Zeitschrift für Datenrecht und Informationssicherheit

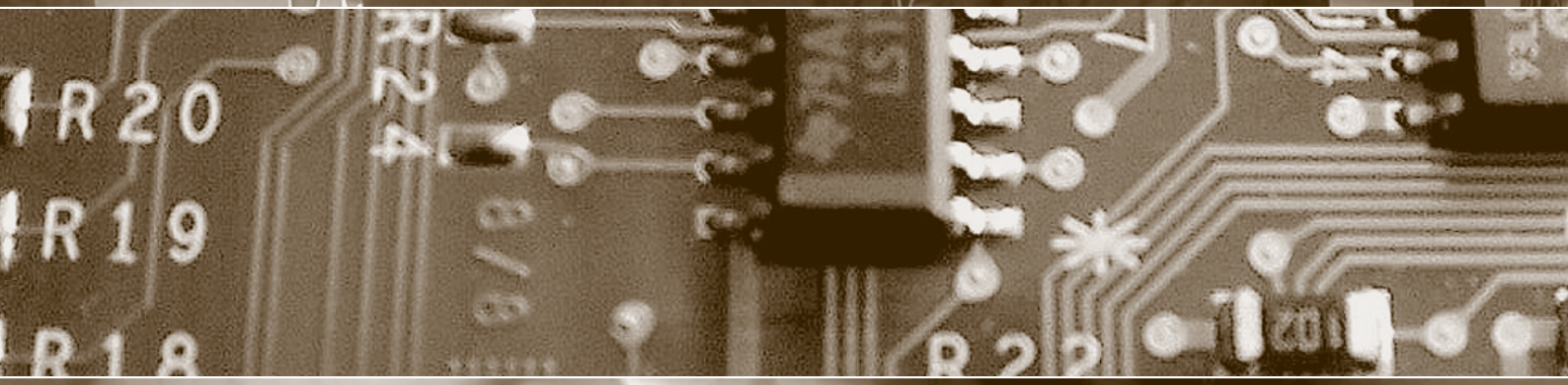
digma

www.digma.info 19. Jahrgang, Heft 4, Dezember 2019

Schwerpunkt:

Rechte an Daten

fokus: Datennutzung und Datensouveränität
fokus: Datenmärkte ohne «Dateneigentum»
report: Datenschutz auf der Intensivstation



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Rechte an Daten

Informationelle Selbstbestimmung

Was leistet das Datenschutzrecht für die Selbstbestimmung der Betroffenen? Welche Kontrollrechte sieht das DSG vor, und sind sie in der heutigen Zeit grundsätzlich überhaupt noch in der Lage, Datenkontrolle zu gewährleisten?

Datenmärkte ohne «Dateneigentum»

Das Datenschutzrecht ermöglicht den Handel mit Personendaten, schränkt ihn andererseits aber auch ein. Könnte die freie Widerrufbarkeit der datenschutzrechtlichen Einwilligung eingeschränkt werden, um den Handel zu fördern?

Sozialpflichtigkeit von Gesundheitsdaten

Damit der Forschung mehr Gesundheitsdaten zur Verfügung stehen, wird die Einführung einer generellen Widerspruchslösung gefordert. Ist das mit dem geltenden Recht und den Grundwerten unserer demokratischen Gesellschaft vereinbar?

Herausforderungen der Datenlöschung

Sensitive Daten müssen, wenn erforderlich, sicher gelöscht werden. Aber nicht immer ist es offensichtlich, ob diese Löschung irreversibel ist.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, Dr. iur. Dominika Blonski

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: 4-mal jährlich (März, Juni, September, Dezember)

Bezugsbedingungen: Jahresabonnement: CHF 178.00 (für Studierende: CHF 98.00), Einzelheft: CHF 48.00, zzgl. Versandkosten. Alle Abo-Preise inkl. 2,5% MWST, zzgl. Versandkosten von CHF 6.00 innerhalb der Schweiz (Versandkosten für Lieferung ins Ausland: CHF 31.00). Studentenpreis gegen Vorlage eines gültigen Nachweises. Abonnementkündigungen sind mit einer Frist von 8 Wochen zum Ende des berechneten Bezugsjahres möglich.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa, Tel. +41 (0)44 928 56 17, marc.schaettin@fachmedien.ch

Verlag und Kundenservice: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Datenschutz auf der Intensivstation

Ein bewusst provokativer Befund eines Privatrechtlers: Das geltende (und künftige) Datenschutzrecht ist nicht in der Lage, die heutigen Probleme überzeugend zu lösen. Wie sähen erste Schritte hin zu einem neuen Ansatz aus?

Vertrauensstiftende Videoüberwachung?

Kann ein soziotechnisches Konzept, das eine reversible Anonymisierung von Bilddaten mit einer Kontrollinstanz kombiniert, die berechtigten Bedenken gegenüber Videoüberwachung überwinden helfen?

