www.jusletter.ch

David Rosenthal

Das neue Datenschutzgesetz

Am 25. September 2020 hat das Parlament das neue Datenschutzgesetz (DSG) verabschiedet. Es soll den Schweizer Datenschutz auf das Niveau der EU bringen. Nichtsdestotrotz weicht das revidierte DSG in manchen Punkten von der EU-Datenschutzgrundverordnung (DSGVO) ab und geht an einigen Stellen sogar darüber hinaus. Dieser Beitrag erläutert und kommentiert die für die Privatwirtschaft relevanten Änderungen des DSG im Detail, beantwortet die wichtigsten Fragen und erklärt, was sie für die Praxis bedeuten.

Beitragsart: Wissenschaftliche Beiträge
Rechtsgebiete: Datenschutz, Verwaltungsrecht, Öffentliches Recht, Strafrecht

Zitiervorschlag: David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020

Inhaltsübersicht

I. Einleitung

[1] Anderthalb Jahre blieb die Botschaft des Bundesrats praktisch liegen, und dann ging es los: Nachdem der Nationalrat den Entwurf des Bundesrats in einigen Punkten etwas gelockert hatte, schärfte ihn der Ständerat in der Wintersession 2019 wieder. Zu gross war die Angst davor, dass die Europäische Kommission der Schweiz die «Angemessenheit» nicht wiederzuerkennen würde. Die Angst davor ist wohl übertrieben und zeugt vom üblichen helvetischen vorauseilenden Gehorsam. Auf die extremsten Änderungsanträge aus den eigenen Reihen gingen die Parlamentarier zum Glück nicht ein. Sie konnten jedoch nicht verhindern, dass sich die Linke und die Bürgerlichen vor allem über das Profiling in die Haare gerieten und zum Schluss nur die Einigungskonferenz die Totalrevision vor dem Absturz retten konnte. Es war, wie noch erläutert wird, ein Streit um des Kaisers Bart.

[2] Herausgekommen ist jedenfalls eine Gesetzesrevision, die zwar einige der weniger sinnvollen Bestimmungen der DSGVO übernimmt, in weiten Teilen jedoch vergleichsweise einfach umsetzbar sein wird – auch wenn der Aufwand zur Datenschutz-Compliance in den kommenden Jahren weiter zunehmen wird. So ist die Informationspflicht vernünftiger ausgestaltet als unter der DSGVO, die Meldepflicht bei Verletzungen der Datensicherheit weniger exzessiv und die Anforderungen an eine gültige Einwilligung sind im Gegensatz zu den Vorgaben der DSGVO weiterhin vernünftig. Manche der Vorschriften im revidierten DSG sind wesentlich flexibler als in der DSGVO ausgestaltet und können damit auch den Umständen entsprechend sinnvoller angewandt werden, so etwa die Regelungen für Datenexporte. Die Strafbestimmungen des revidierten DSG sind zwar allen Unkenrufen zum Trotz scharf (weil persönlicher Natur), finden aber in viel weniger Fällen Anwendung als die hohen Unternehmensbussen, welche die DSGVO vorsieht. Die «Cookie»-Regelungen der EU, welche dort noch in der ePrivacy-Richtlinie[1] geregelt sind, übernahm die Schweiz im Rahmen der Revision gar nicht (und hat es derzeit auch nicht vor).

[3] Allerdings brachte das Gesetzgebungsprojekt auch fragwürdige Regelungen und unschöne politische Kompromisse hervor, wenngleich einige davon schlicht den europarechtlichen Vorgaben geschuldet waren. Problematische Regelungen und verpasste Chancen betreffen beispielsweise die Informationspflicht (noch mehr Datenschutzerklärungen, die kaum einer liest), den Datenschutzberater (für welchen es kaum einen gesetzlichen Anreiz gibt), die Meldepflicht für Verletzungen der Datensicherheit (keine *de-minimis*-Regelung), das Auskunfts- und Korrekturrecht (in beiden Fällen heikle Lücken bei den Ausnahmen), die Datenportabilität (nicht zu Ende gedachte Regelung, die viel unnötigen Aufwand und unbeabsichtigte Folgen nach sich ziehen dürfte) sowie das bereits erwähnte Profiling, dem Reizthema der Revision schlechthin. In letzterem Fall entstand allerdings der Eindruck, dass so mancher Parlamentarier die gesetzliche Regelung dazu konzeptionell gar nicht wirklich verstanden hat. Das Parlament hat sich zwar viele Monate um die Legaldefinition des Profilings «mit hohem Risiko» gezankt, aber keine Aufmerksamkeit in die Ausgestaltung der Rechtsfolgen eines solchen investiert. Nationalrat Cédric Wermuth for-

[1] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

mulierte es in einer Debatte im September 2020 im Hinblick auf die fehlenden Rechtsfolgen sehr treffend so: «Man könne in das Gesetz auch reinschreiben, was ein blauer Pavian sei – das hätte genau die gleiche Wirkung wie das, was die Bürgerlichen wollten[2]». Ganz so weit ist es zwar nicht gekommen, aber am Gesetzesstand von heute ändert sich durch die Revision beim Profiling fast nichts. Dazu aber später mehr.

