich relevanter Weise genutzt oder Dritten zugänglich gemacht werden. Auch hier hat der Rechteinhaber die Möglichkeit, direkt gegen den Betreiber des PIMS vorzugehen.

4.4. Medizinrecht

Software kann unter Umständen als Medizinprodukt im Sinne von Art. 1 Medizinprodukteverordnung zu qualifizieren sein. Sofern dies zutrifft, ist eine Vielzahl gesundheitsrechtlicher Bestimmungen zu beachten (u.a. HMG, MepV, HFG, VKlin, Richtlinie 93/42/EWG über Medizinprodukte[135]).

Sofern ein Angebot nur die Speicherung, Archivierung und Kommunikation von Daten umfasst, gilt es allerdings nicht als Medizinprodukt[136]. Gemäss einem Merkblatt von Swissmedic liegen bspw. in folgenden Fällen keine Medizinprodukte vor: Software und Apps im Bereich Fitness, Wohlbefinden und Ernährung; Software bzw. Apps zur statistischen Auswertung von klinischen oder epidemiologischen

---

132 BSK-MEILI, ZGB 28 N 19, N 21; HAUSHEER/AEBI-MÜLLER, Rz. 13.28, Rz. 13.30; BGE 127 III 481, E. 3a.aa.

133 Bei sensiblen Daten kritisch dazu HAUSHEER/AEBI-MÜLLER, Rz. 12.136

134 Zur weiten Auslegung dieses Begriffs siehe BSK-MEILI, ZGB 28 N 37; HAUSHEER/AEBI-MÜLLER, Rz. 14.07; BGE 141 III 513, E. 5.3.1; BGer vom 6. Mai 2015, 5A_658/2014, E. 4.2.

135 Siehe für eine ausführliche Liste SWISSMEDIC, 1 f.

136 EUROPÄISCHE KOMMISSION, Guidelines, 11; SWISSMEDIC, 3.

Studien oder Registern; elektronische Patientendaten, die lediglich papierene Gesundheitsdaten ersetzen; allgemeine nicht-personalisierte medizinische Informationen[137].

Es ist deshalb davon auszugehen, dass PIMS nur als Medizinprodukte zu qualifizieren wären, wenn sie umfangreiche gesundheitliche Analysemöglichkeiten anbieten würden, die über eine rein statistische Auswertung (grafische Darstellung, Mittelwertberechnung etc.) hinausgehen. Dies könnte beispielsweise zutreffen, wenn das PIMS gestützt auf die gespeicherten Nutzerdaten individuelle Krankheitsprognosen erstellt[138]. Dies dürfte hingegen nicht der Fall sein, wenn die Analyse ausserhalb des PIMS stattfindet und lediglich das Resultat im PIMS gespeichert bzw. angezeigt wird.

5. Fördermassnahmen

5.1. Datenportabilität

Das Funktionieren von PIMS hängt wesentlich von der Möglichkeit der Datensubjekte ab, ihre Daten mit wenig Aufwand einem PIMS zur Verfügung stellen zu können. Eine Übertragung der „eigenen" Daten auf PIMS ist zwar schon auf Grundlage des heutigen Auskunftsrechts möglich[139]. Allerdings besteht nach geltendem Recht keine Verpflichtung, Daten direkt an Dritte, hier also an PIMS, zu übertragen oder diese in einem standardisierten Format und/oder über ein API zur Verfügung zu stellen. Eine entsprechende Regelung – sei es durch den Ausbau des Auskunftsrechts oder durch die Einführung einer spezifischen Regelung zur Datenportabilität[140] – dürfte für den Erfolg von PIMS zentral sein[141]. Entsprechend können bestehende PIMS und neue Angebote durch die Einführung einer Regelung zur Datenportabilität erheblich gefördert werden.

Die Einführung eines Datenportabilitätsrechts dürfte für den Durchbruch von PIMS zwar eine zentrale, aber nicht die alleinige Voraussetzung sein. Denn für zahlende Diensteanbieter hängt der Nutzen von PIMS ganz direkt von der Zahl der PIMS-Nutzer ab[142]. Entscheidend wird deshalb sein, dass PIMS genügend grosse Mengen an qualitativ hochwertigen Daten in ihren Beständen halten, um für die Diensteanbieter eine echte Alternative zu etablierten Akteuren zu sein. Hierzu müsste eine grosse Anzahl von Nutzern ihr Portabilitätsrecht tatsächlich wahrnehmen. Die von der EU befragten Akteure

---

137 SWISSMEDIC, 4.

138 Siehe dazu KLETT, HAVE 2017, 106.

139 Siehe dazu vorne C.3.3.2.

140 Siehe dazu hinten C.5.

141 Die EU Kommission geht davon aus, dass die Ausgestaltung der Datenportabilität zu beobachten sei (EUROPÄISCHE KOMMISSION, Personal information management services, 13 f.) während der Europäische Datenschutzbeauftragte PIMS als hoffnungsvolle „default" Implementation der Datenportabilität beschreibt (EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER, Stellungnahme, 9).

142 Siehe hierzu: AUTORITÉ DE LA CONCURRENCE/BUNDESKARTELLAMT, 27; siehe dazu hinten B.5.3.1.

wünschten sich deshalb eine Informationskampagne, welche Nutzer auf ihr Portabilitätsrecht gemäss DSGVO aufmerksam macht[143].

5.2. Dateneigentum

Entgegen einer vereinzelt vertretenen Auffassung erweist sich die Einführung eines „Dateneigentums" weder als eine wirksame noch als eine sinnvolle Massnahme zur Förderung von PIMS. Denn ein solches Eigentum müsste wohl – bei Sach- ebenso wie bei Personendaten – mit der Möglichkeit zur Übertragung einhergehen. Ohne die Möglichkeit zur Übertragung der entsprechenden Rechte können solche Rechte kaum als Eigentumsrechte qualifiziert werden[144]. Ist ein solches „Dateneigentum" aber übertragbar, dann ist davon auszugehen, dass sich Diensteanbieter die Eigentumsrechte an den Daten ihrer Nutzer von diesen regelmässig übertragen lassen werden. Damit wären die Diensteanbieter in der Lage, gestützt auf ihr Eigentum die Übertragung dieser Daten an und deren Nutzung durch PIMS zu verhindern.

Neben diesem spezifischen Problem sprechen auch weitere gewichtige Gründe gegen die Einführung eines allgemeinen Dateneigentums. Zum einen enthält das geltende Recht bereits eine Vielzahl von Rechtsnormen, die es Privaten und Unternehmen ermöglichen, die Nutzung „ihrer" Daten zu erlauben oder zu verbieten. In ihrem jeweiligen Anwendungsbereich vermitteln diese Normen schon heute durchaus eigentumsähnliche Rechtspositionen. Zum andern fehlt es sowohl an einer überzeugenden theoretischen Rechtfertigung als auch an massgeblichen praktischen Problemen, die nur durch Einführung eines „Dateneigentums" gelöst werden könnten. Die Einführung eines solchen Eigentums würde zudem zahlreiche Folgeprobleme verursachen, nicht nur bei der Ausgestaltung, sondern auch bei der Implementierung eines solchen Rechts. Im Ergebnis dürfte ein „Dateneigentum" deshalb mehr Probleme schaffen als lösen[145].

5.3. Praktische Hürden und mögliche Massnahmen

5.3.1. Geringe Nutzerzahlen

Aktuell dürften die noch recht kleinen Nutzerzahlen die grösste Herausforderung für PIMS sein. Das Erreichen einer kritischen Grösse ist zentral, damit PIMS ihre Vorteile tatsächlich ausschöpfen können. Eine der Hauptursachen für die geringe Nutzung scheint schlicht die fehlende Bekanntheit zu

---

143 EUROPÄISCHE KOMMISSION, Personal information management services, 13 f.

144 THOUVENIN, SJZ 2017, 28.

145 Näheres dazu: WEBER/THOUVENIN, ZSR 2018, *passim*; THOUVENIN/WEBER, Jusletter IT Flash vom 11. Dezember 2017, Rn. 10 ff.; THOUVENIN/WEBER/FRÜH, 136 f.; THOUVENIN/FRÜH/LOMBARD, SZW 2017, 33 f.; THOUVENIN, SJZ 2017, 30 ff., kritisch auch FRÖHLICH-BLEULER, Jusletter vom 6. März 2017, Rn. 31; a.M. ZECH, GRUR 2015, 1159 ff.; DERS., CR 2015, 137−146, sowie ohne vertiefte Untersuchung und nähere Begründung ECKERT, SJZ 2016, 245−249, 265−274.

sein. Eine weitere Ursache liegt sicherlich auch darin, dass viele Angebote noch am Anfang ihrer Entwicklung stehen.

Allerdings stellt sich die Frage, ob bei den Nutzern ein ausreichender Wille zur Wahrnehmung der informationellen Selbstbestimmung vorhanden ist. PIMS setzen nämlich voraus, dass sich der Nutzer aktiv und bewusst mit den eigenen Daten beschäftigt und Entscheidungen über deren Nutzung trifft. Für den Nutzer müssen somit ausreichende Vorteile durch die Nutzung von PIMS erkennbar sein, welche den zusätzlichen Aufwand rechtfertigen.

Die öffentliche Verwaltung könnte hier eine Vorbildfunktion einnehmen und Prozesse beim Umgang mit Bürgerinnen und Bürgern mittels einer E-Identity-Lösung vereinfachen. Dadurch würden die Nutzer Erfahrungen im Umgang mit solchen Systemen sammeln, was das Vertrauen gegenüber diesen Systemen stärken dürfte. Zur Stärkung des Vertrauens beitragen könnte auch ein freiwilliges Zertifizierungssystem, wie dies im Rahmen des elektronischen Patientendossiers[146] sowie des E-IDG vorgesehen ist.

5.3.2. Akzeptanz durch die Diensteanbieter

Damit ein Diensteanbieter die Daten eines Nutzers direkt über PIMS beziehen kann, muss er sein System auf das API des PIMS ausrichten, was bei einer kleinen Nutzerzahl zu einem verhältnismässig grossen Aufwand führt. Es ist deshalb davon auszugehen, dass viele Diensteanbieter sich zumindest vorerst nicht auf PIMS einlassen und Konsumenten ausschliessen werden, welche ihre Daten nicht direkt zur Verfügung stellen. Eine breite Akzeptanz für PIMS wird bei Diensteanbietern deshalb wohl erst erreicht, wenn ein PIMS-Anbieter eine ausreichende Nutzerzahl erreicht hat.

Wirksame Fördermassnahmen müssten wohl relativ weit reichen. In Betracht käme ein rechtlicher Zwang, dass Diensteanbieter eine Datenübernahme über PIMS anbieten müssen. Angesetzt werden könnte aber auch auf der Nutzerseite, indem die Eröffnung eines PIMS (ähnlich wie bei der digitalen Identität in Estland) zur Pflicht gemacht würde.

5.3.3. Technische Hürden

Für die Ausschöpfung des Potentials von PIMS ist es wichtig, dass Daten automatisiert von anderen Datenquellen importiert werden können. Hauptvoraussetzung ist, dass die Daten elektronisch verfügbar sind. Einige grosse Online-Plattformen bieten ihren Nutzern bereits heute die Möglichkeit, ihre Daten gesammelt herunterzuladen. Für Plattformen wie Facebook, Google oder Twitter, die einen solchen Download anbieten, stellt beispielsweise BitsaboutMe[147] seinen Nutzern die erforderlichen Tools zur Verfügung, um die Daten automatisiert zu übernehmen. Schwieriger gestaltet sich die Lage

---

146 Siehe dazu vorne B.3.4.

147 Siehe dazu vorne B.3.1.3.

bei Daten, die nicht als Gesamtheit zum Download zur Verfügung stehen. Mittels *Data Scraping* bestehen zwar auch in einem solchen Fall gewisse Möglichkeiten. Allerdings können dadurch meist nur diejenigen Daten erfasst werden, die dem Nutzer auf der Website der Plattform angezeigt werden. Zudem ist *Data Scraping* mit einem beträchtlichen Aufwand verbunden, weil der *Scraper* für jede neue Plattform konfiguriert werden muss, von dem Daten in das PIMS übertragen werden sollen[148]. Ausserdem besteht für die Plattform die Möglichkeit, Zugriffe durch *Scraper* zu verhindern oder zumindest zu erschweren. Hinzu kommt, dass *Data Scraping* aus rechtlicher Sicht nicht unproblematisch ist. Namentlich kann das *Scrapen* einen Verstoss gegen die Nutzungsbedingungen einer Plattform darstellen und gegen die Vorgaben des UWG verstossen[149].

Damit ein Nutzer einem Diensteanbieter Zugriff auf die im PIMS gespeicherten Daten geben kann, muss dieser die Kompatibilität seines Systems mit dem API des PIMS sicherstellen. Insoweit ist ein gewisser Aufwand des Diensteanbieters erforderlich. Allerdings wird der PIMS-Anbieter bestrebt sein, diesen Prozess zu unterstützen.

5.3.4. Interessenkonflikte

Interessenkonflikte können insbesondere dann entstehen, wenn PIMS-Anbieter durch Diensteanbieter finanziert werden, insb. durch Gebühren für die Gewährung des Zugangs zu Daten. Diese Risiken bestehen vor allem bei gewinnorientierten PIMS-Anbietern. Bis zu einem gewissen Grad kann dieser Gefahr entgegengewirkt werden, indem PIMS-Anbieter als Genossenschaften unter Einbezug der betroffenen Personen organisiert werden.

Das Risiko von Interessenkonflikten besteht ausserdem, wenn PIMS-Anbieter sich nicht auf ihre eigentliche Tätigkeit beschränken, sondern die Daten auch für eigene Forschung nutzen.

5.3.5. Datenqualität

Soweit ersichtlich geben die bestehenden PIMS-Angebote dem Nutzer die Möglichkeit, nur die von ihm genau spezifizierten Daten an einen Dritten weiterzugeben. Diese Möglichkeit ist mit Blick auf die informationelle Selbstbestimmung zu begrüssen, weil die betroffene Person selbst im Einzelnen über die Nutzung ihrer Daten bestimmen kann. Eine solche Situation könnte unter Umständen aber auch zu Problemen führen. So besteht die Gefahr einer Verfälschung von Forschungsresultaten, weil nur einzelne, gezielt ausgewählte Daten zur Verfügung gestellt werden, nicht aber der gesamte Datensatz.

---

148 Dasselbe gilt, wenn bspw. die Struktur der Website des Diensteanbieters verändert wird.

149 Siehe dazu: STAUBER, Jusletter IT Flash vom 11. Dezember 2017. Zur Unzulässigkeit von Scraping, das auch als Spidering bezeichnet wird, siehe schon BGE 131 III 384; anders nun aber KGer Freiburg, sic! 2017, 228–236.

Die Qualität der in PIMS gespeicherten Daten könnte zudem stark verbessert werden, wenn Daten beim Import in ein PIMS mit einer digitalen Signatur des ursprünglichen Diensteanbieters versehen würden. Ein Diensteanbieter, der digital signierte Daten aus einem PIMS erhalten würde, wäre so in der Lage, die Quelle der Daten zweifelsfrei festzustellen und damit die Qualität der Daten besser einzuschätzen. Eine solche Möglichkeit könnte von Diensteanbietern auf freiwilliger Basis angeboten werden. Denkbar wäre aber auch, zumindest bei bestimmten Daten eine Pflicht zur digitalen Signierung im Rahmen der Datenportabilität vorzusehen.

5.3.6. Anonymisierung

Kritisch zu hinterfragen ist die Zuverlässigkeit von Anonymisierungsmassnahmen, falls Daten anonymisiert an den Datenbearbeiter fliessen. Eine De-Anonymisierung kann bei einem Abgleich mit weiteren Datenquellen relativ einfach durchgeführt werden. Wie gross diese Gefahr tatsächlich ist, lässt sich allerdings nur im Einzelfall in Bezug auf den konkreten Datenbearbeiter abschätzen. Angesichts des Wachstums der bestehenden Datenbestände ist davon auszugehen, dass eine wirksame Anonymisierung immer schwieriger zu erreichen sein wird[150].

5.4. Kompatibilität mit internationalen Entwicklungen

Die Europäische Kommission startete im Juli 2014 eine öffentliche Online-Konsultation zu PIMS als Zukunftsvision und veröffentlichte deren Ergebnisse im November 2016 in einem Bericht[151]. PIMS wurden hierbei dadurch charakterisiert, dass sie (i) dem Nutzer Kontrolle über Zugang und Nutzung seiner Daten geben, (ii) Aussenstehende entweder einen sicheren Zugang zu den Daten erhalten oder die Analyse direkt auf der Plattform durchführen können und (iii) die Datensubjekte in irgendeiner Form am Wert ihrer Daten partizipieren[152]. Der Bericht kam zum Schluss, dass PIMS noch in einer frühen Phase der Entwicklung stehen und insbesondere der Zugang zu Kapital für viele der noch kleinen Akteure schwierig sei, was deren Fähigkeiten limitiere, etablierte Akteure zu konkurrenzieren[153]. Die von der EU Kommission befragten Akteure brachten ihre Hoffnung zum Ausdruck, dass die Einführung des Portabilitätsrechts ihrem Geschäftsmodell förderlich wäre. Sie wünschten sich daher bewusstseinsbildende Massnahmen bezüglich des Auskunfts- und Portabilitätsrechts. Datenzugangsrechte, die über sichere Schnittstellen geltend gemacht werden könnten, wurden von gewissen Akteuren als Ideallösung bezeichnet[154]. Die Kommission kam zum Schluss, dass es weitere grundlegende Recherchen, insbesondere zu den praktischen Herausforderungen des Datenportabilitätsrechts, zur Rolle der öffentlichen Hand für vertrauensbildende Massnahmen und zur Bedeu-

---

150 Siehe auch OHM, UCLA Law Review 2010, *passim*.

151 EUROPÄISCHE KOMMISSION, Personal information management services.

152 EUROPÄISCHE KOMMISSION, Personal information management services, 2 f.

153 EUROPÄISCHE KOMMISSION, Personal information management services, 18.

154 EUROPÄISCHE KOMMISSION, Personal information management services, 13 f.

tung der Einwilligung, brauche. Darüber hinaus seien praktische Massnahmen wie politischer Support, Kickstart-Förderungen oder die Unterstützung von Kollaborationen in Erwägung zu ziehen[155].

Im Oktober 2016 veröffentlichte der EDPS eine „Opinion on PIMS". Er sprach PIMS bedeutendes Potential zu, erachtete aber, wie in diesem Gutachten[156], das Erreichen einer kritischen Grösse als zentral[157]. Zudem forderte er die EU Kommission auf, im Rahmen ihrer Strategie für einen digitalen Binnenmarkt mögliche Anreize für PIMS zu prüfen, und wies darauf hin, dass E-Government-Initiativen die Popularität von PIMS fördern könnten[158]. Der EDPS selbst beschränkt sich vorerst allerdings auf Öffentlichkeitsarbeit und auf die Unterstützung von interdisziplinärer Forschung im Rahmen des Internet Privacy Engineering Network[159].

6. Erkenntnisse

PIMS sind in erster Linie als technische Infrastruktur zu betrachten. Sie dienen ihren Nutzern als Plattform für das zentralisierte Sammeln, Verwalten und Weitergeben der eigenen Daten. Die Entscheidung über die Nutzung der Daten liegt damit bei den Nutzern selbst. Die Kontrolle über die Nutzung kann dabei granular ausgeübt, mithin im Einzelnen für spezifische Nutzungen erteilt (und auch wieder entzogen) werden, bspw. für ein bestimmtes Forschungsprojekt. Das primäre Ziel von PIMS besteht darin, die informationelle Selbstbestimmung ihrer Nutzer zu gewährleisten. Zudem vermögen PIMS einen Beitrag zur Datensicherheit zu leisten und als Mittel zur Monetarisierung von Personendaten zu dienen. Der Ertrag kann dabei an die Nutzer ausgeschüttet werden oder ihnen anderweitig zugutekommen. PIMS erscheinen damit als vielversprechende Konzepte zur Verwaltung und Nutzung der eigenen Daten.

PIMS sind eine relativ junge und wenig bekannte Erscheinung. Zwar gibt es bereits einige Angebote in der Schweiz, die meisten sind aber noch in der Entwicklungs- oder Markteinführungsphase. Entsprechend ist heute kaum abzuschätzen, wie sich PIMS mittelfristig entwickeln werden. Das grösste Potential scheint derzeit bei gesundheitsrelevanten Daten zu liegen. Auch wenn PIMS theoretisch und bei einer eher idealistischen Betrachtungsweise den Markt für Personendaten grundlegend verändern könnten, ist in näherer Zukunft wohl kaum mit einer solchen Entwicklung zu rechnen.

Der heutige Rechtsrahmen enthält keine namhaften Hindernisse für die Entwicklung von PIMS. Im Vordergrund steht die Beachtung der Vorgaben des Datenschutzrechts. Diese sollten aber in aller Regel ohne weiteres einzuhalten sein, zumal die Bearbeitung von Personendaten durch PIMS stets

---

155 EUROPÄISCHE KOMMISSION, Personal information management services, 19.

156 Siehe dazu vorne B.5.3.1.

157 EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER, Stellungnahme, 13.

158 EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER, Stellungnahme, 14.

159 EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER, Stellungnahme, 14; siehe dazu vorne B.3.3.3.

auf der Einwilligung der betroffenen Personen beruht. Darüber hinaus bestehen gewisse, aber eher geringe Haftungsrisiken, die sich daraus ergeben, dass sich PIMS für das Speichern rechtswidriger Inhalte nutzen lassen.

Die grösste Herausforderung besteht darin, dass der Erfolg von PIMS unmittelbar von einer ausreichend grossen Nutzerzahl abhängt. Dies ist heute noch nicht der Fall, in erster Linie wohl mangels Bekanntheit von PIMS und wegen der fehlenden Sensibilisierung der betroffenen Personen. Bleiben die Nutzerzahlen gering, dürften PIMS mittelfristig nur schwer zu finanzieren sein. Will man PIMS fördern, stehen zwei Mittel im Vordergrund: Kampagnen zur Förderung der Bekanntheit und die Einführung eines Rechts auf Datenportabilität, das es den (potentiellen) Nutzern erlaubt, ihre Daten mit möglichst geringem Aufwand von den heutigen Diensteanbietern auf PIMS zu übertragen.

C. DATENPORTABILITÄT

1. Fragestellungen

Mit diesem Gutachten ist eine Reihe von Fragen zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht zu beantworten. Diese Fragen werden nachfolgend im Einzelnen untersucht und beantwortet, wenn auch nicht in der im Auftrag vorgesehenen Reihenfolge.

Gemäss Auftrag soll das Gutachten auf Personendaten fokussieren. Der Begriff der Personendaten ergibt sich als Regelungsgegenstand des Datenschutzrechts aus der Legaldefinition des DSG. Erfasst sind alle Daten, welche eine Person identifizieren oder es erlauben, durch weitere Vorkehren die Identifikation vorzunehmen (Art. 3 lit. a DSG). Die Umschreibung ist damit relativ weit. Das Gutachten beschränkt sich aber nicht auf das DSG bzw. E-DSG, sondern analysiert auch weitere Normenkomplexe, welche im Kontext der Personendaten relevant sind.

Hingegen sind die Sachdaten nicht Gegenstand des Gutachtens. Hinzuweisen ist indessen auf die Tatsache, dass die Datenportabilität bei Sachdaten eine ebenso erhebliche Bedeutung haben kann. Ein bekanntes Beispiel betrifft die Vertriebskette in der Automobilindustrie; der Garagist wird gegebenenfalls eine Reparatur nicht auszuführen in der Lage sein, wenn ihm gewisse Daten des Automobilherstellers nicht bekannt sind[160].

[160] Zu Ideen, solche Situationen mit Datenzugangsrechten zu entschärfen, siehe sogleich die Entwicklungen im europäischen Recht, C.2.1.

2. Überblick zu den datenrelevanten Rechtsentwicklungen im Ausland

Bevor auf die einzelnen Aspekte der möglichen Schaffung und Ausgestaltung eines Datenportabilitätsrechts eingegangen wird, erscheint ein Blick auf datenrelevante Rechtsentwicklungen im Ausland sinnvoll. Zur Sprache kommen die Europäische Union, Frankreich, die Vereinigten Staaten und Japan.