Aus den Datenschutzbehörden

Wer hat an der Internationalen Konferenz der Datenschutzbeauftragten eine Auszeichnung erhalten? Wer diskutiert über Social Media und Fake News am ZFF Talk? Wer gewinnt den Datenschutz-Video-Wettbewerb 2019 des Datenschutzbeauftragten des Kantons Zürich? Und wer bietet neu eine Nachdiplom-Masterausbildung an?

Quo vadis KI? Neue OECD-Grundsätze

Künstliche Intelligenz fordert den Regulator heraus. Was sagen die neuen Grundsätze der OECD dazu? Und wo steht die Schweiz?

Gelöscht. Gelöscht?

Löschen. Gelöscht? Unser Cartoonist zeigt, was bleibt …

report

forum

Das Recht auf Datenportabilität

Ein neues datenschutzrechtliches Instrument: Inhalt, Gegenstand sowie Hinweise zur Umsetzung in der Praxis

Christian Laux, Dr. iur., LL.M. (Stanford), Rechtsanwalt, Partner, Laux Lawyers AG, Zürich christian.laux@lauxlawyers.ch

Das Recht auf Datenportabilität stellt ein Novum für das Datenschutzrecht dar. Gegner bezeichnen die Datenportabilität als gesetzgeberisches Experiment.

Am 25. Mai 2018 ist die Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Eines der Betroffenenrechte ist das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Auch in der Schweiz wird derzeit über ein revidiertes Datenschutzgesetz beraten[1]. Die Staatspolitische Kommission des Nationalrats (SPK-N) hat am 16. August 2019 vorgeschlagen, den Grundsatz der Datenportabilität in das DSG aufzunehmen. In der Schlussabstimmung der Herbstsession 2019, d.h. am 25. September 2019, hat der Nationalrat die Art. 25a und Art. 25b EDSG, wie von der Mehrheit der SPKN vorgeschlagen[2], unverändert übernommen: «(1) Jede Person kann vom Verantwortlichen kostenlos die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen, wenn: a. der Verantwortliche die Daten automatisiert bearbeitet; und b. die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden. (2) Die betroffene Person kann zudem vom Verantwortlichen verlangen, dass er ihre Personendaten einem anderen Verantwortlichen überträgt, wenn die Voraussetzungen gemäss Absatz 1 erfüllt sind und dies keinen unverhältnismässigen Aufwand erfordert …».

Das Recht auf Datenportabilität stellt ein Novum für das Datenschutzrecht dar, sowohl in der Europäischen Union[3] als auch in der Schweiz. Schutzziel der Regelung betreffend Datenportabilität ist mehr als nur, Transparenz zugunsten der betroffenen Person zu schaffen[4]: Die Bestimmung erlaubt einen Paradigmenwechsel im Datenschutzrecht. Der Paradigmenwechsel besteht darin, dass die betroffene Person über einen gewissen Zeitraum eine vollständige Sammlung von Angaben über sich selber anhäufen und in Personal-Information-Management-Systemen (sog. PIMS) verwalten kann (ähnlich wie heute Geld auf einem Bankkonto). So würde die betroffene Person über einen gewissen Zeitraum eine wertvolle Ansprechpartnerin mit Gesamtsicht, wenn es um deren persönliche Angaben geht – während Plattformen oft nur einen sektoriellen Blick auf die betroffene Person erhalten.

Andere stehen dem neuen Instrument skeptisch[5] gegenüber. Die Gegner bezeichnen die Datenportabilität als gesetzgeberisches Experiment. Diese Bezeichnung ist insofern nicht falsch, als die Datenportabilität sowohl gemäss DSGVO als auch gemäss EDSG (Fassung des Nationalrats von Ende September 2019) auf offene Rechtsbegriffe abstellt[6]: «in einem strukturierten, gängigen und maschinenlesbaren Format» (DSGVO) bzw. «in einem gängigen elektronischen Format» (EDSG). Soweit solche Standards fehlen, dürfte der Anspruch kaum durchsetzbar sein (siehe dazu unten, 169). Es wird kritisiert, dass die Datenportabilität nach Massgabe der DSGVO *in abstrakter Weise* gegen Lock-in-Effekte von grossen Anbietern wirkt und nicht erst dann, wenn ein Marktteilnehmer seine mächtige Stellung ausnutzt bzw. der Markt sonst nicht funktioniert[7].

Erscheinungsformen der Datenportabilität

«Datenportabilität» kennt nach dem Konzept der DSGVO und des EDSG zwei Spielarten:

- Beim *Recht auf Kopie* geht es um eine Direktbeziehung zwischen dem datenverarbeitenden Verantwortlichen und der betroffenen Person. Das Recht auf Kopie wird in der DSGVO bzw. dem EDSG wie folgt umschrieben: «Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt

hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu *erhalten*» (DSGVO) sowie «vom Verantwortlichen kostenlos die *Herausgabe* ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format zu verlangen» (E-DSG).

