www.jusletter-it.eu

Naomi Toren

Drei wesentliche Veränderungen im Datenschutzrecht der Schweiz

Das Datenschutzrecht in der Schweiz hat sich massgebend durch die Einführung der EU-Datenschutzgrundverordnung («DSGVO») verändert und wird sich durch das Inkrafttreten des revidierten Schweizer Datenschutzgesetzes noch weiter verändern. Die Autorin stellt drei Instrumente vor, welche für das neue Datenschutzverständnis der Schweiz von Bedeutung sein werden: Die Einführung von Privacy by Default, Rechtsregeln zur automatisierten Einzelfallentscheidung und die Datenportabilität. Diese werden mit dem geltenden Recht in der Schweiz und der DSGVO verglichen.

Beitragsart: Datenschutz
Region: Schweiz
Rechtsgebiete: Datenschutz

Zitiervorschlag: Naomi Toren, Drei wesentliche Veränderungen im Datenschutzrecht der Schweiz, in: Jusletter IT 5. Dezember 2019

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1. Einleitung

[1] Durch die Revision des geltenden Datenschutzgesetzes soll die Position jeder Person, die von einer Datenbearbeitung betroffen ist (sog. «betroffene Person»), gestärkt werden – sei dies, indem die Transparenz verbessert (z.B. durch das Auskunftsrecht bei einer automatisierten Einzelfallentscheidung) oder aber indem das informationelle Selbstbestimmungsrecht gestärkt wird (z.B. durch Privacy by Default oder das Datenportabilitätsrecht).[1] Dem Datenbearbeiter (sog. «Verantwortlicher») werden hingegen durch die Revision mehr Pflichten aufgebürdet (z.B. Informationspflichten bei einer automatisierten Einzelfallentscheidung).[2]

2. Privacy by Design und Privacy by Default

2.1. E-DSG, DSG und DSGVO im Vergleich

[2] Da Daten und Informationen sehr beweglich sind, lassen sich Verstösse kaum je wieder rückgängig machen. Ziel ist es somit, Datenschutzverstösse im Vorfeld zu verhindern.[3] Die im E-DSG angelegten Grundsätze «Privacy by Design» und dessen Konkretisierung «Privacy by Default» setzen hier genau an: Privacy by Design, also Datenschutz durch Technikgestaltung, bedeutet, dass bereits während der Entwicklung von Produkten, Diensten oder Anwendungen

1 Husi-Stämpfli Sandra, Die DSG-Revision oder: Ein Beziehungsdrama in drei Akten, in: Jusletter 7. Mai 2018, N 28.

2 Vgl. Bergamelli Manuel, Die Auswirkung der neuen DSGVO auf die Schweiz, in: Jusletter 30. April 2018, N 2 f.

3 Von Lewinski Kai, Die Matrix des Datenschutzes, Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2014, S. 78 ff.

datenschutzrechtliche Massnahmen eingebaut werden sollen.[4] Das geltende Schweizer Datenschutzgesetz kennt diesen Grundsatz von Privacy by Design bereits und sieht technische Massnahmen vor (Art. 7 DSG).[5] Die Statuierung des Grundsatzes Privacy by Default im E-DSG (Art. 6 Abs. 3 E-DSG) stellt hingegen eine Neuerung dar.[6] Unter Privacy by Default versteht man einen Datenschutz durch datenschutzfreundliche Grundeinstellungen. Als Standard muss der Verantwortliche bei mehreren Einstellungsmöglichkeiten die datenschutzfreundlichste Einstellung vorgeben.[7] Die Nutzer sollen keine Änderungen an den Einstellungen vornehmen müssen, um eine möglichst «datensparsame» Verarbeitung zu erreichen. Vielmehr soll umgekehrt jede Abweichung von den datenminimierenden Grundeinstellungen erst durch ein aktives «Eingreifen» der Nutzer möglich werden.[8] Die Regelung soll die Verfügungshoheit der Nutzer über die sie betreffenden Daten sicherstellen und sie vor einer unbewussten Datenerhebung schützen.[9]

[3] Im E-DSG werden die Grundsätze Privacy by Design und Privacy by Default (Art. 6 E-DSG) nun neu von der Datensicherheit (Art. 7 E-DSG) aufgetrennt. Durch diese Auftrennung entstehen neue, allenfalls unbeabsichtigte Schutzlücken, die der Klärung bedürfen. Die Verletzung bzw. Nichtbefolgung von Privacy by Design und Privacy by Default (Art. 6 E-DSG) ist unter keine Sanktionierung gestellt: Das Nichteinhalten des Grundsatzes stellt neuerdings keine Persönlichkeitsverletzung (Art. 26 Abs. 2 Bst. a E-DSG) und auch keine Strafbarkeit (Art. 54 ff. E-DSG) dar. Es wird nicht klar, welchen Mehrwert eine Auftrennung von Art. 7 DSG, der Datensicherheit schafft. Insbesondere widerholen sich die Art. 6 Abs. 1 E-DSG und Art. 7 Abs. 1 E-DSG weitläufig.[10]

[4] Vergleicht man die Regeln zu Privacy by Design und Privacy by Default des E-DSG mit denjenigen der DSGVO erkennt man grundsätzlich eine ähnliche Struktur und einen ähnlichen Inhalt.[11] Zwei Unterschiede werden jedoch deutlich: Art. 25 DSGVO verweist auf eine freiwillige Zertifizierungsmöglichkeit, während der E-DSG dies unterlässt. Dies ist nicht weiter problematisch, da das E-DSG ganz allgemein die Möglichkeit eines Zertifizierungsverfahren vorsieht (Art. 11 DSG, Art. 12 E-DSG). Hinsichtlich der Sanktionen bestehen jedoch grosse Unterschiede zwischen der DSGVO und dem Schweizer Recht: Das geltende DSG sieht noch eine zivilrechtliche Klagemöglichkeit bei einer Verletzung von Privacy by Design vor (Art. 15 DSG), jedoch keine strafrechtlichen Sanktionen. Eine Verletzung der beiden Grundsätze im E-DSG zieht im Unterschied dazu überhaupt keine Rechtsfolgen nach sich. Ganz anders die DSGVO: Hier sind Bussen von bis zu 10 Mio. Euro bzw. 2% des Jahresumsatzes vorgesehen (Art. 83 Abs. 4 Bst. a DSGVO).