2.1. Europäische Union (EU)

Die Frage nach der Einführung gesetzlicher Vorschriften zur Portabilität von Personendaten steht im Kontext weiterer Regulierungen zur rechtlichen Behandlung von Daten. Zu erwähnen sind insbesondere die Aktivitäten der Europäischen Kommission zum Datenzugang, zur Portabilität von Sachdaten und zur Portabilität von Online-Inhalten. Der Stand der europäischen Diskussion ist wie folgt:

- Die Europäische Kommission hat am 10. Januar 2017 ein Diskussionspapier veröffentlicht, das sich nicht nur der Frage des Dateneigentums, sondern auch der Frage des Datenzugangs widmet[161]; die Ausarbeitung entsprechender normativer Vorschriften einschliesslich eines Systems von Zwangslizenzen wird mit diesem Dokument zur Diskussion gestellt. Die Datenportabilität im engeren Sinne wird hingegen nicht thematisiert.
- Am 13. September 2017 hat die Europäische Kommission einen Entwurf für eine Verordnung zum freien grenzüberschreitenden Fluss von Sachdaten in der Europäischen Union vorgelegt[162]. Art. 6 des Entwurfs sieht eine Bestimmung zu „Porting of Data" vor. Angeordnet wird indessen nicht ein zwingendes Recht auf Portabilität von Sachdaten; die Kommission will vielmehr die Industrie ermutigen, Verhaltensrichtlinien zu entwickeln, welche den Wechsel von Internetanbietern erleichtern sollen. Die Diskussion dieses Vorschlags bleibt abzuwarten; die Schweiz hat bisher keine Aktivitäten in diese Richtung unternommen.
- Die Europäische Kommission hat am 10. Januar 2017 einen Entwurf für eine E-Privacy-Verordnung veröffentlicht, die gemäss Erwägungsgrund 12 jede Kommunikation zwischen Maschinen dem Grundsatz der Vertraulichkeit unterstellen will[163].
- Das Europäische Parlament und der Rat haben am 14. Juni 2017 eine Verordnung zur grenzüberschreitenden Portabilität von Online-Inhalten verabschiedet[164]. Die Verordnung räumt das Recht ein, über Online-Bezahldienste (wie z.B. Netflix oder Spotify) abonnierte oder gekaufte Dienste und Inhalte (etwa Musik, Filme oder Spiele) innerhalb der ganzen EU auf dem Wege des

---

161 EUROPÄISCHE KOMMISSION, Aufbau einer europäischen Datenwirtschaft; EUROPÄISCHE KOMMISSION, Commission staff working document.

162 EUROPÄISCHE KOMMISSION, Vorschlag für eine Verordnung über freien Verkehr nicht personenbezogener Daten.

163 EUROPÄISCHE KOMMISSION, Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation.

164 Verordnung (EU) 2017/1128 des europäischen Parlaments und des Rates vom 14. Juni 2017 zur grenzüberschreitenden Portabilität von Online-Inhaltediensten im Binnenmarkt.

Streaming oder des Herunterladens nutzen zu können. Insbesondere soll damit das Geoblocking verhindert werden. Die Anbieter von Online-Inhaltsdiensten sind gegenüber Abonnenten, die sich vorübergehend in einem anderen EU-Mitgliedstaat aufhalten, verpflichtet, den Zugriff auf die gleiche Inhalte-Palette wie im Heimatland zu gewährleisten.

- Die EU hat die für Finanzdienstleister relevante Richtlinie über Zahlungsdienste im Binnenmarkt (sog. *Payment Services Directive 2;* PSD 2) überarbeitet und auf den 12. Januar 2016 in Kraft gesetzt[165]. Die Umsetzungsfrist läuft bis zum 13. Januar 2018[166]. Ein wesentliches Element der PSD 2 besteht darin, dass bisher nicht regulierte Zahlungsauslösedienste und Kontoinformationsdienste reguliert werden, sie dafür aber im Gegenzug objektiven, nicht diskriminierenden und verhältnismässigen Zugang zu Zahlungssystemen sowie zu bei Kreditinstituten geführten Konten erhalten (Art. 35 und 36 PSD 2)[167]. Dieses Datenzugangsrecht mittels Schnittstellenöffnung wird begleitet von detaillierten Vorgaben zur Legitimation und zur Authentifizierung sowie zum Umfang der bekanntgegebenen Daten und war Gegenstand intensiver Diskussionen[168].

Aufgrund der vorliegenden (auf Portabilitätsrechte an Personendaten beschränkten) Fragestellung wird auf diese Entwicklungen nicht weiter eingegangen.

2.2. Frankreich

Im Rahmen einer ehrgeizigen Digitalstrategie hat Frankreich ein neues Gesetz, die „*Loi pour une République numérique*“[169] erlassen. Das Gesetz wurde auf der Grundlage einer breit angelegten Vernehmlassung ausgearbeitet[170] und soll dafür sorgen, dass Frankreich im Bereich der digitalen Technologien auf europäischer Ebene eine Vorreiterrolle einnimmt. Das Gesetz hat im Wesentlichen drei Pfeiler: Daten- und Wissenstransfer, Verbraucherschutz in der digitalen Gesellschaft und Zugang zu digitalen Diensten. Der zweite Teil zum Verbraucherschutz in der digitalen Gesellschaft sieht in Art. 48 ein Recht auf Datenherausgabe und Datenportabilität vor[171]. Die Bestimmung ergänzt den

---

165 Richtlinie (EU) 2015/2366 des europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt.

166 LUTZ, ZVglRWiss 2017, 184.

167 LUTZ, ZVglRWiss 2017, 185.

168 TRÜEB/KEISER, 171 f.; zur Diskussion des autonomen Nachvollzuges der PSD 2 im Schweizer Recht: FERBER MICHAEL, Schweizer Banken warnen vor neuen EU-Regeln zu Online-Zahlungen, NZZ online, 15. November 2017, <https://www.nzz.ch/finanzen/schweizer-banken-warnt-vor-neuen-eu-regeln-zu-online-zahlungen-ld.1328751>, zuletzt besucht am 20. Dezember 2017.

169 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (sog. „Loi Lemaire“).

170 Loi pour une République numérique, Dossier de Presse, 10. Oktober 2016, <https://www.republique-numerique.fr/media/default/0001/02/da09b380f543bfab2d13da7424cec264dca669c6.pdf>, zuletzt besucht am 20. Dezember 2017; RÉPUBLIQUE NUMÉRIQUE, Explanatory Memorandum, erhältlich unter <https://www.republique-numerique.fr/pages/digital-republic-bill-rationale>, zuletzt besucht am 20. Dezember 2017; zum Ergebnis der Vernehmlassung, siehe <http://www.republique-numerique.fr/consultations/projet-de-loi-numerique/consultation/consultation/opinions/section-2-portabilite-des-donnees/article-12-portabilite-des-donnees>, zuletzt besucht am 20. Dezember 2017.

171 Section 2: Portabilité et récupération des données.

Code de la consommation[172]. Der persönliche Anwendungsbereich ist deshalb auf Ansprüche von Verbrauchern beschränkt[173]. Art. 48 soll 2018 gleichzeitig mit der DSGVO in Kraft treten[174].

Für das Recht auf Portabilität von Personendaten verweist das französische Gesetz pauschal auf Art. 20 DSGVO. Für die Portabilität von Sachdaten stellt es aber eigene und recht detaillierte Regeln auf[175]. Erfasst werden namentlich Daten, die von Verbrauchern selbst online gestellt wurden[176] und Daten, die sich aus der Verwendung eines Nutzerkontos ergeben – es sei denn, der Wert der Daten sei durch den Diensteanbieter massgeblich erhöht worden[177]. Das Kriterium der Wertsteigerung soll im Rahmen der Ausführungsverordnung näher umschrieben werden[178]. Auf dem Verordnungsweg können darüber hinaus weitere Daten genannt werden, die mit dem Nutzerkonto im Zusammenhang stehen und dem Portabilitätsrecht unterliegen[179].

Die Herausgabe der Sachdaten muss kostenlos erfolgen und den Diensteanbietern werden Vorgaben gemacht, wie die Daten bereitzustellen sind[180]. Soweit ersichtlich ist – für Personen- und Sachdaten – nur ein Herausgabeanspruch an den Verbraucher selbst, nicht aber an Dritte vorgesehen[181].

Für Sachdaten sieht das Gesetz zudem eine *de minimis*-Regel vor, um kleinere Unternehmen vor unverhältnismässigen Umsetzungskosten zu schützen. Massgeblich sind die Nutzerzahlen des jeweiligen Dienstes. Die Grenzwerte werden gegenwärtig ausgearbeitet und in der Ausführungsverordnung publiziert[182].

---

172 „Récupération et portabilité des données“. In seiner definitiven Fassung modifiziert Art. 48 den verbraucherschutzrechtlichen Abschnitt betreffend „Contrats de services de communications électroniques“ im Kapitel „Règles spécifiques à des contrats ayant un objet particulier“ unter dem Titel „Règles de formation et d'exécution de certains contrats“, im zweiten Buch „Formation et exécution des contrats“. Der Begriff „services de communications électroniques“, reicht gem. der zuständigen Ministerin AXELLE LEMAIRE sehr weit und umfasst auch „services numériques“, d.h. digitale Dienste generell, Discussion de l'article 21 de la Loi pour une République numérique, 2e Séance de l'Assemblée nationale du 21 janvier 2016, 483.

173 Im Entwurf reichte der Anwendungsbereich noch weiter und umfasste auch juristische Personen, COMMISSION DES AFFAIRES EUROPÉENNES, 39.

174 Siehe <https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=ED84EE504FC721E9822A4C1472E7BD84.tplgfr28s_3?idArticle=LEGIARTI000033205186&cidTexte=LEGITEXT000033205014&dateTexte=20171222>, zuletzt besucht am 20. Dezember 2017.

175 Art. L. 224-42-3 Loi Lemaire.

176 Art. L. 224-42-3 al. 1 Loi Lemaire.

177 Art. L. 224-42-3 al. 2 Loi Lemaire: „De toutes les données résultant de l'utilisation du compte d'utilisateur du consommateur et consultables en ligne par celui-ci, à l'exception de celles ayant fait l'objet d'un enrichissement significatif par le fournisseur en cause“.

178 Art. L. 224-42-3 al. 3 Loi Lemaire.

179 Art. L. 224-42-3 al. 3 *in fine* Loi Lemaire.

180 Art. L. 224-42-3 Loi Lemaire.

181 Art. L. 224-42-1 Loi Lemaire.

182 Art. L. 224-42-4 Loi Lemaire; DIRECTION DES AFFAIRES JURIDIQUES, 4; siehe auch den Zeitplan für die Einführung des Gesetzes, <https://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=5E28899619F442FD98680867B45FE2D0.tplgfr32s_1?idDocument=JORFDOLE000031589829&type=echeancier&typeLoi=&legislature=14>, zuletzt besucht am 20. Dezember 2017.

2.3. Vereinigte Staaten (USA)

Die USA kennen kein umfassendes Datenschutzgesetz, sondern ein keineswegs kohärentes System von sektorspezifischen Regelungen, die von Bundesstaaten oder als Selbstregulierung erlassen werden[183]. Die Obama-Regierung hat aber verschiedene MyData-Initiativen ins Leben gerufen[184]. So wurde zusammen mit Akteuren aus der Privatwirtschaft ein Portal für Veteranen geschaffen, welches ihnen ermöglicht, ihre Gesundheitsdaten einzusehen und herunterzuladen (Blue Button Initiative[185]). Weitere solche Initiativen bestehen für Daten über den Energieverbrauch, Sozialversicherungsdaten, Konsumentendaten, im Bildungsbereich sowie für Studentendarlehensinformationen[186]. Die Idee der MyData-Initiativen ist es, dass private Akteure sachgerechte Applikationen zur Visualisierung und Organisation dieser Daten anbieten[187]. Im September 2016 führte das Office of Science and Technology Policy (OSTP) eine Konsultation zur Datenportabilität durch[188]. Die Reaktionen fielen gemischt aus und das OSTP beliess es bei der Feststellung, dass die Datenportabilität ein Entwicklungsgebiet sei[189].

2.4. Japan

Japan kennt zurzeit kein allgemeines Recht auf Datenportabilität[190]. Immerhin wurde die Portabilität von Mobiltelefonnummern durch das Ministerium für Inneres und Kommunikation sichergestellt[191]. Eine Studiengruppe der Japan Fair Trade Commission kam indessen kürzlich zum Schluss, dass verschiedene Aspekte der Wettbewerbsrelevanz grosser Datenbestände noch genauer untersucht werden müssten. Besonderes Augenmerk verdienten insbesondere das Risiko einer Oligopol- bzw. Monopolbildung im Zusammenhang mit digitalen Plattformen, aber auch das Risiko, dass etablierte Player auf Lock-In-Effekte setzen, um Wettbewerbern und Abnehmern einen Wechsel zu erschweren[192]. Die Studiengruppe hielt fest, dass die Gefahr einer Verfestigung von Machtpositionen bestehe, solange keine Portabilität von Personendaten für spezifische Dienstleistungen vorhanden sei. Daher sei es wünschenswert, entsprechende Regelungen zu treffen[193]. Die bereits 2015 verabschiedete Revision des Datenschutzgesetzes sieht allerdings kein Datenportabilitätsrecht vor[194].

---

183 HECKENDORN URSCHELER/ARONOVITZ/CURRAN/DRUCKMAN, 55; HARASGAMA, 74 f.

184 HONEY/CHROUSOS/BLACK, *passim*.

185 <https://www.healthit.gov/patients-families/your-health-data>, zuletzt besucht am 20. Dezember 2017.

186 HONEY/CHROUSOS/BLACK, *passim*.

187 Siehe auch: OFFICE OF EDUCATIONAL TECHNOLOGY, MyData Open Data Specification.

188 MACGILLIVRAY/SHAMBAUGH, *passim*.

189 MACGILLIVRAY, *passim*.

190 HECKENDORN URSCHELER/ARONOVITZ/CURRAN/DRUCKMAN, 30.

191 JITSUZUMI, 11.

192 JAPAN FAIR TRADE COMMISSION, 16, 23.

193 JAPAN FAIR TRADE COMMISSION, 27: „For example (...) as for services including SNSs with which lock-ins can occur, the power to control the service market is likely to be maintained unless the portability of personal

3. Datenportabilitätsregeln im geltenden Recht

3.1. Ausdrückliche Anordnung

3.1.1. Überblick

Der Grundsatz der Datenportabilität ist im geltenden DSG nicht verankert. Der Bundesrat hat im Bericht von 2011 zu den sozialen Medien die Datenportabilität angesprochen, ohne aber konkrete Lösungen zu thematisieren[195]. In seinem Bericht zum Vorentwurf für ein neues DSG vom 21. Dezember 2016 hat der Bundesrat kurz begründet, weshalb er im Gegensatz zur EU auf eine Regelung der Datenportabilität verzichten will[196]. Der Entwurf zum DSG vom 15. September 2017 hält an dieser Beurteilung fest[197]. Denn nach Ansicht des Bundesrates stehen bei der Datenportabilität die Wiederverwendung von Daten und damit die Idee der Wettbewerbsförderung im Vordergrund, weshalb ein entsprechendes Recht problematisch sei. Zudem setze Datenportabilität voraus, dass sich die betroffenen Verantwortlichen auf Datenträger und Informatikstandards einigen und sei sehr kostenintensiv[198].

Die Schweiz befindet sich mit dem Verzicht auf die Schaffung von Datenportabilitätsrechten in Einklang mit den bisherigen Regelungen in anderen Ländern. Wie das Gutachten zum Datenschutzrecht des Instituts für Rechtsvergleichung (Lausanne) von 2016 aufgezeigt hat, kommt das Datenportabilitätsrecht im EU-Ausland kaum vor[199]; von den untersuchten Ländern (Argentinien, Japan, Neuseeland, Singapur, Südkorea, USA) verfügt einzig Argentinien über einzelne verbraucherorientierte Spezialnormen, die dazu berechtigen könnten, die Übertragung von Daten zu verlangen[200]. Eine weitere Ausnahme bildet die EU-Datenschutz-Grundverordnung (DSGVO), die ein spezifisches Datenportabilitätsrecht einführt (Art. 20 DSGVO). Die EU-Mitgliedstaaten sind verpflichtet, dieses direkt anwendbare Recht innerstaatlich durchzusetzen[201].

---

data with respect to a specific service is ensured. Therefore, taking some sort of policy measures is desirable."

194 HECKENDORN URSCHELER/ARONOVITZ/CURRAN/DRUCKMAN, 25 ff., insb. 30.

195 BUNDESRAT, Bericht Social Media, 34 ff.; BENHAMOU/TRAN, sic! 2016, 586.

196 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, 22.

197 Botschaft DSG, BBl 2017 6941, 6982, 6984 f.

198 Botschaft DSG, BBl 2017 6941, 6984 f.

199 HECKENDORN URSCHELER/ARONOVITZ/CURRAN/DRUCKMAN, 6 ff., 60.

200 HECKENDORN URSCHELER/ARONOVITZ/CURRAN/DRUCKMAN, 17 f.

201 Für die Umsetzung in Frankreich siehe vorne C.2.2.

3.1.2. Datenportabilität gemäss Artikel 20 DSGVO

Bei den Arbeiten an der DSGVO war die Regelung der Datenportabilität ein umstrittener Punkt. Mit Blick auf die nachfolgenden Ausführungen zur Ausgestaltung eines Portabilitätsrechts im DSG[202] ist namentlich der Berichtsentwurf des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des EU Parlaments (sog. Albrecht-Bericht) zu erwähnen, welcher die Datenportabilität zusammen mit dem Recht auf Datenzugang in Art. 15 DGSVO regeln wollte. Begründet wurde dieser Ansatz damit, dass das Recht auf Datenportabilität lediglich eine Spezifizierung des Rechts auf Datenzugang sei[203]. Dieser Ansatz konnte sich im politischen Prozess allerdings nicht durchsetzen. Stattdessen wurde das Recht auf Datenportabilität in einer spezifischen Norm geregelt. Das in Art. 20 DSGVO vorgesehene „Recht auf Datenübertragbarkeit" weist insbesondere die folgenden Elemente auf:

a) Herausgabe und „direkte" Portabilität

Die betroffene Person kann verlangen, dass die Daten sowohl an die betroffene Person selbst als auch an einen Dritten übermittelt werden. Im ersten Fall hat die betroffene Person das ausdrückliche Recht, die erhaltenen Daten sogleich an einen Dritten zu übertragen. Der zweite Fall, d.h. die direkte Übermittlung der Daten von einem Datenbearbeiter auf einen Dritten, ist nach dem Wortlaut des Gesetzes davon abhängig, dass dies technisch machbar ist (Art. 20 Abs. 2 DSGVO).

b) Erfasste Daten

Hinsichtlich der vom Portabilitätsrecht erfassten Daten bezieht sich Art. 20 DSGVO auf die den Berechtigten „betreffenden personenbezogenen Daten". Demgemäss lässt sich das Datenpaket nicht auf wesentliche Profildaten (z.B. Name, Alter, Wohnort, E-Mail-Adresse, Foto) beschränken, sondern müsste angesichts des weiten Verständnisses des Begriffs grundsätzlich alle Informationen enthalten, die sich auf eine identifizierte oder identifizierbare Person beziehen. Die Artikel-29-Gruppe[204] schliesst in ihrer Stellungnahme („*Guidelines on the right to data portability*") sogar die Meta- und Rohdaten mit ein, weil sie bei der Kommunikation viel über den Nutzer verraten können und diesem erlauben, die gesamte Bedeutung der Information nachzuvollziehen[205]. Erfasst sind gemäss der Artikel-29-Gruppe auch Daten, „die durch die Nutzung eines Dienstes oder Geräts generiert bzw. erhoben werden"[206]. Dies ginge allerdings über den Wortlaut von Art. 20 DSGVO hinaus, wonach nur jene Daten erfasst sind, welche die betroffene Person selbst „einem Verantwortlichen bereit-

---

202 Siehe dazu hinten C.5.

203 EUROPÄISCHES PARLAMENT, Entwurf, 102 f.

204 Die Artikel-29-(Datenschutz)Gruppe ist ein von der Richtlinie 95/46/EG geschaffenes Gremium, das in Fragen des Datenschutzes beratende Funktion ausübt. Sie besteht aus je einem Vertreter der von den einzelnen EU-Mitgliedstaaten bestimmten Datenschutzbeauftragten, einem Vertreter des EDPS sowie einem Vertreter der EU Kommission.

205 ARTIKEL-29-GRUPPE, 18; KAMANN/BRAUN, DSGVO 20 N 25.

206 ARTIKEL-29-GRUPPE, 9 f.; KAMANN/BRAUN, DSGVO 20 N 13; a.M. KAMLAH, DSGVO 20 N 6.

gestellt“ hat[207], denn das Bereitstellen erfordert eine aktive und wissentliche Handlung[208]. Gemäss einer engen, am Wortlaut orientierten Auslegung wären jene Daten, die von Drittpersonen gesammelt werden, aber für einen Datenaustausch zur Verfügung stehen, oder solche, die aus grösseren Datenanalysen abgeleitet werden, nicht betroffen[209].

Erfasst sind sodann nur diejenigen Daten, deren Verarbeitung auf einer Einwilligung der betroffenen Person beruht, sowie Daten, deren Verarbeitung entweder für die Erfüllung eines Vertrags, deren Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Massnahmen auf Anfrage der betroffenen Person erforderlich sind (Art. 20 Abs. 1 Bst. a DSGVO). Zudem greift das Portabilitätsrecht nur, wenn die Verarbeitung mithilfe automatisierter Verfahren erfolgt (Art. 20 Abs. 1 Bst. b DSGVO). Automatisierte Verfahren können regelmässig mit computergestützten Verfahren gleichgesetzt werden, der EU Gesetzgeber hat aber bewusst einen technologieneutralen Begriff gewählt[210]. Die Einschränkung auf die Verarbeitung mithilfe automatisierter Verfahren schliesst im Wesentlichen nicht-digitale Daten vom Recht auf Datenportabilität aus, weil diese Daten nur in den seltensten Fällen mithilfe automatisierter Verfahren verarbeitet werden.

c) Format

Die Übertragung soll in einem standardisierten Format erfolgen. Die Bestimmung spricht von einem „strukturierten, gängigen und maschinenlesbaren Format“. Vorausgesetzt sind somit standardisierte Datensätze und Schnittstellen (API)[211]. Diese Vorgaben sind in der Praxis derzeit kaum erfüllt, denn die Datenbearbeiter wählen in der Regel ein Datenformat, welches auf ihre spezifischen Anforderungen ausgerichtet ist. Die technische Standardisierung ist umso bedeutender, als die Artikel-29-Gruppe die vom Datenportabilitätsrecht erfassten Daten sehr weit umschrieben hat[212].

d) Entgeltlichkeit und Weigerung

Die Datenübertragung hat unentgeltlich zu erfolgen. Der Datenbearbeiter darf also nicht nur keinen Ersatz der Kosten für den eigentlichen Übertragungsvorgang verlangen, sondern trägt grundsätzlich auch die Aufwendungen für die Bereitstellung der standardisierten Datensätze und Schnittstellen. Sofern der Verantwortliche aber beweisen kann, dass es sich um einen „offenkundig unbegründeten“ oder „exzessiven Antrag“ auf Datenportabilität handelt, darf er ein angemessenes Entgelt

---

207 PARRY, Rz. 13-015.

208 PILTZ, DSGVO 20 N 14; KAMANN/BRAUN, DSGVO 20 N 13.

209 Siehe dazu hinten C.5.2.

210 PLATH, DSGVO 2 N 6 f.

211 Siehe dazu EUROPÄISCHE KOMMISSION, Staff Working Document on the Free Flow of Data, 13; ARTIKEL-29-GRUPPE, 15 f.; COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS, 7 f.; DEUTSCHE GESELLSCHAFT FÜR MEDIZINISCHE INFORMATIK, BIOMETRIE UND EPIDEMIOLOGIE, 14 f.; WIEBE, CR 2017, 88; JANAL, JIPITEC 2017, Rn. 4, 15 f.; CONRAD, Das Recht auf Datenübertragbarkeit (Art. 20 DSGVO), *passim*.

212 ARTIKEL-29-GRUPPE, 9 f.

verlangen (Art. 20 i.V.m. Art. 12 Abs. 5 Satz 2 DSGVO)[213]. Zur Bestimmung der Angemessenheit dieses Entgelts werden die „Verwaltungskosten" der Portierung berücksichtigt[214].