[4] Mit dem **Inkrafttreten** des revidierten DSG wird derzeit im Jahre 2022 gerechnet, möglicherweise sogar erst im Sommer 2022, wie in Bundesbern zu vernehmen ist. Hier wird möglicherweise auch die Europäische Kommission noch ein Wort mitreden, die mit der Erneuerung ihres Angemessenheitsbeschlusses für die Schweiz noch immer zugewartet hat. Mit einem Referendum gegen die Revision wird wiederum nicht gerechnet. Relevante Übergangsfristen sind im Gesetz keine vorgesehen (N 200). In einem nächsten Schritt wird der Bundesrat die revidierten Verordnungen ausarbeiten und zwecks einer Vernehmlassung vorlegen. Darin werden auch zu den neuen Regelungen, wie etwa der Informationspflicht, noch Präzisierungen erwartet, die in diesem Beitrag natürlich noch nicht berücksichtigt werden konnten.

[5] Die nachfolgenden Ausführungen basieren auf einer vertieften Analyse des revidierten DSG, die auch die Praxis und Lehre zur DSGVO (EU-Datenschutz-Grundverordnung) berücksichtigt. Diese Analyse wird in absehbarer Zeit in Form einer Neuauflage des ausführlichen Kommentars des Autors dieses Beitrags und weiterer Co-Autoren zum DSG erscheinen. Auf die Herleitung der Aussagen wird daher weitgehend verzichtet und auf den Kommentar verwiesen. Vorliegend werden zudem nur die Regelungen für private Datenbearbeiter, nicht jene für Bundesorgane besprochen.

[6] Dieser Beitrag verweist auf die Artikelnummerierung des Schlussabstimmungstextes[3]. Ein praktischer synoptischer Vergleich ist auf datenrecht.ch verfügbar, ebenso eine englische Übersetzung. Diverse Formulare für eine Selbsteinschätzung der Datenschutz-Compliance finden sich auf dsat.ch, die derzeit auf den Stand des Schlussabstimmungstextes aktualisiert werden.

II. Zulässigkeit von Datenbearbeitungen

A. Bisheriges Regelungskonzept gilt weiterhin

[7] Die gute Nachricht vorweg: Das **Regelungskonzept des DSG** wird durch die Revision nicht angetastet. Im privaten Bereich gilt weiterhin, dass für die Bearbeitung von Personendaten grundsätzlich weder eine Einwilligung noch sonst ein Rechtfertigungsgrund erforderlich ist. Ein Rechtfertigungsgrund ist nur nötig, wenn entweder die Bearbeitungsgrundsätze (Art. 6 und 8 revDSG) nicht eingehalten werden, die betroffene Person der Bearbeitung widersprochen hat (Art. 30 Abs. 2 Bst. b revDSG) oder einem Dritten besonders schützenswerte Personendaten[4] mitgeteilt werden sollen (Art. 30 Abs. 2 Bst. c revDSG).

---

2 NR Wermuth, Herbstsession 2020, 17. September 2020 (aktuell liegt erst der provisorische Text des amtlichen Bulletins vor).

3 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf (Stand 9. Oktober 2020).

4 Definition in Art. 5 Bst. c revDSG: Die zusätzliche Nennung der «Persönlichkeitsprofile» wurde gestrichen.

[8] Damit unterscheidet sich das DSG wesentlich von der DSGVO, wo Personendaten nach Art. 6, 9 und 10 überhaupt erst bearbeitet werden dürfen, wenn eine angemessene **«Rechtsgrundlage»** besteht. Ähnliches kennt das DSG nur für die Bearbeitung von Personendaten durch Behörden. Da sich auch die Bearbeitungsgrundsätze durch die Revision nicht wesentlich ändern, hat dies zur Folge, dass jene Datenbearbeitungen, die schon bisher DSG-konform waren, auch unter dem revidierten DSG nicht angepasst werden müssen.