---

4 Baumgartner Ulrich, in: Ehmann Eugen/Selmayr Martin (Hrsg.), DS-GVO: Datenschutz-Grundverordnung: Kommentar, 2. Aufl., München 2018, Art. 25, N 11 ff.; Nolte Norbert/Werkmeister Christoph, in: Gola Peter (Hrsg.), Datenschutz-Grundverordnung, VO (EU) 2016/679: Kommentar, 2. Aufl., München 2018, Art. 25, N 2, 15 f.; Härting Niko, Datenschutz-Grundverordnung, Köln 2016, N 110 ff.

5 Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27. November 2017, N 40 ff.

6 Rosenthal (Fn. 5), N 42.

7 PricewaterhouseCoopers AG (PwC), Regulierungsfolgenabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), vom 21.07.16, S. 40, (https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Regulierung/regulierungsfolgenabschaetzung/vertiefte-rfa/datenschutzgesetz–dsg–2016/datenschutzgesetz-2016.html, zuletzt besucht am 31.10.19).

8 Baumgartner (Fn. 4), Art. 25, N 17 ff.; Nolte/Werkmeister (Fn. 4), Art. 25, N 27 ff.; Härting (Fn. 4), N 113 ff; vgl. Rosenthal (Fn. 5), N 43 f.

9 Baumgartner (Fn. 4), Art. 25, N 20; Nolte/Werkmeister (Fn. 4), Art. 25, N 31.

10 Zum Ganzen: Rosenthal (Fn. 5), N 40 ff.

11 So auch Frei Nula, Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, in: Jusletter 17. September 2018, N 38 f.

An dieser Stelle stellt sich die Frage, ob die Europäische Kommission die Sanktionslosigkeit bei einer Verletzung der Grundsätze im Rahmen der Erneuerung des Angemessenheitsbeschlusses für die Schweiz so leicht schlucken wird.

2.2. Kritische Auseinandersetzung

[5] Der Kritik, dass Privacy by Default einen falschen Anreiz setze, indem es Anbieter anrege, ganz auf Wahlmöglichkeiten zu verzichten,[12] ist so nicht zuzustimmen. Datenbearbeitungen müssen ohnehin immer zweckgebunden und datensparsam, also verhältnismässig, ausgestaltet sein (Art. 5 Abs. 2 ff. E-DSG, Art. 5 Abs. 1 Bst. b und c DSGVO). D.h. die erhobenen Daten müssen für den zuvor bekannt gegebenen Zweck geeignet und erforderlich sein. Wenn der betroffenen Person keine zusätzlichen Wahlmöglichkeiten zur Verfügung gestellt werden, kann sie erst gar nicht in datenintensivere Bearbeitungsvorgänge einwilligen. Im Gegenteil, es bestehen also für den Verantwortlichen Anreize, Wahlmöglichkeiten zu schaffen, welche nicht nur die zwingend notwendige Datenpreisgabe vorsieht, damit diese von zusätzlichen Daten profitieren können.

[6] Umgehungspotential besteht allerdings bei der «Zwecksetzung» der betreffenden Datenbearbeitung. Je weiter der bekanntgegebene Zweck ist, desto weitreichender ist die Erforderlichkeit von Datensammeln und -bearbeiten (Art. 5 Abs. 3 E-DSG). Aus Sicht der Verantwortlichen ist es damit vorteilhaft, einen möglichst weiten Bearbeitungszweck für das Datensammeln und -bearbeiten bekanntzugeben. In dieser Hinsicht können in der Tat falsche Anreize entstehen.

[7] Eine denkbare, nachteilige Folge von Privacy by Design und Privacy by Default ist, dass zahlreiche Anbieter, welche ihre Anwendung gegen die Preisgabe persönlicher Daten bis anhin gratis zur Verfügung gestellt haben (z.B. Flughafeninternet), dies allenfalls nicht mehr tun, da es sich für sie nicht mehr rentiert. Es bleibt diesen Anbietern allerdings die Möglichkeit der Einwilligung. Nutzungen sind weiterhin möglich, wenn die Nutzer explizit in die Zurverfügungstellung der Daten einwilligen.[13] Mit dem Instrument der Einwilligung können somit ganz simpel die Grundsätze von Privacy by Default «umgangen» werden. Sobald die betroffene Person vorgängig zu einer datenintensiveren Einstellung einwilligt, ist der Verantwortliche nicht mehr an das Mindestmass des Datensammelns und -bearbeitens gebunden.[14] Bevor man also z.B. die heruntergeladene Jogging-App das erste Mal datensparsam nutzt, willigt man bereits mehrmals ein, die Ortungsdienste usw. zu aktivieren. Somit kommt es de facto nur selten zur datensparsamen Grundeinstellung, da man bereits zu allen datenintensiven Einstellungen eingewilligt hat. Ist Privacy by Default somit nur ein theoretisches Wunschdenken? Wie nützlich es in Realität sein wird, bleibt abzuwarten. Auch falls es faktisch wenige Nutzer geben wird, die nur die Grundeinstellungen eingerichtet haben, verschafft es der betroffenen Person mehr Übersicht und Kontrolle über ihre Einstellungen und weniger unwissentliche Datenpreisgabe.

12 Vgl. RFA (Fn. 7), S. 41.

13 Zum Ganzen: RFA (Fn. 7), S. 41.

14 Rosenthal (Fn. 5), N 44.

2.3. Zwischenfazit

[8] Privacy by Default stellt im Vergleich zum geltenden DSG eine Neuerung dar. Struktur und Inhalt beider Privacy-Grundsätze gleichen derjenigen der DSGVO.

[9] Unbenommen ist, dass durch die Einführung von Privacy by Default das Datensammeln verringert und dass der betroffenen Person mehr Kontrollmöglichkeiten eingeräumt wird. Auch wenn die betroffene Person später in datenintensivere Einstellungen einwilligen sollte, wird die unwissentliche Datenpreisgabe dadurch verringert. Der Vorteil an einer Regelung, die bei der Technik ansetzt, ist, dass diese einen Vorfeldschutz bietet: Es soll erst gar nicht zu Datenmissbrauch kommen.