Der Verantwortliche kann sich aber auch weigern, offenkundig unbegründeten oder exzessiven Anträgen nachzukommen (Art. 20 i.V.m. Art. 12 Abs. 5 Satz 2 DSGVO)[215]. Die Verhältnismässigkeit spricht jedoch dafür, dass die Weigerung im Verhältnis zur Kostenbeteiligung subsidiär ist[216].

e) Frist

Innerhalb welcher Frist die Datenübertragung zu erfolgen hat, ist in Art. 20 DSGVO nicht ausdrücklich geregelt. Es gelten die für alle Rechte der betroffenen Person anwendbaren allgemeinen Regeln von Art. 12 Abs. 3 DSGVO[217]. Demnach muss die Übertragung unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags erfolgen. Es besteht die Möglichkeit zur Verlängerung um weitere zwei Monate, allerdings muss der Verantwortliche diese innerhalb der ersten Monatsfrist begründet mitteilen.

3.1.3. Relevanz der DSGVO für Schweizer Unternehmen

Soweit Schweizer Personen und Unternehmen der DSGVO unterstehen, gilt auch für sie das Recht auf Datenportabilität (Art. 20). Der geographische Anwendungsbereich der DSGVO ist sehr weit und folgt dem sog. Auswirkungs- oder Marktortsprinzip[218]: Gemäss Art. 3 Abs. 2 DSGVO haben nicht nur Tochtergesellschaften und Zweigniederlassungen Schweizer Unternehmen in einem EU-Staat die DSGVO zu beachten, sondern auch in der Schweiz domizilierte Unternehmen, wenn sie (i) grenzüberschreitend Waren oder Dienstleistungen in einem EU-Staat anbieten und dabei Daten von Personen bearbeiten, die sich in der EU befinden (Art. 3 Abs. 2 Bst. a DSGVO) oder (ii) das Verhalten von Personen in der EU beobachten (Art. 3 Abs. 2 Bst. b DSGVO)[219].

Wird ein Produkt an einen EU-Abnehmer geliefert oder eine Dienstleistung zu Gunsten eines EU-Auftraggebers erbracht, ist aufgrund von Art. 3 Abs. 2 die DSGVO offensichtlich anwendbar. Das-

---

213 PAAL, DSGVO 20 N 10.

214 Was hierunter zu verstehen ist, ist unklar. Verwaltungskosten dürften zwar regelmässig höher sein als blosse Mitteilungskosten (KAMLAH, DSGVO 12 N 21), aber gewisse Autoren setzen die Verwaltungskosten den Mitteilungskosten gleich (z.B. HECKMANN/PASCHKE, DSGVO 12 N 44).

215 PAAL, DSGVO 20 N 10.

216 HECKMANN/PASCHKE, DSGVO 12 N 45; a.M. aber PAAL, DSGVO 12 N 63, der von einem Wahlrecht ausgeht.

217 Siehe PARRY, Rz. 13-014; KAMANN/BRAUN, DSGVO 20 N 36.

218 Das der DSGVO zugrundeliegende Auswirkungsprinzip ist keineswegs neu und findet sich auch in der schweizerischen Rechtsordnung: Insbesondere kommt im Falle der Anwendung des Wettbewerbsrechts (UWG) ebenfalls das Marktortsprinzip zur Anwendung; wenn sich Aktivitäten eines Schweizer Unternehmens im Ausland auswirken, sind die entsprechenden Vorschriften des jeweiligen Landes zu beachten (GROLIMUND, Einleitung N 110 f.; ZK-VISCHER, IPRG 136 N 12 ff.). Gleich verhält es sich auch in Bezug auf das Kartellrecht, wo sowohl in der EU als in der Schweiz das Auswirkungsprinzip gilt, für die EU: EuGH Slg. 1988, 5193 – Zellstoff; für die Schweiz: Art. 2 Abs. 2 KG.

219 Statt vieler: HÄRTING, 57 ff.

selbe gilt, wenn ein Schweizer Unternehmen auf seiner Website Leistungen anbietet, die sich auch an betroffene Personen in der EU richten. Während die blosse Zugänglichkeit der Website in der EU hierfür noch nicht ausreicht, können andere Faktoren darauf hindeuten, dass der Verantwortliche beabsichtigt, Personen in der EU Waren oder Dienstleistungen anzubieten[220]. Für Schweizer Unternehmen könnte zumindest theoretisch bereits eine DSGVO-relevante Grenzüberschreitung angenommen werden, falls ein Angebot in Euro gemacht wird.

Die weite Umschreibung des Anwendungsbereichs der DSGVO führt dazu, dass ein grosser Teil der Schweizer Unternehmen der in Art. 20 DSGVO angeordneten Pflicht zur Datenportabilität ab Ende Mai 2018 ohnehin untersteht. Diese Unternehmen müssen folglich entsprechende Prozesse vorsehen, um die Anforderungen der DSGVO erfüllen zu können.

Wie viele Schweizer Unternehmen den Vorgaben der DSGVO unterstehen, ist schwer einzuschätzen; betroffen sind aber mit Sicherheit nicht allein die grossen börsenkotierten Unternehmen, sondern auch mittlere und kleinere Unternehmen, die ihre Leistungen nicht exklusiv in der Schweiz anbieten. Einige Stimmen aus der Wirtschaft, die sich in der Vernehmlassung ganz grundsätzlich gegen eine Datenportabilitäts-Regelung ausgesprochen haben, scheinen diesen – die Realität reflektierenden – Aspekt ausgeblendet zu haben[221].

Zudem werden international tätige Schweizer Unternehmen ihre Systeme ohnehin an die EU-Gesetzgebung anpassen müssen, womit der Aufwand für eine Ausweitung auf zusätzliche Kunden relativ klein sein dürfte. Es ist deshalb durchaus vorstellbar, dass Kunden von Schweizer Unternehmen in der Schweiz ab Ende Mai 2018 ebenfalls in den Genuss des Rechts auf Datenportabilität kommen werden, wenn auch auf freiwilliger Basis. Dieser Effekt liess sich bereits in Bezug auf das sog. „Recht auf Vergessen(werden)“ beobachten. Seit dem entsprechenden Urteil des EuGH vom Mai 2014[222] ermöglicht es beispielsweise Google auch Kunden in der Schweiz, eine Löschung von in der Google-Suche indexierten Links zu verlangen.

3.2. Vertraglich vereinbarte Datenübertragungsrechte

Selbst wenn keine gesetzliche Grundlage vorliegt, können Vertragsparteien Vereinbarungen abschliessen, welche die Übertragung von Daten vorsehen. In IT-Verträgen finden sich regelmässig Bestimmungen, welche z.B. die Rückgabe von Daten im Zeitpunkt der Vertragsbeendigung vor-

---

220 Erwägungsgrund 23 DSGVO; ZERDICK, DSGVO 3 N 18.

221 Siehe bspw. die Stellungnahmen der AZ Direct AG und des Schweizerischen Verbands der Telekommunikation (asut). Anders indes der Verein DuG (Daten und Gesundheit) welcher ausführt, dass „80% aller Schweizer Unternehmen, welche zumindest mit einem EU-Land geschäftliche Beziehungen unterhalten, (…) ab Mai 2018 in jedem Fall dazu gezwungen sein [werden], die Datenportabilität gemäss Artikel 20 der EU-Datenschutzgrundverordnung im Rahmen dieser Geschäftsbeziehungen zu gewährleisten“.

222 EuGH vom 13. Mai 2014, Rs. C-131/12 – Google Spain SL und Google Inc. v. Agencia Española de Protección de Datos (AEPD) und Mario Costeja González.

sehen[223]. Entgegen einer möglicherweise verbreiteten Annahme, dass Datenübertragungsrechte v.a. dann vereinbart werden, wenn sich gleich starke oder ähnlich erfahrene Parteien gegenüberstehen, finden sich solche Rechte auch in den Allgemeinen Geschäftsbedingungen (AGB) der grossen Internetdiensteanbieter. Die AGB enthalten gegenwärtig meist sinngemäss die Bestimmung, die Rechte an den veröffentlichten Inhalten verblieben bei den Nutzern[224], was zumindest ein Recht des Nutzers impliziert, diese Inhalte heraus zu verlangen.

Ob dies allerdings schon einem eigentlichen Portabilitätsrecht gleichkommt, ist zweifelhaft. Denn einerseits ist die Bestimmung bei anderen Diensteanbietern (Streamingdienste, Fitnesstracker, Vergleichsdienste) weitaus seltener anzutreffen und andererseits wird die Möglichkeit, Daten tatsächlich zu portieren, nur in Einzelfällen vertraglich konkretisiert[225]. Eine präzise Umschreibung der Portabilität ist aber entscheidend. Dabei geht es um die von der Portabilität betroffenen Daten, das Format der zu übertragenden Daten, den Zeitpunkt der Datenübertragung und das Tragen der anfallenden Kosten[226].

3.3. Auskunftsrechte

3.3.1. Überblick

Vom Recht auf Datenportabilität zu unterscheiden ist das Auskunftsrecht, das einen Datenzugang ermöglicht, den faktischen Inhaber der Daten aber nicht zu verpflichten vermag, bestimmte Daten an Dritte zu übertragen. Ein solches Auskunftsrecht ist in Art. 8 DSG vorgesehen; diese Norm gilt für alle Personendaten. Neu, und etwas detaillierter, soll das datenschutzrechtliche Auskunftsrecht in Art. 23 E-DSG geregelt werden.

3.3.2. Auskunftsrecht im DSG

Das Auskunftsrecht vermittelt jeder Person ein relativ-höchstpersönliches[227], unverjährbares[228] Recht, vom Inhaber einer Datensammlung Auskunft darüber zu erhalten, ob Daten über sie bearbeitet wer-

---

223 ALBERINI/BENHAMOU, EF 2017, 521 f.

224 Vgl. die AGB von Google („Ihre Inhalte in unseren Diensten", <https://www.google.com/intl/de/policies/terms/>, Version vom 25. Oktober 2017), Facebook (Abs. 2, <https://de-de.facebook.com/legal/terms>, Version vom 30. Januar 2015), Instagram („Rechte", Abs. 1, <https://help.instagram.com/478745558852511>, Version vom 19. Januar 2013), Twitter (Abs. 3, „Ihre Rechte", <https://twitter.com/de/tos>, Version vom 2. Oktober 2017), LinkedIn (Abs. 3.1, <https://www.linkedin.com/legal/user-agreement>, Version vom 7. Juni 2017) und Tumblr (Abs. 6, <https://www.tumblr.com/policy/en/terms-of-service>, Version vom 26. September 2017).

225 Siehe die Datenschutzerklärung von Google, „Transparenz und Wahlmöglichkeit" (<https://www.google.com/intl/de/policies/privacy/>, Version vom 18. Dezember 2017), welche den Export von Nutzerdaten explizit regelt. Siehe immerhin auch die AGB-Seite von Facebook, welche zumindest auf die Hilfestellung zum „Herunterladen deiner persönlichen Daten" verweist, jedoch keine konkreten Rechte oder Pflichten festlegt (<https://de-de.facebook.com/legal/terms>, Version vom 30. Januar 2015).

226 ALBERINI/BENHAMOU, EF 2017, 521 f.

227 GNEHM, 82.

den (Art. 8 Abs. 1 DSG). Das Auskunftsrecht umfasst aber nicht nur Informationen über die Bearbeitung der Daten, sondern auch einen Anspruch auf Herausgabe der sie betreffenden Daten – konkret: auf Herausgabe einer Kopie dieser Daten (Art. 8 Abs. 5 DSG)[229]. Dieses Recht soll in erster Linie die Durchsetzung des Persönlichkeitsschutzes ermöglichen, indem es den betroffenen Personen ermöglicht, das Einhalten der Bearbeitungsgrundsätze zu überprüfen[230]. Dieser Zweckbestimmung entsprechend ist die Auskunft in der Regel kostenlos zu erteilen (Art. 8 Abs. 5 DSG). Vom Grundsatz der Kostenlosigkeit hat der Bundesrat jedoch Ausnahmen vorgesehen (Art. 2 VDSG)[231].

a) Berechtigte und Verpflichtete

Das Auskunftsrecht steht der betroffenen Person zu, ist aber nicht vertretungsfeindlich und kann deshalb auch von einem Dritten im Namen des Berechtigten geltend gemacht werden[232]. Mit Blick auf die mögliche Einführung eines Rechts auf Datenportabilität ist dies zentral. Weil das Auskunftsrecht der betroffenen Person einen Anspruch auf Herausgabe ihrer Daten vermittelt, der auch durch einen Vertreter wahrgenommen werden kann, ist es schon heute möglich, dass ein Unternehmen (als Vertreter einer betroffenen Person) von einem anderen Unternehmen die Herausgabe und Übermittlung der Daten der betroffenen Person verlangt. Zudem kann die betroffene Person bei Ausübung ihres Auskunftsrechts nicht nur Herausgabe der Daten an sich selbst, sondern auch direkt an einen Dritten verlangen. Dieser Vorgang entspricht im Ergebnis demjenigen beim Portabilitätsrecht. Denn in beiden Fällen ist es, wie beim Portabilitätsrecht, die betroffene Person, die darüber entscheidet, dass ein Unternehmen die sie betreffenden Daten an ein anderes Unternehmen übermittelt.

Zur Auskunft verpflichtet ist nicht jeder Bearbeiter der Daten, sondern nur der Inhaber der Datensammlung[233]. Eine Datensammlung ist nach der Legaldefinition von Art. 3 lit. g DSG ein Bestand an Daten, der nach Personen erschliessbar ist; dieser Begriff wird regelmässig weit ausgelegt[234]. Als Inhaber der Datensammlung gilt diejenige Person, die über den Zweck und den Inhalt der Datensammlung entscheidet (Art. 3 lit. i DSG). Das Auskunftsrecht gemäss Art. 23 E-DSG knüpft nicht an die Inhaberschaft einer Datensammlung an, sondern verpflichtet jeden Verantwortlichen im Sinne von Art. 4 lit. i DSG[235].

---

228 SHK-RUDIN, DSG 8 N 30.

229 Siehe dazu vorne, B.4.2.4.

230 SHK-RUDIN, DSG 8 N 1; GNEHM, 83.

231 Siehe dazu gerade nachstehend C.3.3.2.b).

232 SHK-RUDIN, DSG 8 N 9; KANTON ZUG, Abs. 3.1.2; siehe dazu auch hinten C.3.3.4.

233 WIDMER M., Datensubjekte, Rz. 5.9.

234 BSK-BLECHTA, DSG 3 N 80.

235 Zum Unterschied zum DSG siehe vorne B.4.2.4.

b) Umfang

Der Umfang des Auskunftsrechts umfasst die in der Datensammlung über die betreffende Person vorhandenen Daten und deren Herkunft (Art. 8 Abs. 2 lit. a DSG) sowie den Zweck und die Rechtsgrundlage des Bearbeitens. Da das Auskunftsrecht sich auf Personendaten bezieht, die sich in einer Datensammlung befinden, sind Daten vom Anwendungsbereich des Auskunftsrechts ausgeschlossen, wenn sie nicht nach der betroffenen Person erschliessbar sind. Erschliessbarkeit ist im Sinne der Legaldefinition der Datensammlung nur gegeben, wenn der Datenbestand aufgrund seiner Struktur oder mit Hilfsmitteln unter vernünftigem Aufwand einen personenbezogenen Zugriff ermöglicht[236].

Trotz dem klarem Wortlaut und der Systematik ist umstritten, ob der Inhaber nach ausserhalb der Datensammlung befindlichen Daten forschen muss[237]. Bei der Berücksichtigung, was einen „vernünftigen Aufwand" zur Erschliessung der Daten darstellt, ist zu beachten, dass bei grossem Arbeitsaufwand eine Kostenbeteiligung der betroffenen Person bis CHF 300 möglich ist (Art. 2 Abs. 1 lit. b VDSG). Eine Kostenbeteiligung ist daher der Einschränkung des Auskunftsrechts vorzuziehen[238]. Wird Auskunft erteilt, muss diese vollständig und richtig sein. Im (digitalen) Kontext der Datenportabilität stellt diese „Erschliessbarkeit" aber kaum eine Einschränkung dar.

Welche Informationen zur Ermittlung von „Zweck und Rechtsgrundlagen" der Bearbeitung von Personendaten herauszugeben sind, ist in der Praxis schwierig zu eruieren. Das Obergericht Zürich hat unter diesem Titel Dokumente von der Auskunftspflicht als erfasst erklärt, die „geeignet sind, über Zweck und Rechtsgrundlagen des Bearbeitens Auskunft zu geben", ungeachtet dessen, ob diese Dokumente Personendaten des Datensubjekts enthalten oder nicht[239].

Gemäss dem zweiten Teilgehalt des Auskunftsrechts muss über das „Umfeld" der Bearbeitung Auskunft erteilt[240] und insbesondere die Kategorisierung der bearbeiteten Personendaten, der an der Sammlung Beteiligten sowie der Datenempfänger (Art. 8 Abs. 2 lit. b DSG) bekannt gegeben werden.

Das Auskunftsrecht steht einer Person nur über die eigenen Daten zu. Die Daten Dritter sind vom Auskunftsrecht nicht erfasst[241]. Vielmehr sind bei der Auskunftserteilung die Interessen der Dritten dadurch zu schützen, dass mittels Interessenabwägung gegebenenfalls eine Einschränkung der Aus-

---

236 BSK-BLECHTA, DSG 3 N 81; GNEHM, 92.

237 Dafür BSK-GRAMIGNA/MAURER-LAMBROU, DSG 8 N 26; dagegen WIDMER M., Datensubjekte, Rz. 5.31; vermittelnd ROSENTHAL, DSG 8 N 15, der diejenigen Daten vom Auskunftsanspruch als erfasst betrachtet, die zwar nicht direkt durch die Datensammlung erschlossen sind, auf die aber durch die Informationen in der Datensammlung gezielt zugegriffen werden kann.

238 GNEHM, 92.

239 OGer ZH, LB140073, vom 5. Dezember 2014; dieses Urteil als „Fehlurteil" bezeichnend: ROSENTHAL, Jusletter vom 20. Februar 2017, Rn. 55.

240 SHK-RUDIN, DSG 8 N 37.

241 WIDMER M., Datensubjekte, Rz. 5.11.

kunft vorzunehmen ist[242]. Im Sinne einer Verhältnismässigkeitsprüfung ist zunächst festzustellen, ob eine Einschränkung geeignet ist, die Drittinteressen zu schützen. Sodann ist zu gewährleisten, dass die Einschränkung sachlich, räumlich, zeitlich und personell nicht weiter geht als erforderlich. Für letztere Abwägung sind die verschiedenen beispielhaft aufgezählten Arten der Einschränkungen in Art. 9 DSG zu berücksichtigen (Aufschub, Einschränkung, bzw. genauer: Limitierung, und Verweigerung der Auskunft)[243]. Schliesslich muss die Verhältnismässigkeit im engeren Sinne, d.h. die Relation zwischen Zweck der Massnahme (Schutz von Drittinteressen) und Mittel (gewählte Art der Einschränkung), geprüft werden.

Gemäss Art. 23 E-DSG ist im Sinne einer Generalklausel über alle Informationen Auskunft zu geben, die zur Geltendmachung von Rechten nach dem E-DSG erforderlich sind und eine transparente Datenbearbeitung gewährleisten. Im Minimum sind folgende Informationen mitzuteilen: Identität und Kontaktdaten des Verantwortlichen, bearbeitete Personendaten, Zweck der Bearbeitung, Aufbewahrungsdauer, verfügbare Angaben über die Herkunft der Daten, falls diese nicht von der verantwortlichen Person erhoben wurden, automatisierte Einzelentscheidungen und deren Logik, die Empfänger sowie die Kategorien von Empfängern, denen Personendaten bekanntgegeben werden. Daraus ergibt sich ein weiter Anwendungsbereich: Die Mitteilung der hinter einer automatisierten Einzelentscheidung stehenden Logik setzt beispielsweise voraus, dass über die Menge und Art der für ein Scoring herbeigezogenen Daten sowie über deren Gewichtung informiert wird[244]. Die Auskunft ist grundsätzlich kostenlos, aber der Bundesrat kann Ausnahmen vorsehen (Art. 23 Abs. 6 E-DSG).

c) Form

Die Auskunft ist in der Regel schriftlich in Form eines Ausdrucks oder einer Fotokopie zu erteilen (Art. 8 Abs. 5 DSG). Sie kann elektronisch erfolgen, wenn (i) der Inhaber der Datensammlung dies ausdrücklich vorsieht und geeignete Massnahmen trifft, (ii) die Identifizierung des Datensubjekts sicherstellt und (iii) die Daten vor dem unberechtigtem Zugriff Dritter schützt (Art. 1 Abs. 2 VDSG)[245].

Den Bearbeiter trifft eine Aufbereitungspflicht[246], nur schon um eine persönlichkeitsverletzende Bekanntgabe von Personendaten Dritter zu verhindern. Die Lehre betont hierbei jedoch die Informations- und Kontrollfunktion des Auskunftsrechts. So wird vorgebracht, dem Auskunftsrecht sei Genüge getan, wenn aus den Datenträgern eine Liste erstellt werde, aus der die bearbeiteten Personendaten und das „Umfeld" der Bearbeitung hervorgingen[247]. GNEHM hält demgegenüber fest, dass die

---

242 Siehe dazu hinten C.5.5.2.

243 BSK-GRAMIGNA/MAURER-LAMBROU, DSG 9 N 10.

244 Botschaft DSG, BBl 2017 6941, 7067.

245 WIDMER M., Datensubjekte, Rz. 5.21.

246 BSK-GRAMIGNA/MAURER-LAMBROU, DSG 8 N 27.

247 WIDMER M., Datensubjekte, Rz. 5.24.

Auskunft gemäss Art. 8 Abs. 5 DSG „in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie sowie kostenlos zu erteilen" sei. Eine Ausnahme von der Auskunftserteilung in Form einer Kopie oder eines Ausdrucks käme nur zum Zug, wenn sie für die Einschränkung des Auskunftsrechts nach Art. 9 DSG nötig sei[248].

Der Grundsatz, dass die Auskunft in der Regel schriftlich in Form eines Ausdrucks zu erteilen ist wurde im E-DSG gestrichen. Eine inhaltliche Änderung im Sinne eines Verzichts auf Schriftlichkeit ist damit aber kaum beabsichtigt[249].

d) Frist

Die Auskunft hat innert 30 Tagen zu erfolgen. Alternativ muss dem Datensubjekt innert dieser Frist begründet werden, weshalb eine Auskunftserteilung nicht fristgemäss möglich ist und innert welcher Frist mit einer Auskunft gerechnet werden darf (Art. 1 Abs. 4 VDSG).

3.3.3. Weitere Auskunftsrechte

Eine Reihe zivilrechtlicher Vorschriften räumt den jeweiligen Berechtigten ebenfalls Datenzugangsrechte im Sinne eines Auskunftsrechts ein. Der Zugang zu Informationen wird namentlich in familien- und erbrechtlichen Angelegenheiten (z.B. Art. 170 sowie Art. 607 Abs. 3 und Art. 610 Abs. 2 ZGB), in Vertragsverhältnissen (z.B. Art. 400 OR) und im gesellschaftsrechtlichen Kontext (z.B. Art. 697 OR) gesetzlich geregelt. Angeordnet wird jeweils die „Herausgabe" von Informationen in mündlicher oder schriftlicher Form, und zwar gegenüber dem Berechtigten.

3.3.4. Zwischenerkenntnis

Die bestehenden gesetzlichen Auskunftsrechte gehen schon relativ weit. Insbesondere das Auskunftsrecht nach DSG bzw. E-DSG vermittelt der betroffenen Person grundsätzlich einen umfassenden Anspruch auf Herausgabe der sie betreffenden Daten. Die Wirksamkeit dieses Rechts hängt indessen davon ab, in welcher Form es gewährt wird. Im Rahmen der bestehenden gesetzlichen Auskunftsrechte gibt es gegenwärtig kein Erfordernis zur Übertragung in einem standardisierten Format.

Genauso fehlt es an einer Pflicht des faktischen Dateninhabers, die Information auf Weisung des Berechtigten direkt an einen Dritten zu übertragen[250]. Das Fehlen einer solchen Pflicht spielt aber zumindest dann keine Rolle, wenn die Unternehmen bereit sind, sich von der anspruchsberechtigten Person zur Ausübung des Auskunftsrechts ermächtigen zu lassen. In den Konstellationen, die bei einem Recht auf Datenportabilität relevant sind, ist deshalb davon auszugehen, dass sich Auskunfts-

248 GNEHM, 94 f.

249 Botschaft DSG, BBl 2017 6941, 7066 ff.

250 Siehe auch BENHAMOU/TRAN, sic! 2016, 584 f.

rechte künftig auf einfache Weise von Unternehmen im Namen der betroffenen Personen geltend machen lassen. Wird das Recht auf diese Weise wahrgenommen, können die Zwecke einer Datenportabilität schon mit dem heutigen Auskunftsrecht weitgehend erreicht werden.