■ Demgegenüber geht es beim *Recht auf Datenübertragung* um eine Dreiecksbeziehung. Die betroffene Person hat einen Anspruch gegen den datenverarbeitenden Verantwortlichen, die vom Recht erfassten Daten auf einen Dritten übertragen zu sehen. Das Recht auf Datenübertragung wird in der DSGVO bzw. dem EDSG wie folgt umschrieben: «Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu *übermitteln*» (DSGVO); «vom Verantwortlichen verlangen, dass er ihre Personendaten einem anderen Verantwortlichen *überträgt*» (EDSG).

Wenn fortan vom Anspruch auf Datenportabilität gesprochen wird, meint dies jeweils beide Spielarten, ausser dort, wo dies besonders bezeichnet ist oder der Kontext klar auf die eine oder andere Spielart hinweist.

Inhalt und Gegenstand des Anspruchs auf Datenportabilität

Inhalt und Gegenstand des Anspruchs sollen hier nur kurz umrissen werden. Für eine detaillierte Beschreibung der einzelnen Ansprüche und des Gegenstands der Datenportabilität wird auf die einschlägigen Kommentare verwiesen.

Inhalt

Der Anspruch der betroffenen Person auf Datenportabilität richtet sich gegen den Verantwortlichen[8], der die Daten im Zeitpunkt der Geltendmachung des Anspruchs kontrolliert (und nur diesen, der Auftragsbearbeiter ist nicht passivlegitimiert). Sowohl nach Massgabe der DSGVO als auch des EDSG treffen den Verantwortlichen *drei Hauptpflichten:* Erstens muss der Verantwortliche Daten bereitstellen[9], die den Formatanforderungen (zu diesen sogleich) genügen *(Herausgabepflicht);* erfüllt das IT-System, das der Verantwortliche zur Verarbeitung der Personendaten einsetzt, die Formatanforderungen nicht, muss er, zweitens, die herauszugebenden Daten in ein genügendes Zielformat umwandeln *(bedingte Umwandlungspflicht);* drittens darf der Verantwortliche die Weiternutzung der von ihm bereitzustellenden Daten nicht behindern *(Behinderungsverbot[10]).* Diese Pflichten sind nicht kontextabhängig, sondern gelten abstrakt[11].

Negativ gesprochen hat der Verantwortliche *keine Pflicht zum Umbau eigener Systeme*[12], *keine Pflicht zur Ermöglichung von (dauerhafter) Interoperabilität* seiner IT-Systeme mit jenen des Empfängers (Bereitstellen von Application Programming Interfaces, API) und *keine Pflicht zur Einbindung einheitlicher Übermittlungsprotokolle* in die herauszugebenden Datensätze.

Bei der Datenübertragung hat die betroffene Person einen Anspruch gegen den datenverarbeitenden Verantwortlichen, die Daten auf einen Dritten übertragen zu sehen.

Es zeigt sich nach dem Vorstehenden, dass es für das Verständnis der Rechtsfolgen massgeblich darauf ankommt, wie weit die Formatanforderungen gehen. Das E-DSG unterscheidet sich in Bezug auf die Formatanforderungen von der DSGVO, was in der Praxis wohl aber ohne Folgen bleiben dürfte (E-DSG: gängig und elektronisch; DSGVO: gängig, maschinenlesbar und strukturiert).

Gegenstand

Nur elektronisch-digitale Personendaten sind Gegenstand des Anspruchs auf Datenportabilität (keine Paper Records, keine anonymisierten Daten[13]). Die frühere Artikel 29-Datenschutzgruppe hat «Leitlinien zum Recht auf Datenübertragbarkeit» erlassen (WP242 rev.01 vom 13. Dezember 2016, überarbeitete Fassung vom 5. April 2017). Der mit der DSGVO begründete Europäische Datenschutzausschuss hat diese Leitlinien in seiner ersten Plenarsitzung bestätigt[14]. Bei Beurteilung des Anspruchs auf Datenportabilität sollten diese Leitlinien jeweils mitberücksichtigt werden. Gerichtsent-

Kurz & bündig

Die Konturen des neuen Rechts auf Datenportabilität sind zwar noch zu schärfen, aber die Datenschutzpraktiker blicken bereits jetzt gespannt auf die Möglichkeiten, die sich aus dem neuen Instrument ergeben. Mit der Datenportabilität kommt es zu einem Paradigmenwechsel im Datenschutzrecht: Statt formeller Compliance-Massnahmen (wie z.B. Mitteilungspflichten und Dokumentationsvorschriften) erhält die betroffene Person ein Instrument, um zu einer interessanten Anlaufstelle zu werden, wenn es um die eigenen Personendaten geht. Die betroffene Person wird mit der Datenportabilität ganz pointiert ins Zentrum gestellt. Deswegen muss die Datenportabilität als genuin datenschutzrechtliches Instrument verstanden werden. Es geht nicht nur um konsumentenschützerische bzw. wettbewerbspolitische Ziele.