3. Automatisierte Einzelfallentscheide (AEFE) und Profiling

[10] Unternehmen fällen heutzutage etliche automatisierte Entscheide ohne Mitwirkung eines Menschen mittels automatisierter Datenbearbeitung. Im E-DSG werden bei einer automatisierten Einzelfallentscheidung (AEFE) Informationspflichten für die betroffenen Personen eingeführt. Die betroffene Person erhält ausserdem ein Anhörungsrecht, um ihren Standpunkt bei einer natürlichen Person geltend zu machen. Zusätzlich müssen Verantwortliche auf Aufforderung der betroffenen Person dafür sorgen, dass ein Mensch die Entscheidung überprüft (sog. Eskalationsrecht). Diese Rechte sollen dem Problem Rechnung tragen, dass die automatisierte Auswertung von Daten nach gewissen Mustern die Spezialitäten der betroffenen Person möglicherweise nicht erkennt.[15]

[11] Sowohl im E-DSG als auch in der DSGVO wird das Profiling mit der AEFE zusammen geregelt, da diese miteinander zusammenhängen. Sie sind aber voneinander abzugrenzen. Beim Profiling geht es um einen automatisierten Bearbeitungsvorgang einer Bewertung, Analyse und Prognose von Personendaten, etwa zu deren Arbeitsleistung, Wirtschaftlichkeit, Gesundheit, Vorlieben, Interessen, Zuverlässigkeit, Verhalten oder Aufenthaltsort. Dieser automatisierte *Bearbeitungsvorgang* (Profiling) ist insofern einer automatisierten *Entscheidung* vorgelagert. Wenn ein Profiling zu einer Entscheidung, also einer AEFE führt, ist Art. 19 E-DSG bzw. Art. 22 DSGVO anwendbar.[16]

3.1. Profiling

[12] Gerade das Profiling war zuletzt in der Nationalratsdebatte wegen des Einwilligungserfordernisses sehr umstritten (Art. 5 Abs. 6 E-DSG). Es geht um die Frage, ob die ausdrückliche Einwilligung bei einem Profiling im Gesetz verankert werden soll oder nicht. Der Ständerat wird hier

15 Zum Ganzen: RFA (Fn. 7), S. 30 f.

16 Vgl. Schulz Sebastian, in: Gola Peter (Hrsg.), Datenschutz-Grundverordnung, VO (EU) 2016/679: Kommentar, 2. Aufl., München 2018, Art. 22, N 20; vgl. Buchner Benedikt, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG Kommentar, 2. Aufl., München 2018, Art. 22, N 4, 20; vgl. 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 ff., S. 7056 f.

für Klärung sorgen müssen.[17] Diese Frage wird im Rahmen dieses Beitrags nicht weiterverfolgt. Augenmerk soll auf die Einführung von Informationspflichten gelegt werden.

[13] Im geltenden DSG kennen wir bislang keine besonderen Informationspflichten für den Bearbeitungsvorgang Profiling. Eine aktive Informationspflicht besteht gemäss dem DSG aber bei besonders schützenswerten Daten, insbesondere dem Persönlichkeitsprofil (Art. 14 DSG). Als besonders schützenswerte Personendaten gelten Daten über «die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrativen oder strafrechtlichen Verfolgungen und Sanktionen» (Art. 3 Bst. c DSG). Die Verletzung dieser Informationspflicht wird mit Busse sanktioniert (Art. 34 Abs. 1 DSG).[18]

[14] Das im DSG geregelte Persönlichkeitsprofil (Art. 14 DSG) wird nun im E-DSG vom Profiling abgelöst (Art. 19 E-DSG). Das Persönlichkeitsprofil (Ergebnis einer Datenbearbeitung) ist vom Profiling zu unterscheiden. Profiling ist der Vorgang des automatisierten Verarbeitens von Personendaten, um Rückschlüsse z.B. auf das Sortiment zu ziehen. Das Persönlichkeitsprofil stellt hingegen die Sammlung sämtlicher Informationen eines Kunden dar, um damit Rückschlüsse auf das Sortiment zu ziehen.[19] Der E-DSG lehnt sich mit dem neuen Begriff des Profilings an die DSGVO-Sprache an (vgl. Art. 4 Nr. 4 DSGVO, Art. 22 DSGVO.

3.2. AEFE

[15] Nach dem geltenden DSG bestehen keine besonderen Rechte für die betroffene Person bei einer AEFE. Namentlich gibt es kein Recht, den eigenen Standpunkt darzulegen (Anhörungsrecht), geschweige denn ein Recht, dass die betreffende Entscheidung vom Menschen angeschaut wird (Eskalationsrecht).[20] Das DSG sieht auch keine besonderen Informationspflichten bei einer AEFE vor. Zu beachten sind aber die Art. 9 ff. VDSG, welche besondere Massnahmen und gegebenenfalls eine Protokollierungspflicht bei automatisierten Bearbeitungen vorsehen. Beispielsweise wird als eine besondere Massnahme die nachträgliche Überprüfung der eingegebenen Personendaten vorgeschrieben. Die Einführung von Rechten und Pflichten bei einer AEFE auf Gesetzesstufe (Art. 19 E-DSG) stellt also eine Neuerung dar.

3.2.1. Begriff

[16] Betrachtet man den Begriff der AEFE im E-DSG, stellt man fest, dass dieser demjenigen der DSGVO folgt.[21] Erforderlich ist ein Entscheid über eine einzelne betroffene Person. Der Einzelentscheid muss vollständig von einer Maschine getroffen werden. Es liegt keine AEFE bei Computerentscheiden vor, die von einem Menschen am Schluss abgesegnet werden. Umgekehrt führen Stichproben durch den Menschen noch nicht zum Nichtvorliegen einer AEFE. Die automatisierte

17 Mäder Lukas, Nationalrat nähert sich beim Datenschutz der EU an – Frage des Profilings noch ungelöst, in: NZZ vom 24.09.19.

18 Wermelinger Amédéo, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG): Bundesgesetz über den Datenschutz vom 19.06.92, Stämpflis Handkommentar, Bern 2015, Art. 14, N 1.