3.4. Kartellrechtliche Anordnung

3.4.1. Grundlagen und Problematik

Ein Recht auf Datenportabilität kann sich unter Umständen aus dem Kartellrecht ergeben. Denkbar ist die Anwendung des kartellrechtlichen Instrumentariums, wenn der faktische Dateninhaber über eine marktbeherrschende Stellung verfügt und diese ausnützt[251]. Grundsätzlich spielt es für die Anwendung des Kartellgesetzes (KG) keine Rolle, ob Personen- oder Sachdaten zur Diskussion stehen; in der Regel dürften aber die im Gutachten nicht behandelten Sachdaten im Vordergrund stehen. Ebenso kann festgehalten werden, dass das Kartellrecht im Rahmen seiner Zielsetzung – der Gewährung des funktionierenden Wettbewerbs – zwar verschiedentlich wirtschaftliche Akteure vor Lock-in-Situationen und den damit verbundenen versunkenen Kosten schützt[252], allerdings nicht pauschal, sondern nur nach Massgabe der einschlägigen Bestimmung. Einschlägig ist vorliegend Art. 7 KG zum Missbrauch einer marktbeherrschenden Stellung, weil lediglich das Verhalten des einzelnen Diensteanbieters in Frage steht und es nicht um Abreden zwischen Diensteanbietern geht.

Die marktbeherrschende Stellung gemäss Art. 7 KG beurteilt sich auf Grundlage des sachlich, räumlich und zeitlich relevanten Marktes. Insbesondere die weltweit tätigen sozialen Medien und Internetdiensteanbieter (z.B. Facebook, Google) weisen typischerweise ausreichend grosse Marktanteile auf, um als markbeherrschend zu gelten[253]. Dies dürfte im Wesentlichen auch für die Schweiz gelten. Das Kartellrecht hat allerdings bislang aus zwei Gründen Probleme, eine Marktbeherrschung festzustellen:

- Zum einen handelt es sich bei den Märkten, auf denen diese Unternehmen tätig sind, typischerweise um sog. zwei- oder mehrseitige Märkte. Zwischen den verschiedenen Marktteilnehmern bestehen wechselseitige Abhängigkeiten, was sich beispielsweise darin äussert, dass Unternehmen Dienste für gewisse Nutzergruppen kostenlos anbieten, während andere Nutzergruppen (z.B. Werbetreibende) mehr bezahlen. Mit diesen wechselseitigen Abhängigkeiten kann das Konzept der herkömmlichen Marktabgrenzung kaum umgehen[254]. Darüber hinaus ist die kartell-

---

251 WEBER, Concorrenza e Mercato 2016, 65 f.; BENHAMOU/TRAN, sic! 2016, 587.

252 Ein Beispiel ist die Lieferverweigerung im Sinne von Art. 7 Abs. 2 lit. a KG, was sich insb. darin äussert, dass der Abbruch einer bestehenden Geschäftsbeziehung strenger beurteilt wird, als die Geschäftsverweigerung bei erstmaliger Kontaktaufnahme, siehe FRÜH, 394, 412, jeweils m.w.H.

253 Siehe den Entscheid der EUROPÄISCHEN KOMMISSION i.S. Google Search (Shopping), AT 39740, wo die Kommission festhält, dass Google im Bereich der Suchmaschinen in allen Europäischen Ländern seit 2008 marktbeherrschend ist. Zum Marktanteil von Facebook siehe KÖRBER T., ZUM 2017, 94.

254 KÖRBER T., ZUM 2017, 94; AUTORITÉ DE LA CONCURRENCE/BUNDESKARTELLAMT, 27.

rechtliche Beurteilung zweiseitiger Märkte auch deswegen schwierig, weil sich die Marktverhältnisse sehr rasch ändern[255].

- Zum anderen werden Dienstleistungen oft unentgeltlich erbracht, weil und solange die Nutzer den Dienstleistern ihre Daten zur Verfügung stellen. Diese Unentgeltlichkeit stellt die herkömmliche Marktabgrenzung ebenfalls vor Probleme[256].

Wird trotz dieser Schwierigkeiten eine Marktbeherrschung festgestellt, muss das Verhalten der Unternehmen überdies missbräuchlich sein. Die ständige Praxis in der Schweiz und in der EU hat hierfür eine Reihe von Fallgruppen entwickelt. Ob eine dieser Fallgruppen zur Anwendung kommt, bzw. welche, hängt davon ab, ob die Daten an die betreffende Person selbst oder an ein anderes Unternehmen übertragen werden sollen.

3.4.2. Übertragung an ein anderes Unternehmen

Insbesondere das europäische Kartellrecht hat sich in mehreren Grundsatzentscheiden mit dem Zugang zu Informationen in der Hand marktmächtiger Unternehmen auseinandergesetzt[257]. Auch in der Schweiz wird auf diese Fälle Bezug genommen[258]. Es ging hierbei um Fälle des Behinderungsmissbrauchs, bei denen den Wettbewerbern (sowohl in der EU als auch in der Schweiz) solche Zugangsrechte gewährt wurden. Auf die vorliegende Konstellation, in der ein einzelner Nachfrager „seine" Daten auf ein anderes Unternehmen übertragen lassen will, passt diese Fallgruppe aber nicht ohne weiteres. Die betroffene Person kann ohne eine sehr weite Auslegung der Aktivlegitimation keine Ansprüche aus Kartellrecht geltend machen, weil es an der unternehmerischen Wettbewerbsbehinderung fehlt. Anders verhielte es sich möglicherweise, wenn die betroffene Person als Nachfrager in eigenem Namen eine Behinderung dartun könnte, etwa weil ihr der Zugang zu nachgelagerten Märkten verwehrt ist, auf denen sie ihre eigenen Daten verwenden bzw. kommerzialisieren könnte[259]. Solche Fälle sind soweit ersichtlich (und wohl mangels entsprechender Märkte) noch nicht bekannt.

---

255 SCHIESS/SCHALLER, 126 ff.

256 Siehe dazu das deutsche Bundeskartellamt, das gestützt auf diese Tatsache eine Änderung des GWB fordert, BUNDESKARTELLAMT, 5; AUTORITÉ DE LA CONCURRENCE/BUNDESKARTELLAMT, 27; DENOTH/KAUFMANN, sic! 2015, 505.

257 EuGH vom 6. April 1995, verb. Rs. C-241/91 P und C-242/91 P – Magill; EuGH vom 29. April 2004, Rs. C-418/01 – IMS Health; EuGH vom 17. September 2007, Rs. T-201/04 – Microsoft.

258 Siehe hierzu den massgeblichen Fall „SIX/Terminals mit Dynamic Currency Conversion (DCC)", abgedruckt in WEKO, RPW 2011, 96 ff., Rn. 106 ff., sowie die Aufarbeitung des europäischen Rechts in der schweizerischen Lehre, BSK-AMSTUTZ/CARRON, KG 7 N 84 ff.

259 Siehe dazu FRÜH, Jusletter IT Flash vom 11. Dezember 2017, Rn. 11.

3.4.3. Übertragung an die betroffene Person

Für die Übertragung an die betroffene Person ist *prima vista* die Fallgruppe des Ausbeutungsmissbrauchs einschlägig. Ein solcher liegt dann vor, wenn ein Unternehmen aufgrund seiner Marktmacht von den Nutzern unangemessene Preise verlangt oder ihnen unangemessene Konditionen diktiert. Auch die Fallgruppe des Ausbeutungsmissbrauchs ist aber aus zwei Gründen nicht geeignet: Zum einen verlangen viele Diensteanbieter überhaupt kein Entgelt für ihre Dienste, weshalb mangels Preis auch kein Preismissbrauch vorliegen kann[260]. Zum anderen besteht die Rechtsfolge der Bestimmung in einer Anpassung von Preisen und Konditionen der Dienstleistung, nicht aber in einem Zugang zu den Daten[261].

Eine kartellrechtliche Lösung käme folglich nur in Frage, wenn die Fallgruppe so ausgelegt oder angepasst würde, dass ein fehlender Zugriff auf die Daten (auch bei einer unentgeltlichen Dienstleistung) als missbräuchliche Bedingung aufgefasst würde. In diesem Falle liesse sich die Bedingung auf richterliche (oder behördliche) Anordnung anpassen. Hinweise auf eine solche extensive Auslegung oder entsprechende Präjudizien existieren allerdings (noch) nicht.

3.4.4. Weitere Anwendungshindernisse

Darüber hinaus sind – bzw. wären – die entsprechenden Verfahren regelmässig kostenintensiv. Zwar könnte zumindest diese Schwierigkeit zu einem gewissen Grad durch die Möglichkeit eines kollektiven Vorgehens (*collective action, class action*) gemildert werden. Andere Probleme sind dadurch aber noch nicht gelöst. Namentlich der erhebliche Zeitbedarf solcher Verfahren ist bei Daten, die für die tägliche Verwendung zur Verfügung stehen müssen, nicht tragbar[262]. In der (europäischen) Praxis zeigt sich zudem, dass selbst die Anordnung einstweiliger Massnahmen dieses Problem nicht lösen kann[263].

Die Problematik, dass kartellrechtliche Auseinandersetzungen sehr langwierig und kostenintensiv sind, hat sich beispielhaft an den Verfahren der Europäischen Kommission gegen Microsoft und Google in den letzten 15 Jahren gezeigt. Wenn es um die Portabilität von Daten geht, ist eine jahrelange Prüfung, z.B. des Vorhandenseins einer marktmächtigen Stellung oder einer missbräuchlichen Verhaltensweise, nicht hinnehmbar. Die heutigen wettbewerbsrechtlichen Verfahren lassen sich auch nicht ohne weiteres „beschleunigen“. Vielmehr müssten, wenn tatsächlich das Wettbewerbsrecht für die Datenportabilität zur Anwendung kommen sollte, neue Verfahren eingeführt werden, die es in anderen Rechtsbereichen schon gibt.

---

260 Oft erhöhen die Anbieter die Preise einer anderen Marktseite, womit jene Akteure aus Kartellrecht vorgehen könnten, nicht aber die betroffenen Personen, siehe DENOTH/KAUFMANN, sic! 2015, 511.

261 DREXL, NZKart 2017, 415.

262 WEBER, Concorrenza e Mercato 2016, 67 f.

263 FRÜH, 453.

Bereits seit knapp 20 Jahren kennt die ICANN im Falle von Domainnamen-Streitigkeiten ein spezielles Online-Verfahren, das eingeführt wurde, weil die Erfahrungen gezeigt hatten, dass die ordentlichen Gerichte der Einzelstaaten Entscheide nicht innert kurzer Fristen fällen können. Die *Uniform Domain Name Dispute Resolution Policy* (UDRP) der ICANN sieht ein weitestgehend online gestaltetes Verfahren vor, das innert weniger Monate zu einem Entscheid führt. Dieser Entscheid kann direkt gegen die zu Unrecht einen Domainnamen benützende Person durchgesetzt werden.

Seit Anfang 2017 kennt die EU auch eine funktionierende *Online Dispute Resolution* für Verbraucherstreitigkeiten, die allerdings bisher nur eine beschränkte Wirkung entfaltet. Die Online-Streiterledigung ist an sich nicht auf ein bestimmtes Rechtsgebiet beschränkt. Rechtsgrundlage ist die Verordnung 2013/524 zur Online-Streiterledigung in Verbraucherangelegenheiten[264]; eine Ergänzung der Vorschriften ist durch die Implementierungs-Verordnung 2015/1051 erfolgt, welche die Modalitäten für die Ausübung von Funktionen im Rahmen der Online-Streiterledigungs-Plattform, für die Einreichung elektronischer Beschwerdeformulare und die Zusammenarbeit zwischen einzelnen Plattformen festlegt[265]. Mit der Schaffung von solchen Online-Streiterledigungsverfahren ist im Kartellrecht in den nächsten Jahren allerdings nicht zu rechnen. Auch aus diesem Grund ist davon abzusehen, für die Datenportabilität auf einen kartellrechtlichen Ansatz abzustellen.

Aus all diesen Gründen ist sich die Lehre weitgehend einig, dass man sich im Fall, dass ein Recht auf Datenportabilität rechtspolitisch erwünscht ist, nicht auf die bestehenden kartellrechtlichen Regeln verlassen kann, sondern eine Spezialregelung erforderlich ist[266]. Auch für die Schweiz muss man zum Schluss gelangen, dass die Datenportabilität keine eigene Fallgruppe des Missbrauchstatbestands von Art. 7 KG darstellen kann bzw. soll.

3.5. Datenportabilität beim elektronischen Patientendossier

Im Zusammenhang mit dem elektronischen Patientendossier hat der Gesetzgeber jüngst bereits eine sehr spezifische, sachlich eng begrenzte Regelung der Datenportabililtät eingeführt. Gemäss Art. 17 Abs. 1 lit. e EPDV haben die Patientendaten verwaltenden Stammgemeinschaften[267] für den Fall,

---

264 Verordnung (EU) Nr. 524/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Online-Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Verordnung über Online-Streitbeilegung in Verbraucherangelegenheiten).

265 Durchführungsverordnung (EU) 2015/1051 der Kommission vom 1. Juli 2015 über die Modalitäten für die Ausübung der Funktionen der Plattform zur Online-Streitbeilegung, über die Modalitäten des elektronischen Beschwerdeformulars und die Modalitäten der Zusammenarbeit der Kontaktstellen gemäß der Verordnung (EU) Nr. 524/2013 des Europäischen Parlaments und des Rates über die Online-Beilegung verbraucherrechtlicher Streitigkeiten.

266 DREXL, NZKart 2017, 421; KÖRBER T., ZUM 2017, 101; WEBER, Concorrenza e Mercato 2016, 71; DREXL ET AL., Rn. 31.

267 Zum Begriff, siehe Art. 2 lit. e Bundesgesetz über das elektronische Patientendossier (EPDG).

dass eine Patientin oder ein Patient zu einer anderen Stammgemeinschaft wechselt, geeignete Prozesse vorzusehen.

Die EPDV-EDI regelt die Metadaten (Art. 3 EPDV-EDI und Anhang 3) und Austauschformate (Art. 4 EPDV-EDI und Anhang 4[268]) zur Sicherstellung der Kompatibilität. Die Metadaten stellen sicher, dass die betreffenden Daten stets gleich bezeichnet und damit leicht identifizierbar sind. Die vorgesehenen Austauschformate garantieren, dass die Daten in einer einheitlichen Struktur abgelegt werden und die automatisierte Weiterverarbeitung ermöglichen[269].

3.6. Zwischenfazit

Bereits im geltenden Recht bestehen Instrumente und Vorschriften, die eine Datenportabilität ermöglichen. Das Vertragsrecht erlaubt die freie Ausgestaltung solcher Rechte und ein Blick in die AGB der relevanten Internetdiensteanbieter zeigt, dass viele sich (trotz ihrer überragenden Marktstellung) einem Portabilitätsrecht nicht verschliessen. Treiber dieser Entwicklung ist bei den Betroffenen die anstehende Implementierung der DSGVO; eine Rolle spielen aber auch interne Digitalisierungs- und *Data Mapping*-Prozesse. Welche anderen Gründe bei Unternehmen für die freiwillige Einführung von Portabilitätsrechten relevant sind (etwa technologische Offenheit, betriebswirtschaftliches Kalkül, Reputationsmanagement oder Druck von Konsumentenorganisationen), lässt sich ohne weitere Erhebungen allerdings nicht eruieren.

Bei den zwingenden Vorschriften reicht das Auskunftsrecht des DSG am weitesten. Das Kartellrecht hingegen erweist sich in seiner gegenwärtigen Form zur Umsetzung eines Rechts auf Datenportabilität als ungeeignet. In Fällen des Behinderungsmissbrauchs fehlt es den betroffenen Personen an der Aktivlegitimation und die Fälle des Ausbeutungsmissbrauchs zielen lediglich auf die Preis-, nicht aber auf die Zugangskontrolle. Das Gesetz über das Elektronische Patientendossier betrifft nur, aber immerhin, einen kleinen Bereich der Personendaten, nämlich die Patientendaten. Hierzu haben Gesetz- und Verordnungsgeber in technischer Hinsicht sehr detaillierte Vorgaben erlassen. Für alle anderen Daten bietet das Gesetz indessen keine Lösungsansätze.

4. Theoretische Erwägungen zur Einführung eines Datenportabilitätsrechts

Gewisse Erwägungen zur Einführung eines Datenportabilitätsrechts lassen sich unabhängig von dessen Ausgestaltung anstellen. Dazu gehören namentlich die Fragen, ob die Einführung eines Datenportabilitätsrechts mit der Wirtschaftsfreiheit vereinbar ist und wie sie gesetzgeberisch implementiert werden müsste.

---

268 Die Vernehmlassungsfrist für diesen Anhang ist erst am 25. Oktober 2017 abgelaufen, die Ergebnisse sind noch nicht publiziert.

269 Erläuterungen zum Anhang 4 (Austauschformate) der Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI), Fassung vom 4. Juli 2017 für Vernehmlassung, 3.

4.1. Vereinbarkeit eines Datenportabilitätsrechts mit der Wirtschaftsfreiheit

Die Wirtschaftsfreiheit ist in Art. 27 BV verankert. Dieses Grundrecht schützt den Einzelnen darin, uneingeschränkt von staatlichen Massnahmen jede privatwirtschaftliche Erwerbstätigkeit frei auszuüben und einen privatwirtschaftlichen Beruf frei zu wählen. Sowohl natürliche als auch juristische Personen des Privatrechts sind Träger der Wirtschaftsfreiheit; für inländische juristische Personen gilt das Grundrecht mit Blick auf den persönlichen Geltungsbereich uneingeschränkt[270].

Die Einführung eines Datenportabilitätsrechts würde faktisch zu gewissen Einschränkungen der Wirtschaftsfreiheit führen. Ein solches Recht bedingt nämlich in gewissem Umfang technische und organisatorische Vorkehrungen, welche die betroffenen Unternehmen ansonsten möglicherweise nicht treffen würden. Daneben wäre insbesondere die Vertragsfreiheit betroffen, die den Vertragsparteien das Recht einräumt, den Inhalt des Vertrags privatautonom und frei von staatlichem Zwang auszuhandeln und damit ein Datenportabilitätsrecht nicht vorzusehen oder es ausdrücklich auszuschliessen. Einschränkungen der Vertragsfreiheit sind aber zulässig, solange sie mit der Wirtschaftsfreiheit vereinbar sind[271]. Die Lehre geht von einem unlösbaren Zusammenhang zwischen der Wirtschaftsfreiheit und der Vertragsfreiheit als Prinzip des Privatrechts aus[272]. Grundsätzlich betreffen Eingriffe in die Gestaltungsfreiheit der Vertragsparteien einen sensiblen Bereich der Wirtschaftsfreiheit[273].

Wie jedes andere Grundrecht gilt auch die Wirtschaftsfreiheit nicht absolut. Bereits Art. 95 Abs. 1 BV legt fest, dass der Bund berechtigt ist, Vorschriften über die Ausübung der privatwirtschaftlichen Erwerbstätigkeit zu erlassen. Solche interventionistischen Eingriffe müssen die allgemeinen Voraussetzungen von Art. 36 BV erfüllen, d.h. auf einer gesetzlichen Grundlage beruhen, einem öffentlichen Interesse entsprechen und verhältnismässig ausgestaltet sein. Bei schweren Eingriffen ist zudem die Einschränkung auf der Stufe eines Gesetzes vorzusehen und der Kerngehalt des Grundrechts darf nicht beeinträchtigt werden. Überdies ist zu fragen, mit welcher Dichte und Bestimmtheit der Gesetzgeber einen Eingriff auszugestalten hat: Je schwerer der Eingriff wiegt, desto bestimmter ist die entsprechende Eingriffsnorm zu formulieren[274].

Soll ein Datenportabilitätsrecht geschaffen werden, ist die Verankerung auf Gesetzesstufe sachgerecht. Mit der Schaffung einer Gesetzesbestimmung ist die Voraussetzung der gesetzlichen Grundlage auch für einen schweren Eingriff in die Wirtschafts- bzw. Vertragsfreiheit erfüllt. In den Kerngehalt der Wirtschafts- bzw. Vertragsfreiheit würde ein Datenportabilitätsrecht grundsätzlich nicht

---

270 RHINOW/SCHMID/BIAGGINI/UHLMANN, 69; HÄFELIN/HALLER/KELLER/THURNHERR, Rn. 656.

271 BGE 113 I a 126, E. 8c.

272 HÄFELIN/HALLER/KELLER/THURNHERR, Rn. 630.

273 BSK-UHLMANN, BV 27 N 13.

274 BGE 141 I 201, E. 4.1; BGE 136 I 1, E. 5.3.1; BGE 118 Ia 305, E. 2a; BSK-UHLMANN, BV 27 N 43; HÄFELIN/HALLER/KELLER/THURNHERR, Rn. 669.

fallen. Aus diesem Grunde bedürfen die Voraussetzungen des öffentlichen Interesses und der Verhältnismässigkeit einer genaueren Betrachtung.

Das öffentliche Interesse ist durch politische und/oder ökonomische Analysen bzw. empirische Untersuchungen nachzuweisen. Entsprechende Abklärungen sind bisher kaum vorhanden[275]. Zu klären ist in einem ersten Schritt die Frage nach dem Zweck eines möglichen Rechts auf Datenportabilität. Im Zentrum stehen sowohl datenschutzrechtliche (Schutz der informationellen Selbstbestimmung) als auch wettbewerbsrechtliche (Bekämpfung von Lock-in-Effekten) Interessen[276]. Ein öffentliches Interesse ist demnach gegeben, unabhängig davon, welchem Ansatz man folgt.

Das Verhältnismässigkeitsprinzip verlangt, dass die Einschränkung der Vertrags- und Wirtschaftsfreiheit nicht weiter geht als es der Zweck der Datenportabilität erfordert. Vorzunehmen ist also eine Einzelfallabwägung anhand der konkreten Umstände.

Eine Massnahme muss geeignet sein, einen Beitrag zur Erreichung des verfolgten Ziels zu leisten. In der vorgeschlagenen Form stärkt die Einführung eines Rechts auf Datenportabilität die Datenautonomie der betroffenen Person und damit auch deren informationelle Selbstbestimmung. Darüber hinaus würde ein solches Recht auch die Gefahr eines Lock-in im ökonomischen Sinne verkleinern, da der Aufwand für einen Wechsel des Anbieters durch den vereinfachten Datentransfer verringert wird. Keine Auswirkungen dürften hingegen in Bezug auf Netzwerkeffekte und kognitive Lock-in-Effekte zu erwarten sein[277]. Damit eine Massnahme geeignet ist, reicht es indessen bereits aus, wenn sie in Bezug auf das verfolgte Ziel nicht wirkungslos oder gar kontraproduktiv ist[278]. Diese geringen Voraussetzungen werden vom Recht auf Datenportabilität erfüllt.

Die Massnahme muss erforderlich sein, um das verfolgte Ziel zu erreichen. Dies ist nicht der Fall, wenn das Ziel mit einem gleichermassen geeigneten, aber milderen Mittel ebenso gut erreicht werden könnte[279]. Der Eingriff darf in sachlicher, räumlicher, zeitlicher und personeller Hinsicht nicht über das Notwendige hinausgehen[280]. Dies wäre bei der Ausgestaltung des Datenportabilitätsrechts als modifiziertes Auskunftsrecht der Fall.

Zuletzt muss die Massnahme dem einzelnen Betroffenen zumutbar sein. Dazu ist eine Abwägung zwischen den öffentlichen Interessen und den privaten Interessen der Betroffenen vorzunehmen. Wie

---

275 Siehe auch ALBERINI/BENHAMOU, EF 2017, 518 f.

276 Siehe dazu hinten C.5.1.

277 Siehe zum kognitiven Lock-in SÉNÉCAL/FREDETTE/LÉGER/COURTEMANCHE/RIEDL, Journal of Internet Commerce 2015, 277–293.

278 HOFSTETTER, 143 f.

279 BGE 140 I 353, E. 8.7; BGE 137 I 31, E. 7.5.2; BGE 136 I 87, E. 3.2; BGE 133 I 77, E. 4.1; HÄFELIN/MÜLLER/UHLMANN, Rn. 527; KIENER/KÄLIN, 121.