[9] An dieser Stelle ist denn auch klarzustellen, dass das DSG **nicht einfach die DSGVO umsetzt** und die Schweiz hierzu – abgesehen vom Schengen-Bereich – auch nicht verpflichtet ist. Was die Schweiz umzusetzen hat, ist die vom Bundesrat bereits unterzeichnete revidierte Konvention 108 des Europarats[5], deren Ratifikation das Parlament ebenfalls zugestimmt hat[6]. Die meisten Änderungen im revidierten DSG basieren auf der Umsetzung der revidierten Konvention 108. Ausschliesslich aus der DSGVO wurde einzig das Recht auf Datenherausgabe und -kopie übernommen. Bei näherer Betrachtung zeigt sich denn auch, dass das revidierte DSG zwar vom Wortlaut der DSGVO inspiriert wurde, in manchen Punkten aber auch wieder davon abweicht. In den meisten dieser Fälle geht das revidierte DSG weniger weit oder ist weniger formalistisch oder weniger detailliert in seinen Regelungen. In einigen wenigen Fällen ist das revidierte DSG jedoch schärfer als die DSGVO[7]. Unternehmen, die bereits DSGVO-konform sind, können dadurch auf ihre bisherigen Umsetzungsarbeiten aufbauen, kommen aber in der Regel nicht ohne gewisse Zusatzprüfungen und -arbeiten aus.

[10] Trotz allem wird die DSGVO und die dazu bestehende Praxis eine gewichtige Auswirkung auf die **Auslegung und Anwendung des revidierten DSG** haben. Das liegt nur schon daran, dass die DSGVO bereits seit Mai 2018 in Kraft ist und damit bereits mehr Erfahrungswerte, Lehrmeinungen und auch erste Behörden- und Gerichtsentscheide dazu vorliegen. Allerdings ist hier Vorsicht geboten: Was für die DSGVO stimmt, muss selbst bei vergleichbaren Regelungen nicht für das DSG gelten. So wurde in der Parlamentsdebatte immer wieder darauf hingewiesen, dass sich das revidierte DSG zwar an die DSGVO «annähern»[8] und mit ihr «vereinbar»[9] bzw. «äquivalent» sein soll[10], das revidierte DSG «sehr nahe an der DSGVO» liege[11], es aber nicht zu einer «Übernahme der DSGVO» kommen soll[12]. In der Parlamentsdebatte wurde mehrheitlich betont, dass ein (positiver) «Swiss Finish» verhindert werden muss, d.h. das DSG, soll nicht *strenger* sein als die DSGVO[13].

---

5 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1.

6 Parlament, Sommersession 2020, 19. Juni 2020 (https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=49459 [Stand 9. Oktober 2020]).

7 So namentlich im Rahmen des sachlichen Geltungsbereichs (Art. 2 revDSG), der Informationspflicht (Art. 19 revDSG), im Auskunftsrecht (Art. 25 revDSG), in der persönlichen Sanktionierung, einschliesslich der beruflichen Schweigepflicht, welche die DSGVO gar nicht kennt und wohl auch in der Schweiz vielen bisher entgangen ist (Art. 60 ff. revDSG). Auch die Definition der besonders schützenswerten Personendaten geht weiter als unter der DSGVO.

8 BR Keller-Sutter, AB 2019 N 1782, Herbstsession 2019, 24. September 2019.

9 SR Fässler, AB 2019 S 1239, Wintersession 2019, 18. Dezember 2019.

10 NR Romano, AB 2019 N 1778, Herbstsession 2019, 24. September 2019; NR Glättli, AB 2019 N 1814, Herbstsession 2019, 25. September 2019.

11 NR Jauslin, AB 2019 N 1775, Herbstsession 2019, 24. September 2019.

12 NR Wermuth, AB 2019 N 1777, Herbstsession 2019, 24. September 2019.

13 NR Romano, AB 2019 N 1802; NR Fluri, AB 2019 N 1782; BR Keller-Sutter, AB 2019 N 1789; NR Flach, NR Brunner, AB 2019 N 1800, Herbstsession 2019, 24. September 2019.