19 Wermelinger (Fn. 18), Art. 14, N 3; Botschaft E-DSG (Fn. 16), S. 7021 f.

20 Vgl. RFA (Fn. 7), S. 31 f.

21 Vgl. Buchner (Fn. 16), Art. 22, N 6.

Entscheidung muss gemäss Bundesrat ferner eine gewisse Komplexität aufweisen, d.h. es muss sich um eine inhaltliche Beurteilung mit einem Spielraum und nicht eine reine «wenn-dann-Entscheidung» wie bei einem Bancomat handeln.[22] Ansonsten liegt nämlich keine Entscheidung vor.[23]

3.2.2. Kein Ausschluss bei besonders schützenswerten Daten

[17] Die DSGVO sieht grundsätzlich einen Ausschluss einer AEFE bei «sensitiven Daten» vor, also Daten zur rassischen und ethnische Herkunft, zu politischen Meinungen, zu religiösen Überzeugungen, zur Gewerkschaftszugehörigkeit, zur Genetik und Biometrik oder zur sexuellen Orientierung (Art. 22 Abs. 4 DSGVO i.V.m. Art. 9 DSGVO).[24] Ein solcher Ausschluss von «besonders schützenswerten Daten» (i.S.v. Art. 3 Bst. c DSG bzw. Art. 4 Bst. c E-DSG) bei einer AEFE ist weder in Art. 19 E-DSG noch in dessen Botschaft zu finden.[25] Jedoch setzt Art. 5 Abs. 6 E-DSG ganz generell bei jeder Bearbeitung von besonders schützenswerten Daten eine Einwilligung voraus. Diese Lösung ist im Vergleich zu einem grundsätzlichen Verbot deutlich liberaler und daher grundsätzlich vorzuziehen.

3.2.3. Keine besondere Regelung für Kinder

[18] Nach der DSGVO darf eine AEFE keine Kinder betreffen (Erwägungsgrund 71). Dies ist ein relatives Verbot. Ausnahmsweise sind AEFE bei Kindern nur dann zulässig, wenn der Verantwortliche geeignete Sicherungsmassnahmen zum Persönlichkeitsschutz der Kinder getroffen hat. Darunter zu verstehen sind beispielsweise eine kindergerechte Aufklärung oder das Einwilligungserfordernis der Eltern.[26] Eine solche Schutzvorkehrung für Kinder bei einer AEFE ist nach Schweizer Recht nicht vorgesehen.[27] Man könnte sich so etwas aber durchaus auch in der Schweiz überlegen.

3.2.4. Rechtsfolgen

[19] Art. 19 E-DSG ist hinsichtlich der Rechtsfolgen wesentlich liberaler als die DSGVO. Der grosse Unterschied zwischen Art. 22 DSGVO und Art. 19 E-DSG ist derjenige, dass im EU-Recht die AEFE mit einer gewissen Wirkung grundsätzlich verboten sind und nur mit einem Rechtfertigungsgrund vorgenommen werden können. Falls ein Rechtfertigungsgrund vorliegt, müssen Massnahmen wie das Anhörungsrecht gewahrt werden.[28] Im E-DSG sind AEFE bei einer rechtlichen Wirkung oder erheblichen Beeinträchtigung grundsätzlich erlaubt, lösen aber in diesem Fall

22 Vgl. Botschaft E-DSG (Fn. 16), S. 7056 ff.

23 Zum Ganzen: Rosenthal (Fn. 5), N 102 ff.

24 Martini Mario, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018, Art. 22, N 40 f.

25 Vgl. Botschaft E-DSG (Fn. 16), S. 7056 ff.

26 Martini (Fn. 24), Art. 22, N 30.

27 Vgl. Botschaft E-DSG (Fn. 16), S. 7056 ff.

28 Vgl. Hladjk Jörg, in: Ehmann Eugen/Selmayr Martin (Hrsg.), DS-GVO: Datenschutz-Grundverordnung: Kommentar, 2. Aufl., München 2018, Art. 22, N 9, 11 ff.

eine Informationspflicht aus.[29] Bei einem Rechtfertigungsgrund – beispielsweise einer Einwilligung – wird auch diese nicht nötig (Art. 19 Abs. 3 E-DSG). Dieser Unterschied in den Rechtsfolgen ist insbesondere für Schweizer Unternehmen relevant, die unter den Anwendungsbereich der DSGVO fallen und bei Abnehmern aus dem EU-Raum andere Vorkehrungen treffen müssen als für Abnehmer aus der Schweiz. Diese unterschiedlichen Regelungen können bei Unternehmen für Verwirrung sorgen. Andererseits kann sich dieser Unterschied auch als Wettbewerbsvorteil für die Schweiz erweisen, da die E-DSG-Regelung liberaler als diejenige der DSGVO ist.

[20] Der E-DSG weicht in einem weiteren Punkt von der DSGVO ab: Die Informationspflicht entsteht gemäss Art. 19 Abs. 1 und 2 E-DSG wie erwähnt erst, wenn für die betroffene Person (a.) eine Rechtsfolge verbunden oder sie (b.) erheblich beeinträchtigt ist. Aus Sicht der DSGVO muss die Rechtsfolge eine gewisse Intensität aufweisen (Art. 22 Abs. 1 DSGVO).[30] Nicht gemäss E-DSG; hier genügt jede Rechtsfolge, z.B. eine Ausübung eines vertraglichen Rechts.[31] Insofern ist der Anwendungsbereich im E-DSG weiter. Dies erscheint gerechtfertigt, da die Konsequenz kein Verbot, sondern lediglich eine Informationspflicht ist.