280 BGE 142 I 49, E. 9.1; BGE 140 I 2, E. 9.2.2; BGE 138 I 331, E. 7.4.3.1; BGE 136 I 87, E. 3.2; BGE 133 I 77, E. 4.1; BGE 132 I 49, E. 7.2; BGE 128 II 292, E. 5.1; KIENER/KÄLIN, 121; HÄFELIN/MÜLLER/UHLMANN, Rn. 530.

bereits ausgeführt, darf die Datenportabilität nicht so weit reichen, dass Investitions- und Innovationsanreize der zur Portabilität verpflichteten Unternehmen beschnitten werden. Dies scheint allerdings nicht der Fall zu sein, zumal kaum anzunehmen ist, dass Unternehmen mit Blick auf die mögliche Geltendmachung eines Rechts auf Datenportabiliät durch ihre Nutzer auf Investitionen in die Nutzung dieser Daten verzichten würden. Vielmehr vermag die Möglichkeit, dass Nutzer ihre Daten von einem bisherigen zu einem neuen Diensteanbieter portieren können, gerade Anreize zur Entwicklung neuer Geschäftsmodelle zu setzen.

Die Einführung eines Datenportabilitätsrechts, insbesondere in der vorgeschlagenen, auf dem bestehenden Auskunftsrecht des DSG aufbauenden Form, ist u.E. mit der Wirtschaftsfreiheit vereinbar.

4.2. Gesetzgeberische Konkretisierung

Die Schaffung eines Rechts auf Datenportabilität stellt – wie erwähnt – einen signifikanten Eingriff in die Wirtschaftsfreiheit (Art. 27 BV) dar. Die Bedeutung der Datenportabilität erscheint aber als nicht derart zentral, dass die Anordnung auch einen verfassungsrechtlichen Charakter haben müsste. Vielmehr gibt Art. 36 BV bereits vor, welche Rahmenbedingungen zu erfüllen sind, damit die Einschränkungen der Wirtschaftsfreiheit als gerechtfertigt erachtet werden können.

Angesichts der Tatsache, dass Art. 36 Abs. 1 BV als Eingriffsvoraussetzung eine gesetzliche Grundlage vorsieht, wäre die Datenportabilität auf Gesetzesstufe vorzusehen. Wird die Datenportabilität „nur“ für Personendaten vorgesehen, erweist es sich als naheliegend, die Regelung im Datenschutzgesetz vorzusehen. Die Regelungsdichte einer entsprechenden Norm braucht nicht so umfassend zu sein, dass es sich aufdrängt, ein besonderes Gesetz zur Datenportabilität auszuarbeiten und zu erlassen.

Würde der Gesetzgeber allerdings in Betracht ziehen, ein Recht auf Datenportabilität nicht nur für Personendaten, sondern auch (wenn zwar beschränkt), ähnlich dem Verordnungsvorschlag der EU vom September 2017, für Sachdaten einzuführen, liesse sich erwägen, dies in einem besonderen Gesetz zu regeln.

Weil die Schaffung eines Rechts auf Datenportabilität in die Wirtschaftsfreiheit eingreift, erfüllt eine Regelung auf Verordnungsstufe die Voraussetzungen von Art. 36 BV grundsätzlich nicht. Diese Einschätzung gilt insbesondere für den Fall, dass ein eigenständiges Recht auf Datenportabilität, ähnlich wie in Art. 20 DSGVO, vorgesehen werden sollte. Wird das Konzept der Datenportabilität hingegen auf das gesetzlich vorgesehene Auskunftsrecht (Art. 8 DSG) abgestützt[281], wäre eine Verordnungsbestimmung an sich denkbar, soweit sich der Inhalt der Datenportabilität dem Wesen nach unter das Auskunftsrecht subsumieren lässt.

---

[281] Siehe dazu vorne C.3.3.

Mit Blick auf den technologischen Fortschritt, der in vielen Markt- und Sozialbereichen äusserst rasch voran schreitet, hat die Lehre den Gedanken entwickelt, durch eine sog. „experimentelle Gesetzgebung" mit gewissen Normierungen, die regelmässig nur für eine beschränkte Zeit in Kraft stehen, auf Neuerungen zu reagieren. Die experimentelle Gesetzgebung lässt sich mit MADER umschreiben als „legislation enacted for a limited period of time in order to examine if a particular legislative measure will effectively achieve certain goals. It is enacted with a prospective purpose, but from a methodological point of view it requires retrospective evaluation"[282]. Das wichtigste Problem betrifft dabei die Frage, ob der Versuchscharakter der Normsetzung eine Rechtfertigung für die Abweichung vom Erfordernis der zuvor erwähnten gesetzlichen Grundlage darstellt. Diese Frage ist umstritten: Gemäss MADER sind bei Erlassen mit Versuchscharakter keine allzu strengen Anforderungen an die gesetzliche Grundlage zu stellen: „Für Regelungen, welche als Versuche konzipiert und zeitlich begrenzt sind, begnügt man sich oft mit einem Erlass auf Verordnungsstufe (materiell gesetzliche Grundlage), sofern ein rechtsetzender Erlass überhaupt als notwendig erachtet wird und der Versuch nicht gestützt auf blosse verwaltungsinterne Anordnungen oder Richtlinien durchgeführt werden kann. Erst die definitiv gedachte Regelung wird dann auf Gesetzesstufe eingeführt"[283]. Diese Auffassung von MADER, der auch eher das praktische Vorgehen beschreibt als dezidiert selbst Stellung bezieht, wird von MASTRONARDI kritisiert, der die Meinung vertritt, ein experimenteller Erlass müsse sich wie ein Dauererlass auf eine ausreichende gesetzliche Grundlage abstützen können[284].

Auch ein Versuchserlass muss ein Produkt durchdachter Gesetzgebung sein. Bei der Beurteilung der ausreichenden gesetzlichen Grundlage für einen Versuchserlass hat der (materielle) Gesetzgeber auf Verordnungsstufe einen gewissen Ermessensspielraum[285]. Mit Bezug auf die hier interessierende Rechtsfigur der Datenportabilität lässt sich insoweit festhalten, dass für ein umfassendes neues Recht auf Datenportabilität auch in Form eines Versuchserlasses die heutigen gesetzlichen Grundlagen als nicht ausreichend erscheinen. Würde hingegen eine schweizerische Regelung der Datenportabilität im Wesentlichen auf das Auskunftsrecht von Art. 8 DSG abgestützt[286], erschiene es als denkbar, zumindest für einen Versuchserlass die heutige Regelung des Auskunftsrechts als gesetzliche Grundlage genügen zu lassen.

5. Ausgestaltung eines Rechts auf Datenportabilität

Die Ausgestaltung eines Datenportabilitätsrechts hängt davon ab, auf welcher Begründung dieses Recht konzeptionell beruht (C.5.1), welche Daten davon erfasst sind (C.5.2), wer dadurch verpflichtet

---

282 MADER, Evaluating the Effects, 125; VAN GESTEL/VAN DIJCK, European Public Law 2011, 541.

283 MADER, Experimentelle Gesetzgebung, 214 f.

284 MASTRONARDI, ZSR 1991, 459 f.

285 Für einen neueren Überblick siehe KÖRBER S., LEGES 2015, 388 f.

286 Siehe dazu vorne C.3.3.

wird (C.5.3), in welchem Format die Daten vorliegen müssen (C.5.4), welche Einschränkungen gelten sollten (C.5.5) und unter welchen sonstigen Bedingungen das Portabilitätsrecht gewährt wird (C.5.6).

5.1. Konzeptionelle Begründung

Die Einführung eines Datenportabilitätsrechts lässt sich im Wesentlichen auf zwei Ansätze abstützen, einen datenschutzrechtlichen und einen kartellrechtlichen. Die konzeptionelle Begründung und die damit verfolgten Zwecke wirken sich auf die Ausgestaltung des Datenportabilitätsrechts aus.

5.1.1. Datenschutzrechtlicher Ansatz

Das Ziel des Portabilitätsrechts lässt sich darin erblicken, dass es die Herrschaft der betroffenen Personen über die sie betreffenden Personendaten stärkt[287]. Als positiver Rechtsanspruch soll es Steuerungsbefugnisse vermitteln und über die bestehenden datenschutzrechtlichen Abwehrbefugnisse hinausgehen[288]. In der Europäischen Union wird das Portabilitätsrecht oft im Zusammenhang mit zwei anderen Rechtsansprüchen, nämlich dem Recht auf Vergessenwerden und dem datenschutzrechtlichen Berichtigungsanspruch, genannt[289].

In der Schweiz stützt sich der datenschutzrechtliche Ansatz auf den Schutz der Privatsphäre in Art. 13 BV. Dies gilt nicht nur für datenschutzrechtliche Abwehransprüche, sondern nach verbreiteter Auffassung auch für datenschutzrechtliche Steuerungsbefugnisse. Denn die herrschende Lehre leitet unter Hinweis auf die bundesgerichtliche Rechtsprechung[290] das Prinzip der informationellen Selbstbestimmung ebenfalls aus Art. 13 BV ab[291]. Die ausdrückliche Aufnahme der informationellen Selbstbestimmung in die Verfassung wurde vom Parlament nur deswegen nicht weiterbehandelt, weil es der Auffassung war, dies sei überflüssig[292].

5.1.2. Kartellrechtlicher Ansatz

Zum Teil wird die Meinung vertreten, das Portabilitätsrecht solle in erster Linie für Wettbewerb sorgen[293]. Diese Auffassung stützt sich auf ökonomische Erwägungen. Zwar beseitigt ein Porta-

---

287 PAAL, DSGVO 20 N 4; KAMLAH, DSGVO 20 N 1; PILTZ, DSGVO 20 N 2 f.; SYDOW, DSGVO 20 N 3; KAMANN/BRAUN, DSGVO 20 N 4.

288 Siehe für die europäische Ebene ZANFIR, International Data Privacy Law 2012, 161.

289 SYDOW, DSGVO 20 N 3.

290 BGE 141 I 203, E. 4.1; BGE 142 II 347, E. 4.4; BGE 128 III 259, E. 3.2.

291 MAURER-LAMBROU/KUNZ, DSG 1 N 18; ROSENTHAL, DSG 1 N 3. Eingehend zur diesbezüglichen Kontroverse FASNACHT, Rn. 99 ff.

292 Siehe die Parlamentarische Initiative 14.413 VISCHER und den Abschreibungsbeschluss im amtlichen Bulletin des Nationalrates 2017 vom 29. September 2017.

293 So auch der BUNDESRAT im Erläuternden Bericht zum Vorentwurf des DSG vom 21. Dezember 2016, Ziff. 1.6.4, 22 sowie die Botschaft DSG, BBl 2017 6941, 6984 f. Siehe auch in der EU: SYDOW, DSGVO 20 N 1; PILTZ, DSGVO 20 N 1; KAMANN/BRAUN, DSGVO 20 N 3; PAAL, DSGVO 20 N 3, 6; KAMLAH, DSGVO 20 N 2; DREXL, Industrial Data, 56.

bilitätsrecht die direkten und indirekten Netzwerkeffekte auf den Datenmärkten nicht, namentlich nicht für Plattformen wie Google und Facebook. Das Portabilitätsrecht kann aber zumindest die Wechselkosten der Nutzer senken und verhindert dadurch, ökonomisch ausgedrückt, versunkene Kosten der Nutzer, bzw. der betroffenen Personen und damit so genannte Lock-in-Effekte[294]. Beispielsweise müssen die Daten im Falle eines Plattformwechsels nicht noch einmal vollständig neu eingegeben werden. Aus Sicht der potentiellen Wettbewerber auf diesen Märkten senkt dieser Mechanismus die Marktzutrittsschranken, was ein erklärtes Ziel des Kartellrechts ist, bzw. sein kann[295].

5.1.3. Stellungnahme

In Bezug auf das Portabilitätsrecht verhalten sich der datenschutzrechtliche und der kartellrechtliche Ansatz bis zu einem gewissen Grad wie zwei Seiten derselben Medaille: Werden die Nutzer vor einem Lock-in-Effekt geschützt, stärkt diese Anordnung auch ihre Datenautonomie. Umgekehrt leistet die Stärkung der informationellen Selbstbestimmung mittels Portabilität auch einen Beitrag zur Offenheit der Datenmärkte.

Während bei den angestrebten Zwecken des Portabilitätsrechts damit durchaus Parallelen zwischen kartell- und datenschutzrechtlichen Ansätzen bestehen und Mischformen denkbar sind, verlangt die Frage, auf welchem Normenkomplex (Datenschutzrecht oder Kartellrecht) das Portabilitätsrecht inhaltlich abgestützt und in welchem Erlass es geregelt wird, nach einer eindeutigen Antwort. Diese Antwort wirkt sich massgeblich auf die Ausgestaltung des Portabilitätsrechts aus, so namentlich auf die erfassten Daten und die zur Portabilität verpflichteten Personen und Unternehmen[296]. Aus den nachfolgenden theoretischen und praktischen Gründen wird hier empfohlen, das Recht auf Portabilität von Personendaten als datenschutzrechtlichen Anspruch auszugestalten:

- Zunächst lässt sich das Recht auf Datenportabilität als Teil des Rechts auf informationelle Selbstbestimmung verstehen, weil es den betroffenen Personen ermöglicht, „ihre“ Daten mit geringem Aufwand von einem Diensteanbieter auf einen anderen zu übertragen. Damit können die betroffenen Personen nicht nur bei der ersten Wahl eines Diensteanbieters, sondern auch später noch frei entscheiden, bei welchem Diensteanbieter die eigenen Daten gespeichert sein sollen. Ein Lock-in-Effekt liesse sich damit teilweise verhindern. Als Teil des Rechts auf informationelle Selbstbestimmung lässt sich das Recht auf Datenportabilität zudem unmittelbar auf die Verfassung abstützen[297].

---

294 Siehe dazu ausführlich FARRELL/KLEMPERER, *passim*.

295 Siehe die zahlreichen Hinweise auf die Praxis der Schweizerischen Wettbewerbskommission (WEKO) zu Marktzutrittsschranken bei BSK-REINERT/BLOCH, KG 4 II N 318 ff.

296 Siehe dazu gerade nachstehend C.5.2 und C.5.3.

297 Siehe dazu vorne C.5.1.1.

- Vor allem aber ist das Recht auf Datenportabilität aus der Sicht der Beteiligten – betroffene Personen ebenso wie Verantwortliche – nur eine vergleichsweise geringfügige Weiterentwicklung des datenschutzrechtlichen Auskunftsrechts. Denn der strukturelle Unterschied zum Auskunftsrecht besteht letztlich nur darin, dass die betroffene Person nicht nur die Herausgabe an sich selbst, sondern auch direkt die Übertragung an Dritte verlangen kann. Ebendies lässt sich allerdings schon heute erreichen, wenn die betroffene Person Auskunft an einen Dritten verlangt oder ihr Auskunftsrecht durch einen Dritten als Stellvertreter wahrnehmen lässt[298]. Der entscheidende Gehalt dieses Rechts besteht dabei sowohl für die betroffene Person als auch für die Verantwortlichen im Recht auf Herausgabe der Daten. Der normative Kern eines Rechts auf Datenportabilität kann damit bereits *de lege lata* aus dem datenschutzrechtlichen Auskunftsrecht[299] abgeleitet werden. Folgt man dem datenschutzrechtlichen Ansatz, lässt sich das Recht auf Datenportabilität damit nicht nur unmittelbar auf die Verfassung abstützen, sondern auch als vergleichsweise geringfügige Weiterentwicklung des bestehenden Auskunftsrechts ausgestalten.
- Die Anknüpfung am Auskunftsrecht vermag sicherzustellen, dass auch das Portabilitätsrecht nicht ohne Einschränkungen gilt. Namentlich könnte der Inhaber einer Datensammlung die Herausgabe der Daten an die betroffene Person und deren Übermittlung an einen Dritten verweigern, einschränken oder aufschieben, wenn dies wegen überwiegender Interessen Dritter (Art. 9 Abs. 1 lit. b DSG) oder wegen überwiegenden eigenen Interessen (Art. 9 Abs. 4 DSG) erforderlich ist.
- Aus der Pflicht zur Umsetzung des Auskunftsrechts entstehen den Verantwortlichen schon heute massgebliche Kosten, weil sie ihre Prozesse so ausgestalten müssen, dass sie jederzeit in der Lage sind, die eine bestimmte Person betreffenden Daten herauszugeben. Ob die Daten an die betroffene Person selbst oder an einen Dritten herauszugeben sind, spielt für die Ausgestaltung der Prozesse bei den Verantwortlichen kaum eine Rolle. Die Einführung eines Rechts auf Datenportabilität ist für die Verantwortlichen damit kaum mit relevanten Zusatzkosten verbunden.
- Die heutigen kartellrechtlichen Instrumente erscheinen als ungeeignet, die Datenportabilität zu gewährleisten. Dies bedeutet zwar nicht, dass die Schaffung eines sonderkartellrechtlichen Instrumentariums *de lege ferenda* oder eine Weiterentwicklung der Fallgruppen von Art. 7 KG durch die Gerichte ausgeschlossen wäre. Es fehlt aber sowohl an einem dogmatischen Fundament für ein solches Sonderkartellrecht als auch an einer klaren Antwort auf die Frage, inwiefern die Funktionsfähigkeit des Wettbewerbs durch ein solches Recht tatsächlich gestärkt werden könnte.
- Klar ist, dass sich die von den Plattformmärkten ausgehenden faktischen Netzwerkeffekte auch durch das Kartellrecht nicht beseitigen lassen. Ziel eines kartellrechtlichen Eingreifens *de lege*

298 Siehe dazu vorne C.3.3.4.

299 Siehe dazu vorne C.3.6.

ferenda wäre somit „lediglich", die Nutzer vor versunkenen Kosten und unerwünschten Lock-in-Effekten zu schützen. Dabei müsste aber erst einmal der Nachweis erbracht werden, ob und in welchem Umfang diese versunkenen Kosten und Lock-In-Effekte überhaupt bestehen. Gerade auch die historische Auslegung der DSGVO führt nicht zum Schluss, der EU-Gesetzgeber habe mit Art. 20 DSGVO lediglich eine sonderkartellrechtliche Norm zur Eliminierung von Lock-in-Effekten einführen wollen. Vielmehr stand die Stärkung der Kontrollmöglichkeiten des Datensubjekts ebenso im Fokus des Gesetzgebers[300]. Dass eine Regelung des Rechts auf Datenportabilität im Datenschutzrecht zugleich auch Funktionen erfüllen kann, die sonst vom Wettbewerbsrecht zu gewährleisten sind (etwa eine Verminderung von Lock-in-Effekten), steht einer Regelung im DSG nicht entgegen.

5.2. Erfasste Daten

Die Datenportabilität betrifft Daten, weshalb sich bei der Festlegung des Gegenstandes eines Portabilitätsrechts die Frage stellt, ob bzw. welche der in der Lehre verwendeten Differenzierungen zwischen verschiedenen Datenkategorien weiterführend sind[301]. Als hilfreich erweist sich dabei eine Kategorisierung nach dem Gesichtspunkt der Art der Produktion und des Gebrauchs der Daten[302]:

(a) „Freiwillige Daten" stammen von den betroffenen Personen und werden von ihnen bewusst mit anderen Personen geteilt. Typisches Beispiel sind von der betroffenen Person selbst auf eine Plattform hochgeladene Daten.

(b) „Beobachtete Daten" sind Daten, die vom Datenbearbeiter über die betroffene Person und deren Verhalten erhoben werden, etwa deren Browserverhalten, deren Verweildauer im Ladenlokal etc. Solche Daten können auch von Drittanbietern stammen. Kennzeichnend für diese Daten ist, dass sie ohne zusätzliche Informationen über den Kontext ihrer Erhebung für die betroffene Person unverständlich bleiben.

(c) „Abgeleitete Daten" entstammen grösseren Datenanalysen (*Big Data Analytics*), ohne dass die betroffene Individualperson davon Kenntnis hat.

Diese Taxonomie der Daten hat das Potenzial, die Umschreibung der Reichweite der Datenportabilität zu erleichtern. Einzuräumen ist allerdings, dass gerade zwischen den Daten der Kategorien (a) und (b) gewisse Abgrenzungsprobleme auftauchen können[303].

---

300 KAMMANN/BRAUN, DSGVO 20 N 4.

301 Zur syntaktischen, semantischen und pragmatischen Anknüpfung des Datenbegriffs grundlegend ZECH, 24 ff.; siehe auch SPECHT, CR 2006, 288, 290 ff.

302 WORLD ECONOMIC FORUM, Personal data, 7, 14, sowie WORLD ECONOMIC FORUM, Rethinking, 16 f.

303 SWIRE/LAGOS, Maryland Law Review 2013, 347 f., sprechen von einem „Kontinuum ohne natürliche Grenzziehung".

Mit dem hier vertretenen datenschutzrechtlichen Ansatz[304] ist allerdings grundsätzlich klar, dass sowohl die von der betreffenden Person selbst zur Verfügung gestellten Daten (Kategorie a) als auch die (wissentlich oder unwissentlich) über die betreffende Person gesammelten Daten (Kategorie b) zu portieren sind. Liegt der Zweck in der (Wieder-)Erlangung der Herrschaft über Personendaten, so müssen insbesondere auch beobachtete Personendaten eingeschlossen sein. Die Schwierigkeiten bei der Abgrenzung der Kategorien (a) und (b) spielen für das Portabilitätsrecht deshalb keine Rolle.

Der hier vertretene Ansatz geht weiter als das Portabilitätsrecht der DSGVO, das auf Daten beschränkt ist, welche die betroffene Person dem Verantwortlichen bereitgestellt hat (Art. 20 Abs. 1 DSGVO)[305]. Der Unterschied ist allerdings weit geringer, als er auf den ersten Blick scheint, weil auch die DSGVO ein weitgehendes Auskunftsrecht vorsieht, das ein Recht auf Kopie der Daten in einem gängigen elektronischen Format umfasst (Art. 15 Abs. 3 DSGVO)[306]. Wird dieses Auskunftsrecht durch ein Unternehmen als Vertreter der betroffenen Person wahrgenommen, ist es damit auch im europäischen Recht möglich, nicht nur die von der betroffenen Person bereit gestellten, sondern alle Personendaten von einem Unternehmen auf ein anderes portieren zu lassen[307].

Umfasst ein Recht auf Datenportabilität grundsätzlich alle Personendaten, stellt sich die Frage, ob die Interessen der betroffenen Unternehmen hinreichend geschützt sind. Dabei ist zu beachten, dass der Aufwand für die Portabilität kaum in massgeblichem Umfang über den Aufwand hinausgehen wird, den die Unternehmen für die Gewährleistung des Auskunftsrechts ohnehin auf sich nehmen müssen[308]. Hinzu kommt, dass die Anknüpfung am Auskunftsrecht erlaubt, dem Anspruch auf Datenportabilität allfällige überwiegende Interessen der Unternehmen entgegen zu halten und die Portabilität damit zu verweigern, einzuschränken oder aufzuschieben (Art. 9 Abs. 4 DSG)[309]. Liegen überwiegende Interessen der Unternehmen vor, wäre es also denkbar, das Recht auf Datenportabilität im Einzelfall auf freiwillige Daten (Kategorie a) einzuschränken und die Herausgabe oder Übermittlung von beobachteten Daten (Kategorie b) zu verweigern.

Bei der Abwägung zwischen den Interessen der betroffenen Person und denjenigen des bearbeitenden Unternehmens wird auch der Nutzen der Daten für die betroffene Person eine Rolle spielen. So

---

304 Mit einem kartellrechtlichen Ansatz dürften demgegenüber nur die von der betreffenden Person selbst zur Verfügung gestellten Daten – und damit ausschliesslich jene der Kategorie (a) – vom Anspruch auf Portierung erfasst sein. Von den Unternehmen selbst erhobene oder gesammelte Daten der Kategorie (b) gehören in aller Regel nicht zu jenen Daten, welche aus Nutzersicht die Wechselkosten erhöhen. Zugriff auf solche Daten kann bestenfalls das allgemeine Kartellrecht im Falle eines Missbrauchs einer marktbeherrschenden Stellung geben, dann aber wieder nur zugunsten des Wettbewerbers, siehe dazu vorne C.3.4.2. Unter diesem Ansatz ganz sicher ausgeschlossen wäre die Portabilität von Daten der Kategorie (c), die vom Datenbearbeiter entgegengenommen und hernach selber prozessiert werden.

305 Siehe dazu vorne C.3.1.2.

306 EHMANN, DSGVO 15 N 28.

307 Zur entsprechenden Rechtslage im schweizerischen Recht siehe vorne C.3.3.2.a).

308 Siehe dazu vorne C.3.3.2.

309 Siehe dazu hinten C.5.5.

stellt sich namentlich die Frage, was der betroffenen Person Daten bringen, die von ihr oder einem Unternehmen ohne zusätzliche Informationen zum Kontext nicht verstanden oder interpretiert werden können[310]. In solchen Fällen erscheint eine Einschränkung des Rechts auf Portabilität ebenfalls denkbar. Dies gilt erst recht, wenn den Daten Geschäftsgeheimnisse entnommen werden können[311].