scheide zur Datenportabilität sind zum Stand heute soweit ersichtlich nicht verfügbar. Daraus ergibt sich, dass einerseits (anspruchsbegründend) das Kriterium der Speicherursache massgeblich ist, andererseits aber (einschränkend) das Kriterium des Verarbeitungsgrunds zu berücksichtigen ist:

Kriterium der Speicherursache[15]

Wenn man dem WP242 rev.01 folgt (was jedoch nicht herrschende Lehre ist), sind nur direkt durch die betroffene Person *bereitgestellte Daten*[16] und vom Verantwortlichen bei der Nutzung durch die betroffene Person *beobachtete Daten*[17] herauszugeben. Vom Anspruch auf Datenportabilität sind demgegenüber abgeleitete Daten (z.B. Kredit-Scoring-Datenbanken, Bewegungsprofile, welche die Telekomanbieterin erstellt, wenn sie Mobilfunknutzer in ein Netz bzw. Mobilfunkzellen einwählen) ausgenommen. Nach der hier vertretenen Meinung ist auch *Archivgut*[18] zum Nachweis jener Transaktionen, die den aktuellen Datenbestand erst begründet haben, nicht mitzuliefern.

Der Verantwortliche hat keine Pflicht zum Umbau eigener Systeme, zur Ermöglichung von Interoperabilität seiner IT-Systeme und zur Einbindung einheitlicher Übermittlungsprotokolle.

Kriterium des Verarbeitungsgrunds

Der Anspruch auf Datenportabilität wird durch den zugrunde liegenden Verarbeitungsgrund beschränkt. Bereitgestellte Daten und beobachtete Daten sind dann nicht Gegenstand des Anspruchs, wenn der Verantwortliche sie auch unabhängig von der Mitwirkung der betroffenen Person verarbeiten darf oder muss (z.B. gesetzliche Pflicht zur Datenverarbeitung; Wahrung berechtigter eigener Interessen des Verantwortlichen)[19]. Der Anspruch auf Datenportabilität besteht gemäss ausdrücklicher Regelung (Art. 25 Abs. 1 lit. b EDSG; Art. 20[1][a] DSGVO) nur, wenn der Verantwortliche die Personendaten mit Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages zwischen ihm und der betroffenen Person bearbeitet[20].

Praktische Umsetzung des Anspruchs

Geltendmachung des Anspruchs auf Datenportabilität

Der Verantwortliche hat sich von der Identität und der Befugnis desjenigen, der das Recht geltend macht, zu überzeugen[21].

Behandlung eines Anspruchs auf Datenportabilität

Der Verantwortliche, der einen Anspruch einer betroffenen Person auf Datenportabilität zu prüfen hat, behandelt diese am besten wie eine andere Verantwortliche.[22] In Bezug auf «bereitgestellte Daten» darf der Verantwortliche davon ausgehen, dass die betroffene Person zur Bereitstellung der Personendaten berechtigt war (vorbehalten sind klare Anzeichen auf einen Missbrauch).

Der Verantwortliche darf im Sinne einer natürlichen Vermutung auch davon ausgehen, dass die betroffene Person die von ihr bereitgestellten Daten wieder herausverlangen darf (oder die Übertragung an einen Dritten verlangen darf). Bei «beobachteten Daten» wird dies gleichermassen der Fall sein, aber nur in Bezug auf Angaben, die der anspruchsberechtigten betroffenen Person ohnehin bereits erkennbar waren (z.B. im Rahmen der Nutzung des Dienstes, welchen der Verantwortliche bereitstellt). Nur insoweit kann man von einer Pflicht des Verantwortlichen sprechen, Datensätze bei sich «entflechten» zu müssen[23].

Angaben mit Bezügen zu Drittpersonen

Nach dem EDSG soll eine betroffene Person nur «ihre Personendaten» herausverlangen können, nach der DSGVO nur «die sie betreffenden personenbezogenen Daten».[24] Dass Angaben über Dritte Teil der Persönlichkeitssphäre einer anderen Person werden können, ist selbstverständlich[25], was in der Diskussion über das Recht auf Datenportabilität aber mitunter vergessen geht[26]. Das Recht auf Datenportabilität besteht somit auch in Bezug auf Angaben über Drittpersonen, wenn solche Angaben berechtigterweise in die Sphäre der anspruchsberechtigten betroffenen Person gelangt sind. Aus Sicht des passivlegitimierten Verantwortlichen ist zentral, dass er keine Rechte und Freiheiten anderer Personen beeinträchtigt (namentlich von Dritten, die in den vom Berechtigten herausverlangten Angaben beschrieben sind). Dies ergibt sich sowohl aus der DSGVO (Art. 20 Abs. 4 DSGVO als auch aus dem EDSG (Art. 25*b* Abs. 1 EDSG).