[21] Bei der alternativen Voraussetzung der erheblichen Beeinträchtigung nach Art. 19 Abs. 1 E-DSG ist wie der Begriff bereits vermuten lässt – entsprechend der DSGVO – wiederum eine gewisse Intensität verlangt. Dies ist z.B. bei einer Nichtzuteilung einer medizinischen Leistung gegeben.[32] Eine richtige Definition einer erheblichen Beeinträchtigung wird die Praxis herausbilden müssen. Möglicherweise kann die Schweiz hier auch von der Rechtsfortbildung der EU profitieren. Von einer erheblichen Beeinträchtigung nach dem DSGVO-Verständnis werden Beeinträchtigungen der wirtschaftlichen oder persönlichen Situation (z.B. Einstellung als Arbeitnehmer oder ehrverletzende Darstellungen) erfasst.[33]

3.2.5. Verstösse

[22] Bei einem Verstoss gegen Art. 19 E-DSG kann die betroffene Person Anzeige beim EDÖB erstatten, der sie über die weiteren Schritte unterrichtet und daraufhin ggf. eine Untersuchung einleitet (Art. 43 Abs. 4 E-DSG). Der EDÖB kann anordnen, dass der Verantwortliche die betroffene Person gehörig nach Art. 19 E-DSG zu informieren hat (Art. 45 Abs. 3 Bst. c E-DSG). Dies kann eine Gebühr verursachen (Art. 53 Abs. 1 Bst. d E-DSG). Wurden die Pflichten von Art. 19 E-DSG verletzt, zieht dies eine Busse von bis zu CHF 250'000 nach sich (Art. 54 Abs. 1 Bst. a E-DSG). Die DSGVO fährt schwerere Geschütze auf: Die Bussen können bis zu 20 Mio. Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen (Art. 83 Abs. 5 Bst. b DSGVO). Führt eine nach der DSGVO nicht rechtskonform herbeigeführte AEFE zu einem Schaden, ist dieser der betroffenen Person zu ersetzen (Art. 82 DSGVO).[34]

---

29 Rosenthal (Fn. 5), N 100; vgl. Botschaft E-DSG (Fn. 16), S. 7056 ff.; Frei (Fn. 11), N 31.

30 Rosenthal (Fn. 5), N 100 ff; Schulz (Fn. 16), Art. 22, N 22.

31 Rosenthal (Fn. 5), N 102.

32 Rosenthal (Fn. 5), N 100 ff.; vgl. Schulz (Fn. 16), Art. 22, N 22; vgl. Botschaft E-DSG (Fn. 16), S. 7057.

33 Schulz (Fn. 16), Art. 22, N 5, 22 ff.

34 Schulz (Fn. 16), Art. 22, N 46.

3.3. Zwischenfazit

[23] Eine Regelung über AEFE, wie es der E-DSG vorsieht, gibt es so noch nicht im geltenden Schweizer Datenschutzrecht. Sie stellt insofern eine Neuerung dar. Der E-DSG lehnt sich dabei an Art. 22 DSGVO an, welcher allerdings deutlich strenger ausgestaltet ist und einen deutlich höheren Strafrahmen vorsieht. Sobald eine AEFE – welche insbesondere auf einem Profiling beruhen kann – eine rechtliche oder sonstige erhebliche Wirkung hervorruft, ist sie aus Sicht der DSGVO grundsätzlich verboten; in der Schweiz löst sie eine Informationspflicht aus.

4. Datenportabilität

[24] Der Bundesrat hat sich 2017 beim E-DSG dazu entschlossen, in der Schweiz kein Datenportabilitätsrecht einzuführen.[35] In der Zwischenzeit wurde der Versuch angestrengt, ein solches Recht über die Volksinitiative zu implementieren.[36] Nun hat sich im September 2019 der Nationalrat dazu entschieden, ein solches Recht doch ins Gesetz mitaufzunehmen.[37] Wie der Ständerat zur Einführung eines solchen Rechts steht, wird sich nun zeigen. Es ist anzunehmen, dass sich unter anderem die Einführung eines solchen Portabilitätsrechts günstig auf die bevorstehende Angemessenheitsprüfung der EU für die Schweiz auswirken kann (vgl. Art. 45 DSGVO).[38] Im Übrigen müssen Unternehmen, welche unter den weiten Anwendungsbereich der DSGVO fallen, sowieso bereits heute den betroffenen Personen aus dem EU-Raum ein solches Recht gewähren (vgl. Art. 3 DSGVO).[39] Es erscheint fair, dass sie dieses Recht auch für betroffene Personen aus der Schweiz gewähren müssten.

[25] Grundgedanke des Rechts auf Datenportabilität (oder auch Datenübertragbarkeit) ist, dass die betroffene Person alle sie betreffenden Daten vom Verantwortlichen verlangen kann. Damit soll sie diese Daten in das Verarbeitungssystem eines anderen Verantwortlichen, beispielsweise einem konkurrierenden Social-Media-Dienst, übertragen können.[40] Die Ausübung dieses Rechts darf nicht mit rechtlichen Nachteilen verbunden werden und soll grundsätzlich unentgeltlich sein.[41] Einerseits soll dieses Recht der Kontrolle der betroffenen Personen über die sie betreffenden personenbezogenen Daten, andererseits dem Wettbewerb zwischen den Verantwortlichen

---

35 Botschaft E-DSG (Fn. 16), S. 6984 ff.; Vgl. Votum Keller-Sutter Karin, AB 2019 N 1816.

36 Mäder Lukas, Volksinitiative soll den Nutzern mehr Kontrolle über ihre eigenen Daten bringen, in: NZZ vom 24.03.18.

37 SDA Meldung, Nationalrat sagt teilweise zähneknirschend Ja zu Datenschutzgesetz vom 25.09.19.

38 Vgl. Botschaft E-DSG (Fn. 16), S. 6964 f.

39 Bergamelli (Fn. 2), N 14 ff.; Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, von Juli 2018, S. 3 ff., 6 ff. (https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/Die_EU_DSGVO_und_ihre_Auswirkungen_auf_die_Schweiz.pdf.download.pdf/Die_EU_DSGVO_und_ihre_Auswirkungen_auf_die_Schweiz.pdf, zuletzt besucht am 31.10.19).