Grundsätzlich kritisch zu sehen ist hingegen die Portabilität von Daten, welche der Datenbearbeiter aus den bestehenden Daten mittels Analyse gewonnen hat (Kategorie c). Soweit diese Daten nicht als Personendaten zu qualifizieren sind, fehlt schon der Anknüpfungspunkt für ein datenschutzrechtliches Portabilitätsrecht. Besteht ein Personenbezug, ist ein Anspruch in den Kontext der Idee eines „*Sharing the Wealth*" zu stellen, dessen Konturen aber derzeit noch nicht auszumachen sind[312]. Vielmehr müssten entsprechende Modelle erst noch entwickelt werden. Diese können etwa auf dem Grundsatz beruhen, dass ein Datenportabilitätsrecht in einer solchen Konstellation nur besteht, wenn der Datenbearbeiter (entgegen dem allgemeinen Grundsatz der Unentgeltlichkeit der Portabilität) eine gewisse Entschädigung für seine Leistungen (Investitionen) erhält[313].

Dies bedeutet, dass das Portabilitätsrecht Leistungen und Investitionen des Datenbearbeiters jedenfalls dann nicht erfassen darf, wenn sich diese auf die Ergebnisse der Analyse von Personendaten und nicht auf das Sammeln und Bearbeiten dieser Daten beziehen: Hätte eine Person, die einer Versicherung Gesundheitsdaten zur Verfügung gestellt hat, das Recht, die Ergebnisse der Auswertung dieser Gesundheitsdaten (z.B. die Diagnose eines Krebsrisikos) auf eine andere Versicherung zu übertragen, käme es zu einer „Fehlallokation" von Ressourcen.

Vom Portabilitätsrecht nicht erfasst, sind anonymisierte Daten, weil in diesem Fall keine Personendaten vorliegen. Weit weniger eindeutig ist die Rechtslage hingegen bei verschlüsselten Daten. Ein Recht auf Portabilität wird hier jedenfalls dann bestehen, wenn der Inhaber der Datensammlung in der Lage ist, die Daten selbst zu entschlüsseln. Hat er diese Möglichkeit aber nicht, etwa weil nur die betroffene Person über den Schlüssel verfügt, sind zwei Ansätze denkbar: Zum einen lässt sich vertreten, dass der Inhaber der Datensammlung keine Personendaten bearbeitet, weil er mangels Schlüssel nicht in der Lage ist, einen Personenbezug herzustellen. Folgt man diesem Ansatz, kann kein datenschutzrechtliches Portabilitätsrecht bestehen. Zum andern lässt sich argumentieren, dass der Personenbezug mithilfe des Schlüssels (wieder) hergestellt werden kann und nach der allgemeinen Lebenserfahrung auch damit zu rechnen ist, dass dieser Bezug wieder hergestellt wird, wenn

---

310 Beispielsweise lassen sich die betreffend das Einkaufsverhalten in einem physischen Ladenlokal erhobenen Geodaten nicht ohne den zugehörigen Grundriss des Ladens und die Warenanordnung verstehen und nutzen. Gleich verhält es sich, wenn Nutzer auf Webportalen von Online-Medien Kommentarbeiträge zu bestimmten Artikeln verfassen. Isoliert – d.h. ohne den betreffenden Artikel – betrachtet, sind diese Informationen wertlos.

311 Siehe zu möglichen Vorgehensweisen hinten C.5.5.

312 Siehe dazu vorne B.3.6.a).

313 Solche Ansätze können durch PIMS gefördert werden, siehe dazu vorne B.3.6.a).

zwar nicht vom Inhaber der Datensammlung, so doch von der betroffenen Person, die über den Schlüssel verfügt. Die Rechtsprechung des Bundesgerichts steht einer solchen Begründung jedenfalls nicht entgegen, sondern legt vielmehr nahe, dass auch in einem solchen Fall Personendaten vorliegen könnten[314]. Folgt man diesem Ansatz, würde sich ein Datenportabilitätsrecht auch auf verschlüsselte Personendaten beziehen. Dies erscheint grundsätzlich als sinnvoll, weil andernfalls die wenig befriedigende Konstellation eintreten könnte, dass die betroffene Person «ihre» Daten vom Inhaber der Datensammlung nicht herausverlangen könnte, wenn nur sie selbst über den Schlüssel verfügt, nicht aber der Inhaber der Datensammlung.

5.3. Verpflichtete Personen

Die EU hat Art. 20 DSGVO primär mit Blick auf die sozialen Medien (insb. Facebook) erlassen. Die während des Entstehungsprozesses geäusserte Kritik, dass auch kleinere Unternehmen durch die Neuerung verpflichtet würden, Daten in einem standardisierten Format an Dritte weiterzuleiten, fand angesichts der als bedrohlich empfundener Marktmacht grosser sozialer Medien keine Beachtung[315].

Eine Unterscheidung der betroffenen Unternehmen – namentlich nach wirtschaftlicher Grösse – fällt mit dem hier vertretenen datenschutzrechtlichen Ansatz[316] grundsätzlich ausser Betracht. Sollte dennoch eine Differenzierung angestrebt werden – bspw. nach gewissen Branchen oder Datentypen – hätte dies zumindest einen erheblichen Begründungsaufwand zur Folge.

5.4. Datenformat

5.4.1. Grundsatz

Das Portabilitätsrecht der DSGVO bezieht sich nur auf digitale Daten. Diese Beschränkung ist nicht zwingend, erscheint aber im Kontext der digitalen Wirtschaft als vernünftig.

Als Grundsatz ist wohl davon auszugehen, dass die Herausgabe der Daten in der bestehenden Form erfolgen kann. Nur diejenigen Daten, welche in einem nicht allgemein lesbaren Format vorliegen, müssen in ein gängiges Format überführt werden. Das Einlesen der Daten in das System des übernehmenden Datenbearbeiters ist hingegen dessen Sache.

---

314 BGE 136 III 508, E. 3.2.

315 WEBER/CHROBAK, Jusletter vom 4. April 2016, Rn. 38; ENGELS, Internet Policy Review 2016, 4; COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS, 6 f.

316 Wird das Portabilitätsrecht auf den kartellrechtlichen Ansatz gestützt, besteht aufgrund der Marktbezogenheit des Ansatzes die Möglichkeit, Mittellösungen zu suchen. Namentlich könnte ein Portabilitätsrecht mit guten Gründen so konkretisiert werden, dass die Datenportabilität nur für Unternehmen mit einer gewissen Marktmacht gelten würde; dabei könnte auf spezifische Grenzwerte abgestellt werden, etwa in Bezug auf Umsatz, Mitarbeiter- oder Nutzerzahlen, in diese Richtung auch GRAEF/VERSCHAKELEN/VALCKE, Law. The Journal of the Higher School of Economics, Annual Review 2013, 61 ff.

5.4.2. Umgang mit verschiedenen Dateiformaten

Das Dateiformat gibt vor, wie der Computer den Code interpretieren muss, damit der Inhalt in der vorgesehenen Form wiedergegeben werden kann. Kennt ein Computer ein Format nicht, ist diese Interpretation nicht möglich und entsprechend kann der Dateiinhalt auch nicht gelesen werden. Eine solche Situation tritt insbesondere bei proprietären oder wenig gebräuchlichen Formaten auf.

Daten, die im Kontext von Online-Plattformen vom Benutzer eingegeben oder von der Plattform generiert werden, sind üblicherweise in einer Datenbank abgelegt (z.B. MongoDB, MySQL). Die meisten Daten bestehen hier aus Zahlen und Zeichen. Diese Daten lassen sich problemlos in gängigen Datenbankenformaten (bspw. im XML-, CSV- oder JSON-Format) exportieren und können ohne nennenswerte Kompatibilitätsprobleme von anderen Anbietern übernommen werden. Dies wird der Hauptanwendungsfall der Datenportabilität sein[317].

Technische Schwierigkeiten könnten im Rahmen der Datenportabilität höchstens bei speziellen Dateiformaten auftreten. In der Realität dürften aber meist Standard-Dateiformate Verwendung finden, bspw. die üblichen Bild- (z.B. JPEG, GIF, PNG) oder Dokumentformate (z.B. PDF, DOC(X), TXT), weshalb in Bezug auf Dateiformate kaum Probleme zu erwarten sind.

Der Datensatz wird häufig aus vielen verschiedenen Dateien bestehen. Bei einem Download bietet es sich deshalb an, die Dateien in einer komprimierten Archivdatei zusammenzuführen (z.B. ZIP oder TGZ), um den Prozess nutzerfreundlicher zu gestalten.

5.4.3. Zusätzliche Informationen und Datenstruktur

Von der Frage des Dateiformates zu unterscheiden ist die Frage, ob diese Daten durch den übernehmenden Anbieter auch verstanden und mit zumutbarem Aufwand in das eigene System übernommen werden können.

Damit Daten verständlich sind, müssen sie mithilfe von Metadaten bezeichnet werden. Die Metadaten geben Auskunft, welche Daten gespeichert sind (z.B. Titel, Stichwörter), wie sie angeordnet sind und wie sie gesammelt wurden (z.B. Zeitpunkt der Speicherung, Umstände der Messung). Sie stellen sicher, dass die Daten verstanden und sinnvoll in ein anderes System übernommen werden können. Wie sich dieses Problem lösen lässt, zeigt die Regelung beim elektronischen Patientendossier[318]. Ob sich diese Lösung in der Praxis bewährt, bleibt allerdings noch abzuwarten.

Absehbar sind Probleme dann, wenn Daten für die Nutzung durch einen Computer generiert werden und nicht dazu gedacht sind, durch einen Menschen interpretiert zu werden. Ermittelt beispielsweise Google die Suchpräferenzen anhand der Suchhistorie, liegen möglicherweise Daten vor, welche nur

---

317 KAMANN/BRAUN, DSGVO 20 N 23.

318 Siehe dazu vorne B.3.4. Vgl. EPDV-EDI Anhang 3.

von der Suchmaschine selbst verstanden werden. Weiter scheint auch unklar, inwieweit Daten durch zusätzliche Informationen ergänzt werden müssen[319].

Hinzuweisen ist zudem auf die Tatsache, dass Daten nach unterschiedlichen Standards erhoben werden. Beispielsweise variiert das Körpergewicht beträchtlich, je nachdem, ob die Messung morgens vor dem Frühstück oder spät abends erfolgt. Insoweit ist von verschiedenen Daten auszugehen und eine Vermischung dieser Daten würde unter Umständen zu einer Verfälschung von Analyseresultaten führen. Standardisierungsansätze im Rahmen der Datenportabilität vermögen dieses Problem jedoch nicht zu lösen.

Kenntnisse der Datenstruktur sind zentral, damit Daten Dritter ohne übermässigen Aufwand in eigene Systeme übernommen werden können. Es geht dabei v.a. um die Frage, in welcher Ordnung die verschiedenen Daten vorliegen. Für den übernehmenden Anbieter scheint eine Einordnung der Daten in die eigene Datenstruktur grundsätzlich zumutbar, sofern die vom Erstanbieter gelieferte Struktur nicht ständig geändert wird. Ein übernehmender Datenbearbeiter muss bei der erstmaligen Datenübernahme von einem bestimmten Erstanbieter die Struktur dieser Daten analysieren. Dieser Prozess sollte sich aber für jeden weiteren erhaltenen Datensatz desselben Erstanbieters weitgehend automatisieren lassen, weshalb der Aufwand nicht als unverhältnismässig erscheint.

Vorgaben in Bezug auf die Datenstruktur können in der Regel nur für spezifische Anwendungen gemacht werden. Damit sich nämlich die Struktur festlegen lässt, muss vorab bekannt sein, welche Daten überhaupt eingefügt werden. Angesichts der unendlich vielen Möglichkeiten ist eine diesbezügliche Regelung unrealistisch und vermutlich auch kontraproduktiv. Forderungen nach standardisierten Strukturen lassen sich deshalb wohl dadurch erklären, dass die Idee der Datenportabilität in der EU ursprünglich auf soziale Netzwerke zugeschnitten war[320]. Die anfängliche Absicht war, die Vormachtstellung von marktmächtigen Anbietern wie Facebook zu durchbrechen und Konkurrenten den Zugang zu den entsprechenden Märkten zu erleichtern. Bei Wettbewerbsteilnehmern im gleichen Markt ist von „ähnlichen" Daten auszugehen, weshalb die Definition von einheitlichen Dateiformaten und Datenstrukturen naheliegend erschien.

Mit der datenschutzrechtlichen Ausgestaltung wird die Diskussion um die Standardisierung jedoch ungleich komplexer, weil der Kreis der möglichen Nutzer der Daten grundsätzlich offen ist. Während Standards in einem spezialisierten Bereich, wie bspw. beim elektronischen Patientendossier, sinnvoll sein können[321], ist ein allgemeiner Standard für ein Datenportabilitätsrecht kaum denkbar.

---

319 Siehe dazu vorne C.5.2.

320 KAMLAH, DSGVO 20 N 1; siehe auch EU KOMMISSION, Vorschlag Datenschutz-Grundverordnung, Erwägungsgrund 55.

321 Bestrebungen zu einer Vereinheitlichung der Datenstruktur gibt es derzeit im Bereich des elektronischen Patientendossiers. Die Ergebnisse der Ende Oktober abgelaufenen Vernehmlassung liegen noch nicht vor. Vorgesehen sind Vorgaben für drei spezifische Datensätze (eImpfdossier, eMedikation, eLaborbefund). Bei

Dass eine Standardisierung aber auch gar nicht nötig ist, zeigt z.B. BitsaboutMe[322]. Dieses PIMS bietet seinen Nutzern bereits heute die erforderlichen Tools an, um Daten von Plattformen wie Facebook, Google oder Twitter automatisiert zu übernehmen.

5.4.4. Zwischenergebnis

Die Einführung von Standards für Datenformate wäre grundsätzlich möglich. Es ist aber fraglich, ob ein solcher Schritt erforderlich ist. Vielmehr erscheint es als ausreichend, die Verwendung gängiger Formate vorzuschreiben, ohne diese Formate näher oder gar abschliessend zu spezifizieren. Wichtig ist vielmehr, dass die Nutzer und allfällige Diensteanbieter, welche die Daten im Rahmen der Datenportabilität übernehmen, verstehen, um welche Art von Daten es sich handelt. Dies lässt sich aber schon mithilfe von Metadaten oder allenfalls auch durch eine Dokumentation sicherstellen. Die Einführung von Standards erscheint deshalb weder als erforderlich noch als sinnvoll, zumal Vorschriften über technische Standards die Entwicklung neuer Formate hemmen könnten.

Falls sich PIMS durchsetzen und verschiedene Diensteanbieter ihre Systeme auf die angebotenen Schnittstellen ausrichten sollten, könnte dies durchaus zu einer gewissen Standardisierungstendenz führen. Solche freiwilligen Standards wären starren Vorschriften aufgrund der Flexibilität vorzuziehen.

5.5. Grenzen der Datenportabilität

5.5.1. Problemstellung

Der Herausgabe von Daten bei Ausübung des Portabilitätsrechts können massgebliche Interessen entgegenstehen, sowohl seitens der zur Herausgabe Verpflichteten als auch seitens Dritter. Besondere Bedeutung kommt dabei Geheimhaltungsinteressen zu. Der Schutz dieser Interessen kann Einschränkungen des Portabilitätsrechts erfordern und rechtfertigen.

Die DSGVO sieht ausdrücklich vor, dass das Recht auf direkte Übertragung der Daten auf einen Dritten (Art. 20 Abs. 2 DSGVO) die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf (Art. 20 Abs. 4 DSGVO). Für das Recht auf Herausgabe und eigene Übermittlung der Daten an einen Dritten (Art. 20 Abs. 1 DSGVO) gilt diese Einschränkung nach dem Wortlaut der Bestimmung allerdings nicht. Mit den Rechten Dritter sind auch die Geheimhaltungsinteressen des Datenbearbeiters angesprochen. Wie das Spannungsverhältnis konkret aufgelöst werden soll, muss allerdings wohl erst die Rechtsprechung zeigen; eine klare Regel lässt sich aus der Vorschrift jedenfalls nicht ableiten.

Gesundheitsdaten bestehen verschiedene internationale Standards wie z.B. IHE Patient Care Device (PCD) Technical Standard, Continua Design Guidelines oder HL7 International FHIR; siehe dazu eHEALTH SUISSE, mobile Health (mHealth) Empfehlungen I, 16. März 2017, 33 f.

322 Siehe dazu vorne B.3.1.3.

Folgt man dem datenschutzrechtlichen Ansatz, lässt sich das Spannungsverhältnis zwischen dem Recht auf Datenportabilität und den Interessen der zur Herausgabe Verpflichteten und allfälliger Dritter durch eine Orientierung an der Regelung der Einschränkungen des Auskunftsrechts auflösen. Dies entspricht auch dem Ansatz der DSGVO, nach welcher die Einschränkungen des Auskunftsrechts auch auf das Portabilitätsrecht Anwendung finden (Art. 12 Abs. 5 DSGVO). Bei der Orientierung am Auskunftsrecht ist allerdings zu berücksichtigen, dass die heutige Rechtslage kritisiert wird, weil das Auskunftsrecht sog. „*fishing expeditions*" keinen Riegel schiebe[323].

5.5.2. Einschränkungen nach DSG

Die Auskunft kann eingeschränkt werden, wenn ein Gesetz im formellen Sinn dies vorsieht (Art. 9 Abs. 1 lit. a DSG). Gemäss einer teleologischen Auslegung von Art. 9 Abs. 1 lit. a DSG lassen sich dem auskunftsersuchenden Datensubjekt nur Gesetzesbestimmungen entgegenhalten, die das datenschutzrechtliche Auskunftsrecht effektiv einschränken wollen[324]. Geheimhaltungsbestimmungen, welche die Interessen des Datensubjekts schützen, fallen nicht darunter[325].

Eine Einschränkung aufgrund überwiegender Drittinteressen lässt sich auf Art. 9 Abs. 1 lit. b DSG stützen. Diese Einschränkung ist z.B. einschlägig, wenn Drittdaten den Gegenstand eines Auskunftsersuchens bilden, weil sie auf dem gleichen Datenträger gespeichert sind[326] oder die Daten einem Berufsgeheimnis unterstehen, das Drittinteressen schützt[327].

Private Inhaber einer Datensammlung können die Auskunft zudem verweigern, wenn ihre eigenen Interessen überwiegen und keine Personendaten an Dritte bekannt gegeben werden (Art. 9 Abs. 4 DSG). Als berechtigte Interessen gelten dabei auch finanzielle Interessen[328] und Geheimhaltungsinteressen[329]. Die Rechtsordnung stellt verschiedentlich Fabrikations-, Geschäfts-, Amts- und Berufsgeheimnisse unter zivil- und teilweise auch unter strafrechtlichen Schutz[330]. Der Schutz erstreckt sich in all diesen Bestimmungen aber nur auf relative Geheimnisse. Als solche gelten Tatsachen, die weder offenkundig noch allgemein bekannt sind und an deren Geheimhaltung der Geheimnisherr ein berechtigtes Interesse hat, das er wahren möchte[331]. Geheimhaltungsinteressen können aber nur angerufen werden, wenn die auskunftsersuchende Person nicht zum Kreis der Berechtigten gehört

---

323 ROSENTHAL, Jusletter vom 27. November 2017, Rn. 104.

324 HUSI-STÄMPFLI, DSG 9 N 18; BRACHER/TAVOR, SJZ 2013, 48; FRIEDRICH/KAISER, ST 2013, 526, m.H. auf Art. 10a GwG; zu nennen wäre auch Art. 63 Abs. 4 NDG.

325 FRIEDRICH/KAISER, ST 2013, 526

326 BGE 141 III 119, E. 6.2; HUSI-STÄMPFLI, DSG 9 N 21.

327 FRIEDRICH/KAISER, ST 2013, 526.

328 BGE 138 III 425, E. 6.1.

329 BGE 138 III 425, E. 6.1, betreffend befürchteter Wirtschaftsspionage.

330 Z.B. Geschäftsgeheimnisse in Art. 4 lit. c und Art. 6 UWG sowie in Art. 162 StGB; Amtsgeheimnisse in Art. 320 StGB; Berufsgeheimnisse in Art. 321 StGB, in Art. 147 FinfraG sowie in Art. 47 BankG.

331 Statt vieler: BGE 142 II 268, E. 5.2.2.1.

bzw. nicht selber durch die Geheimhaltungsvorschrift gebunden ist, weil es andernfalls an einer der Geheimhaltung entgegenstehenden Offenbarung fehlen würde[332]. Ob das Auskunftsrecht aufgrund berechtigter Geheimhaltungsinteressen einzuschränken ist, muss im Rahmen einer Interessenabwägung entschieden werden. Dabei ist zu berücksichtigen, dass die Auskunft nicht nur verweigert, sondern auch eingeschränkt werden kann.

Alle diese Einschränkungen sind auch in Art. 24 E-DSG vorgesehen; sie lassen sich sinngemäss ebenso auf das Portabilitätsrecht anwenden. Dieses kann zudem, wie das Auskunftsrecht, nicht nur verweigert, sondern auch lediglich eingeschränkt werden, bspw. auf bestimmte Daten. Als Orientierungspunkt mag dabei die vorstehend skizzierte Kategorisierung von Daten dienen[333]. Damit ist es durchaus möglich, das Portabilitätsrecht in gewissen Konstellationen auf diejenigen Personendaten zu beschränken, welche die betroffene Person dem Inhaber der Datensammlung selbst bereitgestellt hat (sog. freiwillige Daten).

5.5.3. Einschränkungen wegen Rechtsmissbrauchs

Obwohl das Auskunftsrecht ohne Nachweis berechtigter Interessen geltend gemacht werden kann, betont das Bundesgericht, dass die Interessen des Berechtigten bei der Frage der Rechtsmissbräuchlichkeit des Auskunftsersuchens zu beurteilen sind[334]. Rechtsmissbrauch liegt insbesondere vor, wenn ein Rechtsinstitut zu Zwecken angerufen wird, welche dieses Institut nicht schützen will (sog. Institutsmissbrauch[335]). Gemäss Bundesgericht fällt Rechtsmissbrauch in Betracht, wenn Daten beschafft werden sollen, die ansonsten kostenpflichtig wären, das Ersuchen schikanös ist oder der Beweisausforschung dient[336].

Bezüglich der Beweisausforschung ist zunächst zu beachten, dass das Auskunftsrecht in hängigen Zivil- und Strafverfahren nicht anwendbar ist (Art. 2 Abs. 2 lit. c DSG). Kommt das DSG zur Anwendung, setzt das Bundesgericht die Hürde für die Rechtsmissbräuchlichkeit hoch an, da Rechtsmissbrauch bereits verneint wird, wenn dem Auskunftsersuchen auch datenschutzrechtliche Motive zugrunde liegen[337]. Dies bedeutet, dass die verpflichtete Person nicht nur Umstände darlegen muss, die eine Beweisausforschung belegen, sondern auch beweisen muss, dass die berechtigte Person keine datenschutzrechtlichen Motive hat. Dieser Beweis ist in zweierlei Hinsicht schwierig: Erstens

---

332 Siehe BGE 141 III 119, E. 7.4.1, wo eine Bank die Auskunft nach Art. 8 DSG ihren ehemaligen Mitarbeitern unter Berufung auf das Bankgeheimnis nicht verweigern konnte, da die Mitarbeiter auch nach Beendigung des Arbeitsverhältnisses dem Bankgeheimnis unterstanden (Art. 47 Abs. 4 BankG).

333 Siehe dazu vorne C.5.2.

334 BGE 141 III 119, E. 7.1.1; BGE 138 III 425, E. 5.4.

335 BSK-HONSELL, ZGB 2 N 51.

336 BGE 138 III 425, E. 5.5.

337 BGE 138 III 425, E. 5.6: „Selbst wenn sie die Datenüberprüfung (auch) im Hinblick auf einen allfälligen Schadenersatzprozess vornehmen möchten, wäre ihr Auskunftsbegehren deshalb noch nicht rechtsmissbräuchlich."; GNEHM, 88; BRACHER/TAVOR, SJZ 2013, 50 Fn. 60.

handelt es sich bei Motiven um innere Tatsachen, die sich meist nur mit Indizien beweisen lassen[338]. Zweitens lässt sich das Bedürfnis nach Kenntnis von Personendaten immer mit dem Grundsatz der Erkennbarkeit einer Datenbearbeitung[339] begründen, steht das Auskunftsrecht doch in einem engen Konnex zu diesem[340]. Die Motive der Beweisausforschung und der Erkennbarkeit einer Datenbearbeitung überschneiden sich derart, dass der vom Bundesgericht geforderte Beweis faktisch unmöglich ist[341]. Dies zeigt sich auch darin, dass Prozessanwälte dazu raten, die Einleitung eines Zivilprozesses sorgfältig zu terminieren, damit nicht die Möglichkeit der Abklärung der Beweis- und Prozesschancen im Vorfeld eines Zivilprozesses mittels Art. 8 DSG verloren geht[342].