Das bedeutet zum Beispiel, dass die betroffene Person von einer Bank nur eigene Banktransaktionen herausverlangen kann (der Anspruch umfasst aber alle der Bank mitgeteilten Angaben über Empfänger von Überweisungen, Kommentare etc.). Ebenfalls sind herauszugeben (im Szenario «Social Media Account»): Kontakte zu anderen Personen eines sozialen Netzwerks (teilweise, d.h., nur soweit die eigene Sicht darauf betroffen ist: «erhaltene Einladungen»), Chatprotokolle[27], empfangene und ver-

sandte Nachrichten in einem Messengerdienst. Herauszugeben sind auch Verlaufangaben über ein- und ausgegangene Telefongespräche über das Telefon des Berechtigten (so im Szenario «Telefonie»). Nicht herauszugeben sind demgegenüber (im Szenario «Social Media Account»): Angaben aus dem Facebook-Account eines «Freunds» oder sonstigen Kontakts oder Angaben, welche die Beziehung zwischen zwei Personen aus der Warte der «Gegenseite» beschreiben.

Verwendung der herausgegebenen Daten durch den Empfänger

Wenn Aufzeichnungen mit Angaben über eine Drittperson auf Wunsch der betroffenen Person an einen neuen Verantwortlichen übermittelt werden, darf dieser neue Verantwortliche die Aufzeichnungen nicht für Zwecke verarbeiten, die die Rechte und Freiheiten der anderen Personen beeinträchtigen (Art. 20[4] DSGVO)[28]. Dies kann in der Praxis zum Beispiel bedeuten, dass der empfangende Verantwortliche die erhaltenen Daten mit einer Kennzeichnung versehen muss (Flags, Tagging), damit sichergestellt ist, dass er diese Daten nicht für seine Marketingaktivitäten oder für sonstige Zwecke einsetzt, ohne dafür die Rechtmässigkeitsprüfung vorgenommen zu haben[29].

Im Einzelfall kann ein Verantwortlicher sich gehalten sehen, Angaben über die betroffene Person erst dann einem Dritten zu übermitteln, wenn er gegenüber seiner Vertragspartnerin (der anspruchsberechtigten betroffenen Person) sichergestellt hat, dass er selber ihr gegenüber keine Vertragsverletzung begeht[30]. Dies kann insbesondere im Kontext von besonderen Geheimnispflichten der Fall sein, wenn der Verantwortliche im Fall einer unsorgfältigen Weiterleitung von Personendaten an einen (wenig vertrauenswürdigen) Dritten ein Haftungsrisiko hätte (Szenario: Wechsel der Bankbeziehung).

Keine Löschung beim ersten Verantwortlichen

Der Verantwortliche, der zur Übertragung von Daten der anspruchsberechtigten betroffenen Person aufgefordert wurde, behält die bei ihm gespeicherten Daten unverändert (siehe Erwägungsgrund 68, Satz 9, zur DSGVO), es sei denn, die betroffene Person würde ihren Löschanspruch geltend machen (Art. 17 DSGVO oder Art. 28 Abs. 2 EDSG).

Keine Vertragsauflösung zum ersten Verantwortlichen

Wer den Anspruch auf Datenportabilität geltend macht, bringt damit nicht zum Ausdruck, dass er die Vertragsbeziehung zum ersten Verantwortlichen kündigen will[31].

Durchsetzbarkeit des Anspruchs bei Fehlen von standardisierten Formaten

Da sich der Anspruch auf Datenportabilität letztlich nur auf die Bereitstellung von Daten unter Einhaltung der Formatanforderungen (dazu vorn, Ziffer III) bezieht, stellt die Regelung bereits per se keine allzu strengen Anforderungen auf[32]. Hinzu kommt Folgendes: Soweit standardisierte Formate in einer Branche fehlen, lässt sich der Anspruch nach Art. 20 DSGVO bzw. Art. 25*a* ff. EDSG nicht vollständig durchsetzen. Eine gefestigte Praxis ist dazu heute allerdings noch nicht verfügbar.

Der zur Übertragung aufgeforderte Verantwortliche behält die bei ihm gespeicherten Daten, es sei denn, die betroffene Person würde ihren Löschanspruch geltend machen.