40 Thouvenin Florent, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, in: SJZ 113/2017, S. 27.

41 Kamann Hans-Georg/Braun Martin, in: Ehmann Eugen/Selmayr Martin (Hrsg.), DS-GVO: Datenschutz-Grundverordnung: Kommentar, 2. Aufl., München 2018, Art. 20, N 44; Paal Boris P., in: Paal Boris P./Pauly Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018, Art. 20, N 7; vgl. Weber Rolf/Thouvenin Florent, Gutachten zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS), vom 22.12.17, S. 50 ff. (https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/datenpolitik/180321%20BJ-Gutachten_final.pdf.download.pdf/180321%20BJ-Gutachten_final.pdf, zuletzt besucht am 31.10.19).

dienen.[42] Es fördert zudem die Wiederverwendung der Daten und die Entwicklung neuer Dienstleistungen.[43]

[26] Oft wird vertreten, dass ein solches Recht systemfremd sei und zum Konsumentenschutz- oder eher Wettbewerbsrecht gehöre. Verfechter des Datenportabilitätsrechts halten entgegen, dass es sich hierbei um ein innovatives Recht auf Privatleben und Datenschutz im digitalen Zeitalter handelt: Das Datenschutzrecht sei durch die Digitalisierung verzahnt und nicht zu trennen von Nachbardisziplinen wie dem Wettbewerbsrecht.[44] Neben dem Schutz von Lock-in-Effekten und der Öffnung der Datenmärkte stärkt diese Anordnung auch die Datenautonomie der betroffenen Personen.[45]

4.1. Geltendes Recht in der Schweiz

[27] Das DSG kennt kein Portabilitätsrecht. Jedoch steht der betroffenen Person bereits heute ein Recht auf kostenlose Auskunft der über sie vorhandenen Daten zu (Art. 8 DSG, Art. 1 f. VDSG).[46] Der Auskunftserteilende hat die Pflicht, die verschlüsselten Daten zu entschlüsseln und die Daten schriftlich und lesbar aufzubereiten. Zudem besteht ein Anspruch auf Herausgabe der betreffenden Daten mittels eines Ausdrucks oder einer Kopie dieser Daten (Art. 8 Abs. 5 DSG). Da das Auskunftsrecht nicht vertretungsfeindlich ist, kann auch Dritten mittels Vollmacht die Auskunft erteilt werden.[47] Der wesentliche Unterschied zwischen dem Portabilitätsrecht und dem Auskunftsrecht besteht letztlich darin, dass das Auskunftsrecht nur einen Anspruch auf eine Auskunft in Schriftform gewährt, aber keine elektronischen Daten erhält. Die Auskunft zielt auf die Kontrolle und nicht auf die Nutzung der Daten ab.[48]

[28] Das Auskunftsrecht kann abschliessend durch Art. 9 f. DSG, insbesondere durch eine gesetzliche Grundlage, überwiegende Interessen Dritter oder überwiegender Eigeninteressen, eingeschränkt werden. Zu den Eigeninteressen gehören gemäss BGer auch finanzielle Interessen, etwa ein hoher finanzieller Aufwand, wenn auch Auskunft über den Inhalt archivierter Datenbestände oder über Backups erteilt werden soll.[49]

[29] Die betroffene Person hat keine zeitliche Frist für die Geltendmachung des Auskunftsrechts. Ihr ist grundsätzlich 30 Tage nach Auskunftsrechtsbegehren Auskunft zu erteilen (Art. 1 Abs. 4

---

42 Piltz Carlo, in: Gola Peter (Hrsg.), Datenschutz-Grundverordnung, VO (EU) 2016/679: Kommentar, 2. Aufl., München 2018, Art. 20, N 1 ff.; vgl. Artikel-29-Datenschutzgruppe, Artikel-29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP242rev.01, vom 05.04.17, S. 4 (https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48142, zuletzt besucht am 31.10.19).

43 Vgl. Botschaft E-DSG (Fn. 16), S. 6982.

44 Kamann/Braun (Fn. 41), Art. 20, N 3; Piltz (Fn. 42), Art. 20, N 1; Herbst Tobias, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG Kommentar, 2. Aufl., München 2018, Art. 20, N 4.

45 Weber/Thouvenin (Fn. 41), S. 69; Kamann/Braun (Fn. 41), Art. 20, N 3.

46 RFA (Fn. 7), S. 36.

47 BGE 125 III 321.

48 Vgl. Rudin Beat, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG): Bundesgesetz über den Datenschutz vom 19. Juni 1992, Stämpflis Handkommentar, Bern 2015, Art. 8, N 19 f., 38.

49 Zum Ganzen: BGE 135 III 425 E 6.1; Husi-Stämpfli Sandra, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG): Bundesgesetz über den Datenschutz vom 19. Juni 1992, Stämpflis Handkommentar, Bern 2015, Art. 9, N 33.

VDSG). Die Auskunft kann klageweise durchgesetzt werden (Art. 15 Abs. 4 DSG). Eine Verletzung der Auskunftspflicht wird auch von Strafbestimmungen erfasst (Art. 34 DSG).[50]

4.2. E-DSG

[30] Wie erwähnt hat sich die Schweiz erst seit Kurzem für ein Datenportabilitätsrecht entschieden.[51] Der Bundesrat verzichtete auf dessen Einführung im E-DSG, weil «[...] dieses Recht mehr darauf ausgerichtet [sei], den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen, als ihre Persönlichkeit zu schützen. Ausserdem könnte die Umsetzung dieses Rechts schwierig sein, da es die gegenseitige Abstimmung unter den Verantwortlichen und zweifellos eine – zumindest implizite – Einigung über die verwendeten Datenträger und Informatikstandards voraussetzt.»[52] Eine Einführung eines Rechts auf Datenportabilität könnte sich gemäss Bundesrat zudem als sehr kostenintensiv erweisen.[53]

[31] Im Rahmen der Strategie «Digitale Schweiz» ist bereits ein Gutachten ergangen, welches zum Schluss gelangt, dass ein Recht auf Datenportabilität mit nur wenigen Anpassungen des geltenden Auskunftsrechts ausgestaltet werden könnte:[54]

- Der Anspruch der betroffenen Person auf Herausgabe der eigenen Daten könnte ergänzend zum heutigen Recht 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.[55]
- Für die Frist zur Datenportierung erscheint ein Monat wie beim Auskunftsrecht als passend.[56] Eine Frist von einem Monat sieht im Übrigen auch die DSGVO vor (vgl. Art. 12 Abs. 3 DSGVO).[57]
- Auch bei der Tragung der Kosten drängt sich eine Anlehnung an das Schweizer Auskunftsrecht auf: Die Daten sind damit grundsätzlich unentgeltlich, an betroffene Personen und Dritte herauszugeben.[58] Dieser Aspekt gleicht im Übrigen ebenfalls der DSGVO.[59]
- Wie das Auskunftsrecht müsste auch das Portabilitätsrecht gewissen Grenzen unterliegen, die es erlauben, den Interessen von Verantwortlichen und Dritten angemessen Rechnung zu tragen (vgl. Art. 24 E-DSG). Als berechtigte Interessen können dabei auch finanzielle Interessen und Geheimhaltungsinteressen gelten.[60]

---

50 Zum Ganzen: Gramigna Ralph/Mauerer-Lambrou Urs, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Datenschutzgesetz Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014, Art. 8, N 35 f., 64; Rudin (Fn. 48), Art. 8, N 30.