Nach dem E-DSG kann das Auskunftsersuchen eingeschränkt werden, wenn es offensichtlich unbegründet oder querulatorisch ist (Art. 24 Abs. 1 lit. c E-DSG). Dies entspricht der Einschränkung des Auskunfts- und Portabilitätsrechts gemäss DSGVO bei „offenkundig unbegründeten oder exzessiven Anträgen" (Art. 12 Abs. 5 DSGVO). Die Botschaft geht allerdings davon aus, dass die Auskunft nur verweigert werden darf, wenn das Datensubjekt einen haltlosen Grund angibt[343], was nur diejenigen Ersuchen ausschliesst, die mehr oder weniger „ausdrücklich" einen Rechtsmissbrauch einräumen. Diese Lösung wird kritisiert, da sie die skizzierten Probleme nicht löst[344]: Der Nachweis einer offensichtlichen Unbegründetheit stellt die Verpflichteten im Wesentlichen vor die gleichen Probleme wie der Nachweis, dass einem Auskunftsbegehren keine datenschutzrechtlichen Motive zugrunde liegen.

Nimmt das Bundesgericht die missbräuchliche Geltendmachung des Auskunftsrechts weiterhin nur derart zurückhaltend an, werden sich die verfahrensrechtlichen Editionsregeln mithilfe des Auskunftsrechts auch unter der Geltung von Art. 24 Abs. 1 lit. c E-DSG leicht umgehen lassen. ROSENTHAL schlägt deshalb vor, dass der Verantwortliche selbst dann die Auskunft aufgrund eigener Interessen einschränken dürfen soll, wenn er die Daten Dritten bekannt gibt. Dies würde dem Gericht immer eine Interessenabwägung ermöglichen[345]. Zur Beschränkung des Missbrauches erwähnt er die Möglichkeit, die Daten nicht mehr dem Datensubjekt, sondern einer dritten Stelle bekannt zu geben[346]. Für das Portabilitätsrecht ist dies allerdings keine taugliche Lösung.

---

338 Statt vieler: SUTTER-SOMM, Rn. 774.

339 Siehe dazu vorne B.4.2.2.c).

340 Siehe RUDIN, DSG 8 N 1; MEIER, Rn. 696.

341 Im Ergebnis ebenso: ROSENTHAL, Jusletter vom 27. November 2017, Rn. 110.

342 GNEHM, 88; RÜD/MICHLIG, 176 f., welche das Auskunftsrecht als „ideales Mittel" zur vorprozessualen Beweismittelausforschung bezeichnen; kritisch zu dieser Entwicklung: ROSENTHAL, Jusletter vom 27. November 2017, Rn. 104.

343 Botschaft DSG, BBl 2017 6941, 7069.

344 Eingehend: ROSENTHAL, Jusletter vom 27. November 2017, Rn. 110 f.

345 ROSENTHAL, Jusletter vom 27. November 2017, Rn. 114.

346 ROSENTHAL, Jusletter vom 27. November 2017, Rn. 104 Fn. 130.

Denkbar wäre stattdessen, dass die über das Auskunfts- oder Portabilitätsrecht erhaltenen Dokumente und Dateien nicht in Verfahren verwendet werden dürfen, die keinen Bezug zum Datenschutz- oder Persönlichkeitsrecht haben. Diese Einschränkung würde die informationelle Selbstbestimmung ins Zentrum rücken und damit Sinn und Zweck des datenschutzrechtlichen Auskunfts- und Portabilitätsrechts entsprechen. Möglich wäre dabei auch eine zeitliche Befristung dieses Verwertungsverbotes, um tatsächlich nur der verpönten vorprozessualen Beweisausforschung einen Riegel zu schieben.

5.6. Zeit und Kosten

Um wirksam zu sein, muss ein Portabilitätsrecht innert einer gewissen Frist durchgesetzt werden können. Sowohl das Auskunftsrecht des DSG als auch das Portabilitätsrecht der DSGVO sehen heute eine Frist von einem Monat vor[347]. Dies erscheint als sachgerecht.

Ausserdem muss klar sein, wer die Kosten der Übertragung der Daten trägt. Die bestehenden Regeln sehen weitgehend Kostenlosigkeit vor. Das erscheint grundsätzlich richtig, zumal den Unternehmen durch das Recht auf Datenportabilität kaum zusätzliche Kosten entstehen[348]. Je nach Datentyp wäre es allerdings denkbar, für die Herausgabe der Daten und deren direkte Übermittlung an einen Dritten ein Entgelt zu verlangen[349].

5.7. Konsequenzen

5.7.1. Handlungsoptionen

Hält man die Einführung eines Rechts auf Datenportabilität für sinnvoll und versteht man dieses – wie hier – als Weiterentwicklung des datenschutzrechtlichen Auskunftsrechts, so lässt sich ein solches Recht mit Blick auf die Rechtslage *de lege lata* im Wesentlichen auf drei Arten umsetzen:

(a) durch Einführung eines Datenportabilitätsrechts nach dem Vorbild der DSGVO;

(b) durch Anwendung des datenschutzrechtlichen Auskunftsrechts in seiner heutigen Form; oder

(c) durch eine Anpassung des datenschutzrechtlichen Auskunftsrechts.

Aus den angeführten Gründen erscheint das Auskunftsrecht des DSG als sinnvoller Ausgangspunkt. In seiner gegenwärtigen Form reicht es schon sehr weit, verfügt aber noch über Unzulänglichkeiten, die für dessen Anpassung und damit für die Umsetzung von Option (c) sprechen.

---

347 Siehe dazu vorne C.3.1.2 und C.3.3.2.d).

348 Siehe dazu vorne C.5.1.3.

349 Siehe dazu vorne C.5.2 *in fine*.

5.7.2. Anpassungsbedarf

Die Einführung eines Rechts auf Datenportabilität als Weiterentwicklung des Auskunftsrechts erfordert nur einige wenige Anpassungen bzw. Präzisierungen der bestehenden Regelung:

Erstens ist ein Datenportabilitätsrecht nur sinnvoll, wenn die Daten der betroffenen Person in einer brauchbaren Form übermittelt werden müssen, was unter verschiedenen Aspekten zu beurteilen ist. Die „schriftliche Übermittlung in Form eines Ausdrucks", wie sie das geltende DSG noch vorsieht, erfüllt diesen Anspruch nicht. Angesichts der heutigen Dienste und Nutzungen käme eine Übermittlung von physischen Ausdrucken an die betreffende Person einer Umgehung durch den Bearbeiter gleich. Dass die entsprechende Passage im E-DSG gestrichen wurde, ist deshalb zu begrüssen. Die Streichung geht aber noch nicht weit genug: Vorzusehen wäre ein ausdrückliches Recht auf Kopie der Daten in einem gängigen elektronischen Format. Für den Fall, dass die Daten nicht in einem solchen Format vorliegen, muss zudem eine Konvertierungspflicht des Bearbeiters vorgesehen werden.

Zweitens ist eine Bezeichnung der Datenelemente zu verlangen, weil Daten sonst nur schwierig einzuordnen sind. Sofern die Datenelemente bezeichnet sind, erweist sich eine besondere Strukturierung der Daten dagegen nicht als notwendig[350]. Eine solche würde die Unternehmen wohl nur unnötig einschränken. Dennoch wäre es wünschenswert, dass ein bestimmter Anbieter seine Daten stets im gleichen Format weitergibt, damit übernehmende Anbieter den Prozess automatisieren können. Jedenfalls muss vertieft darüber nachgedacht werden, wie mit einer technologieneutralen Regelung eine böswillige Erschwerung der Portabilität verhindert werden kann.

Drittens fehlt dem Auskunftsrecht das in Art. 20 DSGVO vorgesehene Recht, die Daten direkt auf Dritte übertragen zu lassen. Da eine Weitergabe an Dritte zur Erreichung des Zwecks des Portabilitätsrechts häufig zentral sein dürfte, erscheint eine Ergänzung des Auskunftsrechts im Sinne einer „Mitteilung an Dritte" sinnvoll. Dabei handelt es sich allerdings um wenig mehr als eine Klarstellung der heutigen Rechtslage, zumal die betroffenen Personen schon heute Auskunft an Dritte verlangen oder einen Dritten als Stellvertreter einsetzen können, welcher das Auskunftsrecht in ihrem Namen geltend macht. Auf beiden Wegen lässt sich schon mit dem geltenden Auskunftsrecht eine direkte Übermittlung der Daten an Dritte erwirken[351].

---

350 Siehe zur Datenstruktur vorne C.5.4.3.

351 Siehe dazu vorne C.3.3.4.

6. Betroffene Branchen

6.1. Überblick

Auch in der Schweiz dürfte in der Praxis das Anliegen einer Person, die auf einem bestimmten Konto eingegangenen Mails, das auf Facebook hochgeladene Profil oder die zur Verfügung gestellte Fotosammlung auf einen anderen Anbieter zu übertragen, im Vordergrund stehen. Das Recht auf Datenportabilität kann aber auch in anderen Wirtschaftssektoren und Branchen eine Rolle spielen. Im Vordergrund stehen diejenigen Unternehmen, die grosse Mengen von Personendaten bearbeiten, etwa im Gesundheitsbereich, in der Versicherungs- und Finanzbranche, im Einzelhandel, im Medienbereich und bei anderen Diensteanbietern.

6.2. Gesundheitsbereich

Im Gesundheitsbereich fallen viele Personendaten an, die oft auch sensitiv sind. Angesichts stetig steigender Gesundheitskosten sind Patienten gegebenenfalls veranlasst, zu einem anderen Anbieter von Gesundheitsdienstleistungen zu wechseln. Die Regelung des elektronischen Patientendossiers sieht zwar eine gewisse Datenportabilität vor, jedoch nur auf freiwilliger Basis[352]. Damit stellt sich die Frage, ob ein Recht auf Datenportabilität geltend gemacht werden kann.

Im Gesundheitsbereich kommt der wertsteigernden Bearbeitung von Daten besondere Bedeutung zu[353]. Wird ein Datenportabilitätsrecht gesetzlich verankert, sind ohne Zweifel die vom Patienten zur Verfügung gestellten Personendaten erfasst. Hingegen wird der Datenbearbeiter, der durch Datenanalysen zu weiteren (und neuen) Datenbeständen gekommen ist, diese Daten nicht unentgeltlich herausgeben wollen[354].

Ein weiteres Problem stellt sich im Kontext des Berufsgeheimnisses. Im Einzelfall ist zu prüfen, ob die der Portabilität unterliegenden Daten nicht auch Berufsgeheimnisse einer Drittperson enthalten[355].

6.3. Versicherungs- und Finanzbranche

Zum Teil eng verbunden mit dem Gesundheitsbereich sind die Versicherungsmärkte. Schon seit Jahren sammeln Versicherungen grosse Mengen an Personendaten der Versicherten, um diese unter Anwendung neuer Technologien wie Big Data Analytics zu nutzen [356]. Will der Versicherungsnehmer die Versicherung wechseln, hat er ein Interesse daran, die Daten portieren zu können. Schranken ergeben sich aber auch hier, wenn die Versicherung durch eigene Leistungen

---

352 Siehe dazu vorne C.3.5.

353 Siehe dazu vorne B.3.

354 Siehe dazu vorne C.5.

355 Siehe dazu allgemein vorne C.5.5.

356 Siehe dazu WEBER, Jusletter vom 12. Dezember 2016, Rn. 7 ff.

und Investitionen den Wert der Personendaten vergrössert hat[357]. Die Grenzziehung muss dann anhand der vom Portabilitätsrecht erfassten Daten erfolgen.

Das Recht auf Datenportabilität kann auch gegenüber Banken und Effektenhändlern relevant sein. Beabsichtigt der Kunde, die Bank zu wechseln, hat er ein Interesse daran, gewisse Personendaten zu portieren. Die neueren und noch bevorstehenden Finanzmarktregulierungen (z.B. Finanzdienstleistungsgesetz) stellen immer höhere Anforderungen mit Bezug auf die Erfassung personenbezogener Daten, um den Geeignetheitstest durchzuführen. Das für einen Kunden zu erstellende Risikoprofil enthält z.B. überwiegend Personendaten[358]. Ein Recht auf Portierung von Daten könnte die Aufnahme einer neuen Bankbeziehung gegebenenfalls vereinfachen, weil der Kunde die bisherigen Unterlagen übertragen lassen kann.

6.4. Einzelhandel

Einzelhändler wie Migros und Coop sammeln über ihre Kundenbindungs- und Rabattprogramme vielfältige Nutzerdaten. Gleich gehen E-Commerce-Anbieter vor. Während aus Sicht der Konsumenten gute Gründe für die Geltendmachung des Auskunftsrechts bestehen, dürften diese in der Regel nicht an einer Übertragung der Daten von einem Einzelhändler auf einen anderen interessiert sein, zumal die Datenpools der Einzelhändler und E-Commerce-Anbieter durch Ausübung der Portabilität noch grösser würden als sie es ohnehin schon sind. Hinzu kommt, dass das Recht auf Datenportabilität von den Anbietern auch für das Setzen von Fehlanreizen genutzt werden könnte, etwa wenn die Kunden mit zusätzlichen Punkten oder Rabatten zum Wechsel und zur gleichzeitigen Übertragung ihrer Kundendaten verleitet würden.

6.5. Medien

Content Provider in den verschiedensten Bereichen sammeln vielfältige Nutzerdaten. Dazu gehören beispielsweise Online-Zeitungen oder die digitalen Angebote der SRG. Die Nutzerdaten, die hier von Interesse sind und für eine Portierung in Frage kommen, sind häufig kontextabhängig und haben einen Bezug zu bestimmten Inhalten (etwa die Bewertung eines redaktionellen Beitrags oder ein Kommentar dazu). Eine Portabilität macht hier im Grunde deshalb nur Sinn, wenn die Daten gemeinsam mit den Inhalten übertragen werden – was in der Regel nicht in Frage kommt – oder wenn der Drittanbieter über identische Inhalte verfügt, denen die Daten wieder zugeordnet werden können.

6.6. Andere Diensteanbieter

Verschiedenartige Diensteanbieter, wie etwa Internet-Zugangsprovider, TV-Anbieter (z.B. Swisscom und Wilmaa), Streamingdienste (z.B. Spotify, Netflix), Anbieter von E-Mail- und Messengerdiensten

---

357 Siehe dazu vorne C.5.

358 Siehe Art. 17 Abs. 1 lit. a E-FIDLEG.

(z.B. WhatsApp, Facebook Messenger), sammeln Daten über das Verhalten ihrer Nutzer, beispielsweise zum Anzeigen von personalisierter Werbung. Auch diese Daten, also insb. die Historie des Surf- und Kommunikationsverhaltens sowie des Medienkonsums der betroffenen Personen, sind vom Portabilitätsrecht umfasst.

D. HANDLUNGSEMPFEHLUNGEN

Zusammenfassend lassen sich die folgenden Handlungsempfehlungen zum Recht auf Datenportabilität und zu den *Personal Information Management Systems* (PIMS) formulieren:

1. Das Recht auf Datenportabilität ist ein Instrument, das es dem „Dateninhaber" erlaubt, bei einem Datenbearbeiter gespeicherte Daten mit geringem Aufwand auf einen anderen Datenbearbeiter zu übertragen. Angesichts seiner Bedeutung für die informationelle Selbstbestimmung sollte die Einführung eines solchen Rechts – auch in der Schweiz – in Betracht gezogen werden.

2. Ein auf dem datenschutzrechtlichen Ansatz basierendes Recht auf Datenportabilität ist einer kartellrechtlichen Regelung klar vorzuziehen. Ein solches Recht lässt sich auf das Grundrecht der informationellen Selbstbestimmung stützen und auf der Grundlage des bestehenden datenschutzrechtlichen Auskunftsrechts als dessen Weiterentwicklung ausgestalten. Dieser Ansatz erlaubt auch, den Interessen der Datenbearbeiter angemessen Rechnung zu tragen, indem ein solches Recht im Einzelfall gewissen Einschränkungen unterworfen werden kann.

3. Zur Einführung eines Rechts auf Datenportabilität müsste das DSG im Zusammenhang mit der Regelung des Auskunftsrechts durch einige Elemente präzisiert und ergänzt werden. Eine solche gesetzliche Regelung würde die verfassungsrechtlichen Vorgaben (gesetzliche Grundlage, öffentliches Interesse und Verhältnismässigkeitsprinzip) insbesondere mit Blick auf die Wirtschaftsfreiheit (Art. 27 BV) erfüllen.

4. Das Recht auf Datenportabilität, verstanden als Ergänzung des Auskunftsrechts, ist materiell wie folgt zu konkretisieren:

   - Der Anspruch der betroffenen Person auf Herausgabe der eigenen Daten sollte ergänzend zum heutigen Recht auch ausdrücklich einen Anspruch auf Herausgabe in einem gängigen elektronischen Format enthalten.
   - Über das Auskunftsrecht hinausgehend muss der Anspruch der betroffenen Person auf Herausgabe der eigenen Daten auch die direkte Übertragung der Daten an Dritte umfassen.
   - Der Gesetzgeber sollte in angemessener Form (wohl in der Verordnung oder in der Botschaft) klarstellen, dass der Inhaber der Datensammlung die Datenelemente so zu bezeichnen hat, dass die Daten von den betroffenen Personen und den Dritten verstanden und gegebenenfalls in das eigene System übernommen werden können. Bestehen solche Vorgaben, sind Vorschriften zu Standards für Datenformate verzichtbar.
   - Für die Frist zur Datenportierung erscheint ein Monat wie beim Auskunftsrecht als plausibel. Auch bei der Tragung der Kosten drängt sich eine Anlehnung am Auskunftsrecht auf; die Daten sind damit grundsätzlich unentgeltlich an betroffene Personen und Dritte herauszugeben. Anderes gilt nur für abgeleitete Daten, also Daten, die der Bearbeiter durch Datenanalysen selbst erzeugt hat.

- Wie das Auskunftsrecht untersteht auch das Portabilitätsrecht gewissen Grenzen, die es erlauben, den Interessen von Datenbearbeitern und Dritten angemessen Rechnung zu tragen.

5. Die allgemeine Regelung des Rechts auf Datenportabilität im Datenschutzgesetz sollte mit einer Analyse konkreter Negativeffekte einhergehen, die durch ein solches Recht verursacht werden könnten, insbesondere mit Bezug auf konkrete Branchen (z.B. Gesundheitsbereich). Als Folge dieser Analyse wären allenfalls einzelne Branchen der Regelung der Datenportabilität gar nicht oder nur beschränkt zu unterwerfen oder es wären spezifische Kriterien für deren Anwendung zu formulieren.

6. Im Hinblick auf eine Regelung des Rechts auf Datenportabilität, aber auch mit Bezug auf PIMS erscheint es sinnvoll, die Idee von „*Sharing the Wealth*“ (Beteiligung der betroffenen Personen an mti Daten erzielten Wertschöpfung) genauer zu analysieren.

7. Der Erfolg von PIMS hängt von den Nutzerzahlen und vom Aufwand ab, den die (potentiellen) Nutzer betreiben müssen, um ihre Daten von den bisherigen Anbietern auf PIMS zu übertragen. Dieser Aufwand lässt sich durch die Einführung eines Rechts auf Datenportabilität massgeblich verringern. Weitere gesetzgeberische Massnahmen erscheinen nicht erforderlich. Als sinnvoll erweisen könnte sich aber eine vertiefte Untersuchung der Regeln über die Datensicherheit, zumal der Sicherheit von PIMS mit der wachsenden Menge der dort gespeicherten Daten eine zentrale Bedeutung zukommen wird.

E. LITERATUR

ACAR ABBAS/AKSU HIDAYET/ULUAGAC A. SELCUK/CONTI MAURO, A Survey on Homomorphic Encryption Schemes: Theory and Implementation, 6. Oktober 2017, <https://arxiv.org/abs/1704.03578>

AEBI-MÜLLER REGINA, Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Habil., Abhandlungen zum Schweizer Recht, Bd. 710, Bern 2005

ALBERINI ADRIEN/BENHAMOU YANIV, Data Portability and Interoperability, EF 2017, 518–522

AMSTUTZ MARC/REINERT MANI (Hrsg.), Basler Kommentar, Kartellgesetz, Basel 2010 (zit. BSK-AUTOR)

BAERISWYL BRUNO/PÄRLI KURT (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz (DSG), Bern 2015 (zit. SHK-AUTOR)

BAUR ISABEL/BLUM-SCHNEIDER BRIGITTE/EGGER DAVID MICHAEL/MAIRE DÉLIA, Das elektronische Patientendossier, Jusletter vom 28. August 2017

BEGLINGER JACQUES/BURGWINKEL DANIEL/LEHMANN BEAT/NEUENSCHWANDER PETER K./WILDHABER BRUNO, Records Management – Leitfaden zur Compliance bei der Aufbewahrung von elektronischen Dokumenten in Wirtschaft und Verwaltung mit Checklisten, Mustern und Vorlagen, 2. Aufl., Zollikon 2008

BENHAMOU YANIV/TRAN LAURENT, Circulation des biens numériques: de la commercialisation à la portabilité des données, sic! 2016, 571–591

BERANEK ZANON NICOLE, Melde- und Benachrichtigungspflichten nach EU DSGVO + rev. DSG, Jusletter vom 2. Oktober 2017

BRACHER NICOLAS/TAVOR EYAL, Das Auskunftsrecht nach DSG: Inhalt und Einschränkung im Vorfeld eines Zivilprozesses, SJZ 2013, 45–51

BRANSCOMBE MARY, Why you need DRM for your documents, CIO 3. Mai 2016, <www.cio.com/article/3065036/security/why-you-need-drm-for-your-documents.html>, zuletzt besucht am 20. Dezember 2017

CONRAD CONRAD, Das Recht auf Datenübertragbarkeit (Art. 20 DSGVO), Datenschutz Notizen vom 6. Januar 2017, <https://www.datenschutz-notizen.de/das-recht-auf-datenuebertragbarkeit-art-20-dsgvo-3516934/>, zuletzt besucht am 20. Dezember 2017

DENOTH SERAINA/KAUFMANN OLIVER, Kartellrechtliches Erfassen von Wettbewerbswirkungen grosser Datenbestände (Big Data), sic! 2016, 501–516

DEUTSCHE GESELLSCHAFT FÜR MEDIZINISCHE INFORMATIK, BIOMETRIE UND EPIDEMIOLOGIE E. V., Hinweise/Stellungnahme zum „Recht auf Datenübertragbarkeit" gemäß Art. 20 DS-GVO, 4. Dezember 2016

DREXL JOSEF ET AL., Zur aktuellen Diskussion über Ausschliesslichkeits- und Zugangsrechte an Daten, Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb, 16. August 2016

DREXL JOSEF, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, Max Planck Institute for Innovation and Competition Research Paper No. 16-13, 31. Oktober 2016 (zit. „Industrial Data")

DREXL JOSEF, Neue Regeln für die Europäische Datenwirtschaft?, Ein Plädoyer für einen wettbewerbspolitischen Ansatz – Teil 2, NZKart 2017, 415–421

ECKERT MARTIN, Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, SJZ 2016, 265–274

ECKERT MARTIN, Digitale Daten als Wirtschaftsgut: Digitale Daten als Sache, SJZ 2016, 245–249

EHEALTH SUISSE, EPD-Zertifizierung, <https://www.e-health-suisse.ch/gemeinschaften-umsetzung/epd-gemeinschaften/epd-zertifizierung.html>, zuletzt besucht am 20. Dezember 2017

EHMANN EUGEN/SELMAYR MARTIN (Hrsg.), Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, München 2017

ENGELS BARBARA, Data portability among online platforms, Internet Policy Review 2016, 1–17

EPINEY ASTRID, Allgemeine Grundsätze, in: Belser/Epiney/Waldmann (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, 510–558

EPINEY ASTRID/FASNACHT TOBIAS, Rechte Einzelner, in: Belser/Epiney/Waldmann (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, 597–637

EPINEY ASTRID/NÜESCH DANIELA, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, 88–98