Nach der hier vertretenen Auffassung reduziert sich der Anspruch auf Datenportabilität bei Fehlen von standardisierten Datenformaten auf einen Herausgabeanspruch im Rahmen des ohne Weiteres Machbaren. Der Verantwortliche muss m.E., wenn er einen Antrag betreffend Datenportabilität zu erfüllen hat, Personendaten auch dann «datenmässig» herausgeben, wenn standardisierte Datenformate fehlen («datenmässige Herausgabe», hier verstanden als Gegensatz zur blossen Information darüber, welche Daten der Verantwortliche gespeichert hält, wie es z.B. nach Art. 15 Abs. 1 DSGVO ausreichend wäre; eine solche blosse Information würde nicht genügen). Es muss aber bei einer solchen datenmässigen Herausgabe auf jeden Fall genügen, wenn der Verantwortliche die Daten in einem der folgenden Formate herausgibt: In Textform darstellbare Angaben können in einem *Tabellenkalkulationsblatt,* das von aktuellen Office-Programmen gelesen und weiterverarbeitet werden kann, *oder* einer *Text-Datei mit Strukturelementen* (namentlich sog. Comma Separated Value-Files sind ausreichend) *oder* einer *XML-Datei* herausgegeben werden (die Aufzählung schliesst andere Formate nicht aus, soweit diese die Weiterverarbeitung der Daten in ähnlicher Weise wie die genannten Formate ermöglichen). Soweit der Verantwortliche – meist in Ergänzung dazu – Dateien in im Wesentlichen unstrukturiertem Format bei sich hält (Bilddateien wie z.B. Röntgenbilder etc.), sind diese in unveränderter

Form (mit) herauszugeben (eine Umformatierung ist entsprechend nicht geschuldet).

Würdigung

Das Recht auf Datenportabilität ist ein neues Instrument. Es liegt in der Natur der Sache, dass seine konkrete Handhabung in der Praxis noch nicht gefestigt ist. Der vorliegende Beitrag versucht, das Institut zu schärfen und berichtet von ersten Erkenntnissen dazu, wie das neue Institut in der Praxis umgesetzt werden könnte. Rechtsprechung fehlt jedoch noch, weswegen noch nicht absehbar ist, ob sich das neue Instrument in der Hand der betroffenen Person bewährt. Kurz: Die Konturen des Instruments sind weiterhin zu schärfen.

Das Recht auf Datenportabilität verspricht einen Paradigmenwechsel insofern, als die betroffene Person Instrumente an die Hand bekommt, selber in die Datenwirtschaft einzugreifen. Wenn das Recht auf Datenportabilität rege genutzt wird, könnten bestehende Plattformeffekte durchbrochen werden, indem der betroffenen Person die Migration in Konkurrenzprodukte zu bestehenden Anbietern erleichtert wird[33]. Es besteht durchaus berechtigte Hoffnung, dass dadurch die betroffene Person stärker ins Zentrum rückt. Dies ist zu begrüssen, dies umso mehr, als zwar die Konturen des Instruments noch zu schärfen sind, es aber ohne erhöhte Compliance-Massnahmen wie unnötige Melde-, Hinweis- oder Aufklärungspflichten auskommt. Insofern erscheint das Recht auf Datenportabilität als ein stark vom freiheitlichen Gedanken geprägtes Instrument. Auch dies kann als willkommene Neuerung in der Datenschutzlandschaft anerkannt werden. Auf jeden Fall ist das Recht auf Datenportabilität ein Signal des Gesetzgebers, dass der Fokus in Zukunft auf die betroffene Person zu legen ist. Mit Blick auf diese Überlegung ist dem oft gehörten Argument entgegenzutreten, dass der Anspruch auf Datenportabilität v.a. ein wettbewerbspolitisches oder allgemein verbraucherschützendes Ziel verfolge[34]. Dem ist nicht so: Die Datenportabilität öffnet die Türe zu einem datenschutzrechtlichen Paradigmenwechsel.

Abzuwarten bleibt nur noch, ob sich das Instrument in der Praxis bewährt. So oder so: Datenschutzrecht bleibt spannend! ■

Fussnoten

1 Geschäft mit der Nummer 17.059, Materialien dazu finden sich unter dem Stichwort auf parlament.ch (<https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/ratsunterlagen?AffairId=20170059&k=PdAffairId:20170059>) (letztmals besucht: 15.10.2019).

2 Die Minderheit (Glättli) verlangt die Datenportabilität statt nur für «Personendaten, die sie [d.h. die betroffene Person] ihm [d.h. dem Verantwortlichen] bekanntgegeben hat» generell für alle Personendaten (Stand 25.9.2019).

3 Jülicher Tim/Röttgen Charlotte/v. Schönfeld Max, ZD 2016, 358 (359); Dehmel/Hullen, ZD 2013, 147 (153).

4 Erwägungsgrund 68 der DSGVO lautet wie folgt: «Um im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, sollte die betroffene Person außerdem berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln.»