51 SDA Meldung, Nationalrat sagt teilweise zähneknirschend Ja zu Datenschutzgesetz vom 25.09.19.

52 Botschaft E-DSG (Fn. 16), S. 6984; vgl. RFA (Fn. 7), S. 37.

53 Botschaft E-DSG (Fn. 16), S. 6984 f.

54 Weber/Thouvenin (Fn. 41), S. 70, 78 f., 86 f.

55 Zum Ganzen: Weber/Thouvenin (Fn. 41), S. 70, 86 f.

56 Weber/Thouvenin (Fn. 41), S. 81, 86 f.

57 Artikel-29-Datenschutzgruppe (Fn. 42), S. 17.

58 Weber/Thouvenin (Fn. 41), S. 86.

59 Paal (Fn. 41), Art. 20, N 7.

60 BGE 138 III 425, E. 6.1; Weber/Thouvenin (Fn. 41), S. 77, 86 f.

- Bei Verstössen gegen das Portabilitätsrecht könnten ebenfalls die bestehenden auskunftsrechtlichen Bestimmungen massgebend sein, nach welcher ein Klagerecht und gegebenenfalls strafrechtliche Sanktionen bestehen würden (vgl. Art. 15 Abs. 4, 34 DSG).

[32] In der EU gilt das Portabilitätsrecht seit Inkrafttreten der DSGVO im Mai 2018. So können wir in der Schweiz von Diskussionen profitieren, die in der EU bereits geführt wurden. Es fragt sich nämlich, ob die direkte Übermittlung wie in der DSGVO von der technischen Machbarkeit der Übertragung abhängig gemacht werden soll (vgl. Art. 20 Abs. 2 DSGVO, Erwägungsgrund 68 der DSGVO).[61] Weiterhin stellt sich auch in der Schweiz die Frage welche Daten Gegenstand vom Portabilitätsrecht sein sollen.[62] Sollen nur die aktiv und wissentlich bereitgestellten Daten oder auch Daten, die aus Beobachtung der Tätigkeiten eines Nutzers resultieren (z.B. Web-Suchverlauf, Verkehrs- und Standortdaten, von einem Trackinggerät aufgezeichnete Herzfrequenz) von der Portabilität erfasst werden? Gemäss der Artikel-29-Datenschutzgruppe, einem unabhängigem europäischem Gremium mit beratender Funktion, werden nur diejenigen Daten vom Portabilitätsrecht ausgeschlossen, die aus Rückschlüssen erzeugte und abgeleitete, personenbezogene Daten beinhalten, welche von dem Diensteanbieter selbst erzeugt werden (z.B. algorithmische Ergebnisse, Analyse des beobachteten Verhaltens).[63] Wie das in der Schweiz aussehen wird, zeigt die Zukunft.

4.3. Kritische Auseinandersetzung

[33] Inwieweit die angeprangerten Lock-in-Effekte bei Social-Media-Plattformen durch das Portabilitätsrecht überwunden werden können, ist nach wie vor fragwürdig. So lässt man bei einer Datenübertragung doch einen ganz wesentlichen Teil seines Accounts bei Social-Media-Plattformen «liegen», nämlich seine «Follower» bzw. seine Freunde und Anhänger. Ob die betroffenen Personen die Daten tatsächlich an eine neue Plattform ohne die Übernahme ihrer «Follower» übertragen lassen werden, wird sich zeigen.

[34] Der Bundesrat hat 2017 in der Botschaft zum E-DSG die Nichteinführung des Portabilitätsrechts unter anderem wegen der anfallenden Kosten begründet.[64] Die Regulierungsfolgeabschätzung zur Revision des Schweizer Datenschutzgesetzes rechnet nämlich mit einer hohen Kostenflut für Unternehmen.[65] Anderer Ansicht ist das Gutachten zur Datenportabilität, welches keine Vermehrung der Kosten prognostiziert, da Unternehmen wegen des bereits geltenden Auskunftsrechts die Informationen ohnehin schon aufbereiten können müssen: Ob die Daten nun der betroffenen Person selbst oder einem Dritten zur Verfügung gestellt werden, dürfte sich bei den Kosten kaum auswirken, erklärt das Gutachten.[66] Dem ist zumindest nicht vollständig zuzustimmen, da ein wesentlicher Unterschied – wie gesehen – auch darin besteht, dass beim Auskunftsrecht ein Ausdruck der Daten genügt, hingegen das Portabilitätsrecht ein standardisiertes,

61 Weber/Thouvenin (Fn. 41), S. 50; Artikel-29-Datenschutzgruppe (Fn. 43), S. 6, 18.

62 Vgl. Votum Keller-Sutter Karin, AB 2019 N 1816.

63 Artikel-29-Datenschutzgruppe (Fn. 42), S. 9 ff., 18; vgl. Kamann/Braun (Fn. 41), Art. 20, N 13; vgl. Piltz (Fn. 42), Art. 20, N 14 ff.

64 Botschaft E-DSG (Fn. 16), S. 6984 f.

65 Vgl. Weber/Thouvenin (Fn. 41), S. 37, 81.

66 Vgl. Weber/Thouvenin (Fn. 41), S. 70.

gängiges Format vorschreibt. Die Kostenfrage scheint also – wie so häufig – nicht geklärt und kaum abschätzbar zu sein.