FARRELL JOSEPH/KLEMPERER PAUL, Coordination and Lock-in: Competition with Switching Costs and Network Effects, in: Armstrong/Porter (Hrsg.), Handbook of Industrial Organization, Bd. 3, Amsterdam 2007, 1967–2072

FASNACHT TOBIAS, Die Einwilligung im Datenschutzrecht, Zürich/Basel/Genf 2017

FRECH PHILIPP, Zivilrechtliche Haftung von Internet-Providern bei Rechtsverletzungen durch ihre Kunden, Eine rechtsvergleichende Untersuchung des schweizerischen, des amerikanischen und des deutschen Rechts unter besonderer Berücksichtigung des Urheber- und Markenrechts, Zürich/Basel/Genf 2009

FRIEDRICH ALAIN/KAISER MARKUS, Datenschutzrechtliche Auskunftspflicht und Arbeitspapiere einer Revisionsstelle, ST 2013, 524–528

FRÖHLICH-BLEULER GIANNI, Eigentum an Daten?, Jusletter vom 6. März 2017

FRÜH ALFRED, Immaterialgüterrechte und der relevante Markt, Köln 2012

FRÜH ALFRED, Zum Bedarf nach Datenzugangsrechten, Jusletter IT Flash vom 11. Dezember 2017

GIRSBERGER DANIEL ET AL. (Hrsg.), Zürcher Kommentar zum IPRG, 2. Aufl., Zürich 2004 (zit. ZK-AUTOR)

GNEHM OLIVER, Das datenschutzrechtliche Auskunftsrecht, in: Epiney/Nüesch (Hrsg.), Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes/La mise en oeuvre des droits des particuliers dans le domaine de la protection des données, Forum Europarecht Bd. 35, Zürich 2015, 77–106

GORDON CLARA-ANN, Personal Information Management Systems (PIMS), Jusletter IT Flash vom 11. Dezember 2017

GRAEF INGE/VERSCHAKELEN JEROEN/VALCKE PEGGY, Putting the right to data portability into a competition law perspective, Law. The Journal of the Higher School of Economics, Annual Review 2013, 53–63

GRESSIN SEENA, The Equifax Data Breach: What to Do, FTC Consumer Information vom 8. September 2017, <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>, zuletzt besucht am 20. Dezember 2017

GROLIMUND PASCAL, in Jung/Spitz (Hrsg.), Stämpflis Handkommentar, Bundesgesetz gegen den unlauteren Wettbewerb (UWG), 2. Aufl., Bern 2016 (zit. SHK-AUTOR)

HÄFELIN ULRICH/HALLER WALTER/KELLER HELEN/THURNHERR DANIELA, Schweizerisches Bundesstaatsrecht, 9. Aufl., Zürich 2016

HÄFELIN ULRICH/MÜLLER GEORG/UHLMANN FELIX, Allgemeines Verwaltungsrecht, 7. Aufl., Zürich/St. Gallen 2016

HARASGAMA REHANA, Erfahren – Wissen – Vergessen: Zur zeitlichen Dimension des staatlichen Informationsanspruchs, Zürich/St. Gallen 2017

HARGITTAI ESZTER/MARWICK ALICE, „What Can I Really Do?", Explaining the Privacy Paradox with Online Apathy, International Journal of Communication 2016, 3737–3757

HÄRTING NIKO, Datenschutz-Grundverordnung, Köln 2016

HAUSHEER HEINZ/AEBI-MÜLLER REGINA E., Das Personenrecht des Schweizerischen Zivilgesetzbuches, 4. Aufl., Bern 2016

HEBERLEIN HORST, in: Ehmann/Martin (Hrsg.), Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, München 2017

HECKENDORN URSCHELER LUKAS/ARONOVITZ ALBERTO/CURRAN JOHN/TOPAZ DRUCKMAN KAREN, Allgemeine Regelungen und die Berücksichtigung neuerer technischer Entwicklungen im Datenschutzrecht, Elektronische Publikationsreihe von Gutachten des Schweizerischen Instituts für Rechtsvergleichung, E-Avis ISDC 2017-07, 3. August 2016

HECKMANN DIRK/PASCHKE ANNE, in: Ehmann/Martin (Hrsg.), Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, München 2017

HOFSTETTER DAVID, Das Verhältnismässigkeitsprinzip als Grundsatz rechtsstaatlichen Handelns (Art. 5 Abs. 2 BV), Diss., Zürich 2017

HONEY KRISTEN/CHROUSOS PHAEDRA/BLACK TOM, My Data: Empowering All Americans with Personal Data Access, 15. März 2016, <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access>, zuletzt besucht am 20. Dezember 2017

HONSELL HEINRICH/VOGT NEDIM PETER/GEISER THOMAS (Hrsg.), Basler Kommentar, Zivilgesetzbuch I, Art. 1–456, 5. Aufl., Basel 2014 (zit. BSK-AUTOR)

HONSELL HEINRICH/VOGT NEDIM PETER/WIEGAND WOLFGANG (Hrsg.), Basler Kommentar, Obligationenrecht I, 6. Aufl., Basel 2015 (zit. BSK-AUTOR)

HÜRLIMANN DANIEL, Suchmaschinenhaftung: Zivilrechtliche Verantwortlichkeit der Betreiber von Internet-Suchmaschinen aus Urheber-, Marken-, Lauterkeits-, Kartell- und Persönlichkeitsrecht, Diss., Bern 2012

JANAL RUTH, Data Portability – A Tale of Two Concepts, JIPITEC 2017, 59–69

JITSUZUMI TOSHIYA, Recent Development of Net Neutrality Conditions in Japan: Impact of Fiber Wholesale and Long-term Evolution (LTE), 26th European Regional Conference of the International Telecommunications Society (ITS), Madrid 24. bis 27. Juni 2015

KAMANN HANS-GEORG/BRAUN MARTIN, in: Ehmann/Martin (Hrsg.), Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, München 2017

KAMLAH WULF, in: Plath (Hrsg.), BDSG/DSGVO, Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen von TMG und TKG, 2. Aufl., Köln 2016

KERNEN ALEXANDER, Volle Verantwortlichkeit des Host Providers für Persönlichkeitsverletzende Handlungen seines Kunden, Jusletter vom 4. März 2013

KIENER REGINA/KÄLIN WALTER, Grundrechte, 2. Aufl., Bern 2013

KLABUNDE ACHIM, in: Ehmann/Martin (Hrsg.), Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, München 2017

KLEINER JAN, Meldepflicht bei Datenschutzverletzungen, digma 2017, 170–175

KLEINER JAN/STOCKER LUKAS, Meldepflichten bei Datenpannen de lege lata und de lege ferenda, digma 2015, 90–94

KLETT BARBARA, Digitalisierte Gesundheit – Abgrenzungen und Regulierung, HAVE 2017, 104–113

KÖRBER SANDRO, Experimentelle Rechtsetzung, LEGES 2015, 385–402

KÖRBER THORSTEN, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, 93–101

LOBSIGER ADRIAN, Digitales Potenzial für Datenschutz, NZZ vom 27. September 2017, <www.nzz.ch/meinung/digitales-potenzial-fuer-datenschutz-ld.1318499>, zuletzt besucht am 20. Dezember 2017

LUNDKVIST CHRISTIAN/HECK ROUVEN/TORSTENSSON JOEL/MITTON ZAC/SENA MICHAEL, uPort: A Platform for Self-Sovereign Identity, Draft, 21. Februar 2017, <https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf>, zuletzt besucht am 20. Dezember 2017

LUTZ PETER, Regulatorische Herausforderung von Bezahlsystemen: PayPal & Co, ZVglRWiss 2017, 177–188

MACDONALD ROGER/LEETARU KALEV, Internet Archive's Virtual Reading Room Empowers Data Mining On A Societal Scale, Knight Foundation, 7. Januar 2014, <www.knightfoundation.org/articles/internet-

archives-virtual-reading-room-empowers-data-mining-societal-scale>, zuletzt besucht am 20. Dezember 2017

MACGILLIVRAY ALEXANDER, Summary of Comments Received Regarding Data Portability, 10. Januar 2017, <https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability>, zuletzt besucht am 20. Dezember 2017

MACGILLIVRAY ALEXANDER/SHAMBAUGH JAY, Exploring Data Portability, 30. September 2017, <https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability>, zuletzt besucht am 20. Dezember 2017

MADER LUZIUS, Evaluating the Effects: A Contribution to the Quality of Legislation, Statute Law Review 22 (2001), 119–131 (zit. „Evaluating the Effects")

MADER LUZIUS, Experimentelle Gesetzgebung, in: Grimm/Maihofer (Hrsg.), Gesetzgebungstheorie und Rechtspolitik, Jahrbuch für Rechtssoziologie und Rechtstheorie, Bd. XIII, Opladen 1988, 211–221 (zit. „Experimentelle Gesetzgebung")

MASTRONARDI PHILIPPE, Experimentelle Rechtsetzung im Bund, ZSR 1991, 449–469

MAURER-LAMBROU URS/BLECHTA GABOR P. (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-AUTOR)

MEIER PHILIPPE, Protection des données: Fondements, principes généraux et droit privé, Bern 2010

NOUREDDINE HUSSEIN, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, 98–108

OHM PAUL, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review 2010, 1701–1777

PAAL BORIS P., in: Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, Beck'sche Kompakt-Kommentare, München 2017

PARRY ELLIS, Subject Access and Data Portability, in: Jay (Hrsg.), Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice, 4. Aufl., London 2017, 231–262

PASQUIER THOMAS/SINGH JATINDER/POWLES JULIA/EYERS DAVID/SETZER MARGO/BACON JEAN, Data provenance to audit compliance with privacy policy in the Internet of Things, Personal and Ubiquitous

Computing 2017, <https://doi.org/10.1007/s00779-017-1067-4>, zuletzt besucht am 20. Dezember 2017, 1–12

PFISTER JOACHIM, Electronic Data Safes – Personal Information Management at the Intersection of Electronic Process Support and User-Managed Access in E-Business and E-Government, Diss., Zürich 2017

PILTZ CARLO, in: Gola (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München 2017

PLATH KAI-UWE, in: Plath (Hrsg.), BDSG/DSGVO, Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen von TMG und TKG, 2. Aufl., Köln 2016

PROCIVIS, val:ID, your data, your asset, Whitepaper v2, < https://valid.global/static/valid-wp-2.pdf (https://valid.global/static/valid-wp-2.pdf>, zuletzt besucht am 20. Dezember 2017

REDDY RAJIDI SATISH CHANDRA/REDDY GOPU SRINIVAS, Enterprise Digital Rights Management for Document Protection, 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2017, <http://ieeexplore.ieee.org/document/7929697>, zuletzt besucht am 20. Dezember 2017

RHINOW RENÉ A./SCHMID GERHARD/BIAGGINI GIOVANNI/UHLMANN FELIX, Öffentliches Wirtschaftsrecht, 2. Aufl., Basel 2011

RIGAMONTI CYRILL P., Providerhaftung – Auf dem Weg zum Urheberverwaltungsrecht?, sic! 2016, 117–134

ROHN PATRICK, Zivilrechtliche Verantwortlichkeit der Internet Provider nach schweizerischem Recht, Zürich 2004

ROSENTHAL DAVID, Der Entwurf für ein neues Datenschutzgesetz, Jusletter vom 27. November 2017

ROSENTHAL DAVID, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, Jusletter vom 20. Februar 2017

ROSENTHAL DAVID, in: Rosenthal/Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich/ Basel/Genf 2008

ROSENTHAL DAVID, Internet-Provider-Haftung – ein Sonderfall?, in: Jung (Hrsg.), Aktuelle Entwicklungen im Haftungsrecht, Bern/Zürich/Basel/Genf 2007, 150–206 (zit. „Haftung“)

ROSENTHAL DAVID, Zivilrechtliche Haftung von Internet-Providern für Unrecht Dritter, sic! 2006, 511–519

RÜD ANDREAS/MICHLIG MATTHIAS, Beweismittelbeschaffung aus Sicht des Geschädigtenvertreters, in: Romerio/Bazzani (Hrsg.), Interne und regulatorische Untersuchungen II, Zürich/Basel/Genf 2016, 151–178

SCHÄFER MARC-FRÉDÉRIC/DORDI ELSA, Über die Rechtfertigung von Persönlichkeitsverletzungen, medialex 2011, 142–148

SCHIESS DAVID/SCHALLER OLIVIER, Online-Plattformen – Chancen und Herausforderungen im Wettbewerbsrecht, in: Thouvenin/Weber (Hrsg.), Werbung – Online, Zürich 2017, 111–130

SCHMIDT-GABAIN FLORIAN, Die Passivlegitimation bei Unterlassungs- und Beseitigungsansprüchen nach Art. 62 Abs. 1 lit. a und b URG – insbesondere bei Urheberrechtsverletzungen im Internet, sic! 2017, 451–467

SCHOCH NIK/SCHÜEPP MICHAEL, Provider-Haftung, «de près ou de loin»?, Jusletter vom 13. Mai 2013

SÉNÉCAL SYLVAIN/FREDETTE MARC/LÉGER PIERRE-MAJORIQUE/COURTEMANCHE FRANÇOIS/RIEDL RENÉ, Consumers' Cognitive Lock-in on Websites: Evidence from a Neurophysiological Study, Journal of Internet Commerce 2015, 277–293

SPECHT LOUISA, Ausschliesslichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2006, 288–296

STAUBER DEMIAN, Web Scraping, Jusletter IT Flash vom 11. Dezember 2017

SUTTER-SOMM THOMAS, Schweizerisches Zivilprozessrecht, 3. Aufl., Zürich/Basel/Genf 2017

SWIRE PETER/LAGOS YIANNI, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, Maryland Law Review 2013, 335–380

SYDOW GERNOT, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, Baden-Baden 2017

THOUVENIN FLORENT, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Weber/Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich/Basel/Genf 2014, 61–83 (zit. „Grundprinzipien")

THOUVENIN FLORENT, Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze, in: Boehme-Nessler/Rehbinder (Hrsg.), Big Data: Ende des Datenschutzes? – Gedächtnisschrift für Martin Usteri, Schriften zur Rechtspsychologie, Bd. 15, Bern 2017, 27–53 (zit. „Big Data")

THOUVENIN FLORENT, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 2017, 21–32

THOUVENIN FLORENT/FRÜH ALFRED/LOMBARD ALEXANDRE, Eigentum an Sachdaten: Eine Standortbestimmung, SZW 2017, 25–34

THOUVENIN FLORENT/WEBER ROLF H., Zum Bedarf nach einem Dateneigentum, Jusletter IT Flash vom 11. Dezember 2017

THOUVENIN FLORENT/WEBER ROLF H./FRÜH ALFRED, Data ownership: Taking stock and mapping the issues, in: Dehmer/Emmert-Streib (Hrsg.), Frontiers in Data Science, Boca Raton 2018, 111–145

TRÜEB HANS-RUDOLF/KEISER BARBARA A., Regulierung und Marktzutritt dritter Zahlungsdienstleister, in: Weber/Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich/Basel/Genf 2015, 161–180

TSAI JANICE Y./EGELMAN SERGE/CRANOR LORRIE/ACQUISTI ALESSANDRO, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Information Systems Research 2011, 254–268

VAN GESTEL ROB/VAN DIJCK GIJS, Better Regulation through Experimental Legislation, European Public Law 2011, 539–553

VASELLA DAVID, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, Jusletter vom 16. November 2015

VASELLA DAVID/SIEVERS JACQUELINE, Der „Swiss Finish“ im Vorentwurf des DSG, digma 2017, 44–49

WALDMANN BERNHARD/BELSER EVA MARIA/EPINEY ASTRID (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015 (zit. BSK-AUTOR)

WEBER ROLF H., Big Data in the Insurance Industry, Jusletter vom 12. Dezember 2016

WEBER ROLF H., Big Data: Herausforderungen für das Datenschutzrecht, in: Epiney/Nüesch (Hrsg.), Big Data und Datenschutzrecht, Zürich 2016, 1–22 (zit. „Datenschutzrecht“)

WEBER ROLF H., Data Portability and Big Data Analytics, New Competition Policy Challenges, Concorrenza e Mercato 2016, 59–72

WEBER ROLF H./CHROBAK LENNART, Rechtsinterdisziplinarität in der digitalen Datenwelt, Jusletter vom 4. April 2016

WEBER ROLF H./THOUVENIN FLORENT, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 2018, 41–71

WHITTAKER ZACK, AdultFriendFinder network hack exposes 412 million accounts, ZDNet vom 13. November 2016, <http://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users/>, zuletzt besucht am 20. Dezember 2017

WIDMER BARBARA, Das elektronische Patientendossier – ein Mammutprojekt wird Realität, AJP 2017, 765–779

WIDMER MICHAEL, Informations- und Meldepflichten bei der Bearbeitung von Personendaten, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, 121–147 (zit. „Personendaten“)

WIDMER MICHAEL, Rechte der Datensubjekte, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, 149–165 (zit. „Datensubjekte“)

WIEBE ANDREAS, Von Datenrechten zu Datenzugang – Ein rechtlicher Rahmen für die europäischen Datenwirtschaft, CR 2017, 87–93

WORLD ECONOMIC FORUM, Personal data: The emergence of a new asset class, Januar 2011 (zit. „Personal Data“)

WORLD ECONOMIC FORUM, Rethinking personal data: A new lens for strengthening trust, Mai 2014 (zit. „Rethinking“)

ZANFIR GABRIELA, The right to Data portability in the context of the EU data protection reform, International Data Privacy Law 2012, 149–162

ZECH HERBERT, „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151–1160

ZECH HERBERT, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“, CR 2015, 137–146

ZECH HERBERT, Information als Schutzgegenstand, Tübingen 2012

ZERDICK THOMAS, in: Ehmann/Martin (Hrsg.), Beck’sche Kurz-Kommentare, Datenschutz-Grundverordnung, München 2017

F. MATERIALEN

ARTIKEL-29-GRUPPE, Guidelines on the right to data portability, WP 242 rev.01, 5. April 2017

AUTORITÉ DE LA CONCURRENCE/BUNDESKARTELLAMT, Competition Law and Data, Mai 2016

Botschaft zum Bundesgesetz über das elektronische Patientendossier (EPDG) vom 29. Mai 2013, BBl 2013 5321 (zit. „Botschaft EPDG“)

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 413 (zit. „Botschaft DSG“)

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 (zit. „Botschaft DSG“)

BUNDESAMT FÜR JUSTIZ, Änderung von Art. 12 Abs. 2 lit. a DSG: Auslegungshilfe, 10. Oktober 2006, <https://www.edoeb.admin.ch/datenschutz/00628/00784/index.html?lang=de> (zit. „Auslegungshilfe“)

BUNDESAMT FÜR JUSTIZ, Erläuternder Bericht zum Vorentwurf Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz), 22. Februar 2017 (zit. „Erläuternder Bericht“)

BUNDESAMT FÜR JUSTIZ, Kommentar zur Vollzugsverordnung vom 14. Juni 1993 (Stand am 1. Januar 2008) zum Bundesgesetz über den Datenschutz (VDSG, RS 235.11), 14. Juni 2011 <https://www.edoeb.admin.ch/org/00129/index.html?lang=de> (zit. „Kommentar“)

BUNDESKARTELLAMT, Arbeitspapier „Marktmacht von Plattformen und Netzwerken“, Ergebnisse und Handlungsempfehlungen, Juni 2016

BUNDESRAT, Auf dem Weg zu einer Datenpolitik des Bundes, Medienmitteilung vom 22. März 2017, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-66068.html>, zuletzt besucht am 20. Dezember 2017 (zit. „Datenpolitik des Bundes“)

BUNDESRAT, Die zivilrechtliche Verantwortlichkeit von Providern, Bericht des Bundesrates vom 11. Dezember 2015, <www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/ber-br-d.pdf>, zuletzt besucht am 20. Dezember 2017 (zit. „Bericht zivilrechtliche Verantwortlichkeit von Providern“)

BUNDESRAT, Rechtliche Basis für Social Media, Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29. September 2011 (zit. „Bericht Social Media“)

COMMISSION DES AFFAIRES EUROPÉENNES, Rapport d’information N° 3366 portant observations sur le projet de loi pour une République numérique (n° 3318) vom 16. Dezember 2015

COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS, Consultation publique sur le Règlement européen sur la protection des données, Synthèse des contributions, Ort 2016

DIRECTION DES AFFAIRES JURIDIQUES, Rapport relatif à la mise en application de la Loi N°2016-1321 du 7 octobre 2016 pour une République Numérique vom 11. Mai 2017

EDÖB, Datenschutzaspekte beim Internetprotokoll IPv6, Mai 2016, <https://www.edoeb.admin.ch/datenschutz/00683/01350/01351/index.html>, zuletzt besucht am 16. November 2017 (zit. „Internetprotokoll IPv6")

EDÖB, Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetzes über den Datenschutz (DSG), Oktober 2007 (zit. „Erläuterungen")

EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, August 2015 (zit. „Leitfaden Massnahmen")

EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE, Stellungnahme 9/2016, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20. Oktober 2016, <https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_de>, zuletzt besucht am 20. Dezember 2017 (zit. „Stellungnahme")

EUROPÄISCHE KOMMISSION, An emerging offer of „personal information management services" – Current state of service offers and challenges, 23. November 2016, <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118>, zuletzt besucht am 20. Dezember 2017 (zit. „Personal information management services")

EUROPÄISCHE KOMMISSION, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, SWD(2017) 2 final, 11. Januar 2017 (zit. „Staff Working Document on the Free Flow of Data")

EUROPÄISCHE KOMMISSION, Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDEV 2.1/6, 15. Juli 2016 (zit. „Guidelines")

EUROPÄISCHE KOMMISSION, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Aufbau einer Europäischen Datenwirtschaft, COM(2017) 9 final, 10. Januar 2017 (zit. „Aufbau einer Europäischen Datenwirtschaft")

EUROPÄISCHE KOMMISSION, 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, COM(2017) 10 final, 10. Januar 2017 (zit. „Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation“)

EUROPÄISCHE KOMMISSION, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union, COM(2017) 495 final, 13. September 2017 (zit. „Vorschlag für eine Verordnung über freien Verkehr nicht personenbezogener Daten“)

EUROPÄISCHE KOMMISSION, 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), 2012/11 COD, 25. Januar 2012 (zit. „Vorschlag Datenschutz-Grundverordnung“)

EUROPÄISCHES PARLAMENT, AUSSCHUSS FÜR BÜRGERLICHE FREIHEITEN, JUSTIZ UND INNERES, Entwurf eines Berichts über den 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), 2012/0011(COD), 16. Januar 2013, <www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fDE>, zuletzt besucht am 20. Dezember 2017 (zit. „Entwurf”)

JAPAN FAIR TRADE COMMISSION, COMPETITION POLICY RESEARCH CENTER, Report of Study Group on Data and Competition Policy, Tentative Translation, 6. Juni 2017

KANTON SCHAFFHAUSEN, PROCIVIS und der Kanton Schaffhausen präsentieren eID-Lösung am *eGovernment Day* Schaffhausen, News vom 4.12.2017, <https://www.sh.ch/index.php?id=316&no_cache=1&tx_ttnews%5Btt_news%5D=3440&cHash=7320b8df237456f9e51f8fd5b3f6462b>, zuletzt besucht am 20. Dezember 2017

KANTON ZUG, Gerichts- und Verwaltungspraxis GVP 2012, <https://www.zg.ch/behoerden/staatskanzlei/kanzlei/gvp/gvp-2012>, zuletzt besucht am 20. Dezember 2017

OFFICE OF EDUCATIONAL TECHNOLOGY, MyData Open Data Specification, Version 1.3, 22. Mai 2012, <https://tech.ed.gov/files/2012/05/MyDataOpenDataSpecificationv1.3.pdf>, zuletzt besucht am 20. Dezember 2017

OFFICE OF MANAGEMENT AND BUDGET, Circular No. A-130, Managing Information as a Strategic Resource, 28. Juli 2016, <https://a130.cio.gov/>, zuletzt besucht am 20. Dezember 2017

STADT ZUG, Blockchain-Identität für alle Einwohner, 7. Juli 2017, <http://www.stadtzug.ch/de/ueberzug/ueberzugrubrik/aktuelles/aktuellesinformationen/?action=showinfo&info_id=383355>, zuletzt besucht am 20. Dezember 2017

SWISSMEDIC, Merkblatt für eigenständige Medizinprodukte-Software, Fassung vom 15. Dezember 2016

WEKO, Recht und Politik des Wettbewerbs, RPW 2011, <https://www.weko.admin.ch/weko/de/home/dokumentation/recht-und-politik-des-wettbewerbs--rpw-.html>, zuletzt besucht am 20. Dezember 2017