5 <https://www.economiesuisse.ch/de/artikel/gesetzliche-datenportabilitaet-instrument-mit-unliebsamen-nebenwirkungen>.

6 Soweit ersichtlich wird das Recht auf Datenportabilität sonst nur noch in Kalifornien unter dem California Consumer Privacy Act of 2018 (CCPA) angesprochen, dort jedoch deutlich weniger weitgehend. Die dortige Formulierung lautet wie folgt: «1798.100 (d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information *may* be delivered *by mail or electronically,* and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period. 1798.100 (e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.» [Hervorhebung nicht im Original]. Der CCPA hat jedoch anders als die DSGVO und das DSG (auch das EDSG) einen eingeschränkten Anwendungsbereich: Es ist nur anwendbar auf Unternehmen, die (i) einen Umsatz von 25 Mio. USD erzielen oder (ii) auf Data Brokers [wobei es diesbezüglich gewisse «de minimis»-Regeln gibt]. Das Recht bezieht sich nicht auf Daten, die öffentlich zugänglich sind («‹Personal information› does not include publicly available information»).

7 Swire Peter/Lagos Yianni, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Md. L.Rev. 335 (2013), 350; <http://digitalcommons.law.umaryland.edu/mlr/vol72/iss2/1>.

8 Der Begriff des «Verantwortlichen» ist umfassend zu verstehen. Der Anspruch richtet sich gegen jeden Verantwortlichen, nicht nur gegen solche, die einen «Dienst der Informationsgesellschaft» anbieten (sprich: Online-Anbieter): Piltz, in: Gola (Hrsg.), Datenschutz-Grundverordnung, München 2017, DSGVO 20 N 6.

9 Der Anspruch auf Datenportabilität ist jedoch erst erfüllt, wenn die relevanten Daten in den Verfügungs- und Machtbereich des angegebenen Empfängers fallen (betroffene Person direkt oder – auf Geheiss der betroffenen Person – empfangener Verantwortlicher), Piltz Carlo (Fn. 8), DSGVO 20 N 8.

Fussnoten (Fortsetzung)

10 Zu denken ist an Hindernisse technischer oder rechtlicher Art: Herbst Tobias, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, München 2017, DSGVO 20 N 22.

11 Zum Beispiel ist der Anspruch auf Datenportabilität nicht abhängig vom Bestand einer besonderen Vertragsbeziehung (wie z.B. relevant für Art. 400 OR), gilt nicht nur im Kontext der Vertragsbeendigung, wie es z.B. relevant wäre unter Art. 16(4) DCD (DCD für Digital Content Directive oder Richtlinie (EU) 2019/770 vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0770&from=EN#d1e1502-1-1>, und gilt auch ausserhalb einer wettbewerblichen Missbrauchssituation (Swire/Lagos, [Fn. 7], 350).

12 Die Pflicht, interoperable Systeme zu betreiben, besteht gerade nicht, Hennemann Moritz, Datenportabilität, Ping 01.2017, 5 ff., 8. Derjenige, der Daten auf Geheiss der betroffenen Person dieser oder Dritten zur Verfügung stellt, muss nicht dafür sorgen, dass sie beim Empfänger mit vertretbarem Aufwand in ein neues Zielsystem eingespiesen werden können.

13 Zum Beispiel anonymisierte Daten. «Eine Portabilitätsanfrage kann sich ausschließlich auf personenbezogene Daten beziehen», gleichwohl aber auch auf pseudonymisierte Daten (WP242 rev.01, 10).

14 <https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-data-portability_de>.

15 Hervorzuheben ist, dass die unter dem Aspekt «Speicherursache» vorgenommene Kategorisierung auf dem Ansatz der Artikel 29-Arbeitsgruppe beruht. Diese Sicht hat sich weitgehend durchgesetzt, wurde aber richterlich soweit ersichtlich noch nicht bestätigt.

16 Hennemann (Fn. 12), 5 ff. 6 f., sieht den Anwendungsbereich beschränkt auf die Daten, die Art. 13 DSGVO unterstehen, was dem Umfang nach einer Beschränkung auf Kategorie 1 entspricht. Art. 13 DSGVO bezieht sich auf die «Erhebung von personenbezogenen Daten bei der betroffenen Person», im Gegensatz zu Art. 14, dessen Bestimmung das Szenario beschreibt, in dem «die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden». Die Verweisung auf Art. 13 DSGVO kann aber von vornherein nicht so gemeint sein, dass die betroffene Person keinen Anspruch auf Datenportabilität geniessen soll, wo der Verantwortliche – ohne Verschulden oder sonstiges Zutun der betroffenen Person – die Datenerhebungsmethodik (weniger transparent) anderswo als bei der betroffenen Person beschafft. Ein solches Resultat wäre weder gesetzgeberisch naheliegend, noch stünde es mit dem Zweckgedanken (Transparenz) im Einklang. Zudem wäre die Beschränkung des Rechts der betroffenen Person zufällig und abhängig vom Verhalten des Verantwortlichen und würde sogar Anreize schaffen für die betroffene Person, Daten im Zweifel selber an den Verantwortlichen zu übermitteln (anstatt sich dem Risiko auszusetzen, dass der Verantwortliche diese Daten anderswo beschafft). Das kann so nicht gewollt sein.