[35] Neben der Kostenfrage besteht für den Bundesrat auch noch Ungewissheit in puncto Einigung auf ein standardisiertes Format zur Übertragung der Daten.[67] Gemäss dem Gutachten zur Datenportabilität erscheint diese Befürchtung nicht von Nöten. Eine Einigung wird es ohnehin nie geben. Klare Vorgaben der Datenstruktur sind kontraproduktiv und können höchstens für spezifische Anwendungen gemacht werden. Dem ist zuzustimmen wohlwissend, dass private Anwendungen wie BitsaboutMe[68] bereits heutzutage Tools anbieten, Daten von verschiedenen Plattformen auszutauschen.[69] Fraglich bleibt ferner der Sicherheitsaspekt bei der Übertragung: Es besteht die Gefahr, dass die Downloads von betroffenen Personen nicht genügend geschützt werden und daher Opfer von Datenangriffen sein werden.[70] Betroffene Personen müssten dazu aufgefordert werden, ebenfalls geeignete Schutzmassnahmen zu treffen.

[36] In diesem Zusammenhang stellt sich die oft gestellte Frage, warum das Portabilitätsrecht nicht nur für bestimmte Unternehmen, insbesondere die Online-Plattformen, gelten soll, da es schliesslich für Online-Plattformen konzipiert wurde.[71] Stattdessen gilt es für alle noch so unterschiedlichen Unternehmen ganz nach dem Motto «One-size-fits-all». Aus Sicht der Artikel-29-Datenschutzgruppe sind allerdings auch ausserhalb des Social Media Bereichs Konstellationen denkbar. So können z.B. Banken Kundendaten nutzen, die ursprünglich im Rahmen eines Energieversorgervertrags erhoben worden sind.[72] Sollte dennoch eine Differenzierung der Anwendung des Portabilitätsrechts angestrebt werden – beispielsweise nach wirtschaftlicher Grösse, Anzahl der Nutzerzahlen oder gewissen Branchen oder Datentypen – hätte dies zumindest einen erheblichen Begründungsaufwand zur Folge.[73] Welche Differenzierung wäre zu wählen? Solche Vorgaben hätten wiederum ein grosses Umgehungspotential.

4.4. Zwischenfazit

[37] Das geltende Auskunftsrecht in der Schweiz verfügt bereits heute über Teile der Ansprüche des Portabilitätsrechts mit einem grossen Unterschied: Es besteht kein Anspruch auf Erhalt der Daten in einem weiter verwendbaren Format. Dieses wurde mit der DSGVO zum ersten Mal auf europäischer Ebene eingeführt und stellt somit eine wesentliche Neuerung im Datenschutzrecht dar. Das revidierte DSG soll sich gemäss Nationalrat dieser Entwicklung anschliessen.[74] Das Portabilitätsrecht erscheint vielversprechend: Es wäre ein zentrales Element für die Stärkung der Rechtspositionen der betroffenen Person und leistet einen wettbewerbsrechtlichen Beitrag. Aller-

67 Botschaft E-DSG (Fn. 16), S. 6984.

68 Vgl. https://bitsabout.me (zuletzt besucht am 30.10.19).

69 Weber/Thouvenin (Fn. 41), S. 74 ff.; vgl. RFA (Fn. 7), S. 37.

70 RFA (Fn. 7), S. 37.

71 Paal (Fn. 41), Art. 20, N 6; Kamann/Braun (Fn. 41), Art. 20, N 5; vgl. Weber Rolf H./Chrobak Lennart, Rechtsinterdisziplinarität in der digitalen Datenwelt, in: Jusletter 4. April 2016, N 38; vgl. Weber/Thouvenin (Fn. 41), S. 74.

72 Herbst (Fn. 44), Art. 20, N 1; Artikel-29-Datenschutzgruppe (Fn. 42), S. 4; vgl. RFA (Fn. 7), S. 37.

73 Vgl. Weber/Thouvenin (Fn. 41), S. 74.

74 SDA Meldung, Nationalrat sagt teilweise zähneknirschend Ja zu Datenschutzgesetz vom 25.09.19.

dings muss das Portabilitätsrecht mit den zu erwartenden Risiken, den Kosten und dem Sicherheitsaspekt abgewogen werden.

5. Schlussfolgerungen

[38] Die Schweiz befindet sich zurzeit in einer Phase einer erheblichen Weiterentwicklung des Datenschutzrechts. Insbesondere die drei aufgeführten Instrumente (Privacy by Default, Regeln zur AEFE und das Datenportabilitätsrecht) zeigen diese Veränderungen auf.

[39] Gerade Privacy by Default sorgt dafür, dass bereits das Datensammeln systemtechnisch reduziert wird, damit es erst gar nicht zu einem Datenbearbeiten von nicht zwingend notwendigen Daten kommt. Durch das Portabilitätsrecht soll die betroffene Person autonomer mit den sie betreffenden Daten umgehen können. Zudem schafft das Portabilitätsrecht einen Beitrag gegen die Abhängigkeitsverhältnisse zu (monopolen) Anbietern. Mit der Informationspflicht bei der AEFE im Falle einer rechtlichen oder sonstigen Beeinträchtigung wird mehr Transparenz geschaffen und durch das Anhörungs- und Eskalationsrecht die Position einer betroffenen Person gestärkt.

[40] Einige Elemente des E-DSG gleichen denjenigen der DSGVO (z.B. Privacy by Design und Default). Analog zur DSGVO soll nun neu auch das Recht auf Datenportabilität in der Schweiz eingeführt werden. Gleichwohl unterscheidet sich der E-DSG in manchen Aspekten zur DSGVO. Beispielsweise stellt die AEFE bei einer rechtlichen oder sonstigen Beeinträchtigung kein Verbot dar, sondern löst lediglich Informationspflichten aus (vgl. Art. 19 Abs. 1 E-DSG).

Naomi Toren hat im Frühlingsemester den Master of Law an der Universität Zürich abgeschlossen. Dieser Beitrag stammt aus einem neu aufbereiteten Teil der Masterarbeit der Autorin zum Thema «DSGVO und Revision des Schweizer DSG: Fundamentale Änderungen im Datenschutzrecht der Schweiz?».