17 Für eine restriktive Auslegung, die sich daran orientiert, ob die Gefahr eines Lock-in entsteht, tritt demgegenüber Flemming ein, <http://eudatareg.com/datenschutz-im-unternehmen/datenportabilitaet-eine-gefahr-fuer-daten-getriebene-unternehmen>.

18 Die Grenze zwischen Archivgut und anderen Datenhaltungen ist auf Basis der vertraglichen Regelung zu ziehen, die konkret zwischen den Parteien vereinbart ist (Beispiel: Wenn eine Bank einem Bankkunden historische Transaktionen nur für die Dauer von fünf Jahren bereithält, sollte sie dem Bankkunden im Rahmen des Anspruchs auf Datenportabilität alle noch über die Kundenschnittstelle einsehbaren Transaktionen ohne Weiteres herausgeben, mitsamt den noch aktuellen Daueraufträgen etc. Ältere Transaktionen und nicht mehr aktuelle Daueraufträge wären nicht Gegenstand des Anspruchs auf Datenportabilität. Die Herausgabe solcher Einzeltransaktionen richtet sich nach dem anwendbaren Vertragsrecht, weil sonst im Rahmen des Anspruchs auf Datenportabilität Weiterungen geschaffen würden, die keine ausdrückliche Stütze im Gesetzestext haben (weder in der DSGVO noch im EDSG).

19 Es kann aufgrund der massgeblichen Verarbeitungsgründe im Sinne eines Regelungszwecks geschlossen werden, dass das Recht auf Datenportabilität nicht in Datenverarbeitungsrechte des Verantwortlichen eingreifen soll.

20 Herbst (Fn. 10), DSGVO 20 N 12. Wenn ein Datensatz unter mehr als einem Verarbeitungsgrund verarbeitet wird, wird die betroffene Person den Anspruch auf Datenportabilität geltend machen können, auch wenn nur einer der Verarbeitungsgründe sie dazu berechtigen sollte (durch Nennung von zwei Verarbeitungsgrundlagen hat der Verantwortliche zu erkennen gegeben, dass er diesbezüglich auf Mitwirkung der betroffenen Person angewiesen ist, weswegen in einem solchen Fall das Recht auf Datenportabilität zu bejahen ist).

21 Im Einzelnen hierzu: Herbst (Fn. 10), DSGVO 20 N 32 ff.

22 Siehe auch Veil Winfried, in: Gierschmann Sibylle/Schlender Katharina/Stentzel Rainer/Veil Winfried (Hrsg.): Datenschutz-Grundverordnung, Köln 2018, DSGVO 20 N 60.

23 So Hennemann (Fn. 12), 5 ff., 8.

24 Siehe Herbst (Fn. 10), DSGVO 20 N 3.

25 So auch Herbst (Fn. 10), DSGVO 20 N 3, 10.

26 Siehe z.B. Piltz (Fn. 8), DSGVO 20 N 33 f.

27 Herbst (Fn. 10), DSGVO 20 N 11.

28 Dies ergibt sich schon aus dem geltenden Datenschutzrecht, zu weitgehend also Piltz, der von der betroffenen Person verlangt, das Recht auf Datenportabilität nicht ohne diesbezügliche Weisungen auszuüben: Piltz (Fn. 8), DSGVO 20 N 10.

29 Insoweit kein Widerspruch zu Veil (Fn. 22), DSGVO 20 N 60.

30 Dies muss möglich sein und darf nicht als rechtliche Behinderung aufgefasst werden.

31 Hennemann (Fn. 12), 5 ff., 7.

32 Hennemann (Fn. 12), 5 ff., 7.

33 Herbst (Fn. 10), DSGVO 20 N 1.

34 Herbst (Fn. 10), DSGVO 20 N 4.

(Alle URL letztmals besucht: 15.10.2019).

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement **digma** (4 Hefte des laufenden Jahrgangs) à **CHF 178.00**
(Versandkosten: Schweiz inklusive)

Name Vorname

Firma

E-Mail

Strasse/Nr.

PLZ Ort

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8001 Zürich
Telefon +41 44 200 29 29
Telefax +41 44 200 29 28
E-Mail: zeitschriften@schulthess.com
Homepage: www.schulthess.com

Schulthess §