[11] Es ist davon auszugehen, dass die Rechtsprechung des EuGHs zur EU-Datenschutz-Grund*verordnung* (DSGVO) und die Stellungnahmen der europäischen Datenschutzbehörden eine grössere Auswirkung auf die Schweiz haben wird, als die Rechtsprechung zur bisherigen Datenschutz*richtlinie* der EU, die in der Schweiz keine grosse Beachtung fand. Ebenfalls ist damit zu rechnen, dass manche Verantwortliche, Berater und Behörden in der Schweiz die zur DSGVO entwickelten Ansichten (z.B. ausländischer Datenschutzbehörden oder Kommentatoren der DSGVO) aus Risikoerwägungen unbesehen ins Schweizer Recht übernehmen werden. Dies wird im Ergebnis zur Angleichung des DSG an die DSGVO führen, und zwar auch dort, wo die Schweizer Regelung an sich weniger streng angelegt worden wäre. Dieser (absehbare) **Trend zur Gleichschaltung von DSG und DSGVO** mag in der praktischen Umsetzung Vorteile mit sich bringen und gerechtfertigt sein, weil er die Arbeit vereinfacht. Er widerspricht jedoch dem Willen des Gesetzgebers und stösst an seine Grenzen, wenn es um die Beurteilung von Einzelfällen oder darum geht, die genauen Grenzen des rechtlich unter dem DSG noch Zulässigen zu erörtern. Das betrifft beispielweise Streitfälle und Untersuchungen durch den EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter). Speziell in diesen Situationen darf die Lehre und Praxis zur DSGVO bei der Auslegung des DSG nicht einfach übernommen werden. In manchen Bereichen ist das DSG nicht einfach eine knapper formulierte Fassung der DSGVO, auch wenn es vergleichbare Bestimmungen enthält. Die Regelungen haben auch konzeptionelle Unterschiede, wie etwa bei der Beantwortung der Fragen, wann genau welche Informationspflicht zur Anwendung gelangt oder wie mit einem Widerspruch gegen eine Datenbearbeitung von betroffenen Personen umzugehen ist. Die Schweiz hat ein eigenes Datenschutzrecht und soll es auch so anwenden. Damit können auch die in der Parlamentsdebatte immer wieder von diverser Seite kritisierten, durch das EU-Recht verursachten Datenschutz-Exzesse und «unintended consequences» hierzulande vermieden werden.

[12] Das gilt umso mehr, als die DSGVO nicht nur andere Regelungskonzepte verfolgt (Stichwort «Verbotsregelung», N 8), sondern auch hinsichtlich ihres Zwecks weiter geht als das DSG, indem mit der DSGVO nicht nur die Persönlichkeit der betroffenen Personen, sondern auch die «Grundfreiheiten» geschützt werden sollen. Dieses Konzept des EU-Rechts kennt die Schweiz so nicht. Im Ergebnis führt dies dazu, dass die DSGVO nicht nur vor Diskriminierung durch den Staat, sondern auch durch Private schützt, was bei der Anwendung der betreffenden Normen zu berücksichtigen ist. Das DSG hingegen bezweckt nicht den Schutz der Grundfreiheiten und damit auch nicht den darin enthaltenen Diskriminierungsschutz. Das DSG erwähnt zwar in manchen Bestimmungen nebst dem Schutz der Persönlichkeit auch den **Schutz der Grundrechte** (z.B. Art. 22 Abs. 1 revDSG), doch bezieht sich dieser Verweis ausschliesslich auf Fälle, in denen *Bundesorgane* Personendaten bearbeiten. Wo es lediglich um private Datenbearbeitungen geht (z.B. Art. 12 Abs. 5 revDSG) fehlt der Hinweis auf den Schutz der Grundrechte dementsprechend.

B. Neue und erweiterte Begriffe

1. Verantwortlicher und Auftragsbearbeiter

[13] Von der DSGVO vollständig übernommen hat der Schweizer Gesetzgeber die beiden Begriffe des **«Verantwortlichen»** und des **«Auftragsbearbeiters»**. Es sind dies die beiden wesentlichen Rollen, auf welchen das neue DSG aufbaut. Der bisherige «Inhaber der Datensammlung» wurde abgeschafft. Seine Rollenumschreibung wurde aber weitgehend in die Definition des «Ver-

antwortlichen» übernommen. Als Verantwortlicher gilt, wer allein oder zusammen mit anderen «über den Zweck und die Mittel der Bearbeitung entscheidet». Damit ist derjenige gemeint, **der die wesentlichen datenschutzrechtlichen Parameter einer Datenbearbeitung festlegt**. Dahinter steckt die Logik, dass derjenige primär für die Einhaltung des Datenschutzes verantwortlich sein soll, der *de facto* dafür verantwortlich ist, wie die Datenbearbeitung ausgestaltet ist. Das kann eine Person (z.B. ein Unternehmen) alleine sein, es ist aber auch denkbar, dass mehrere Personen – mehr oder weniger stark – an den Entscheidungen über den Zweck und die Mittel einer Datenbearbeitung beteiligt sind. Nicht erforderlich ist, dass alle Entscheide gemeinsam gefällt werden; ein arbeitsteiliges Zusammenwirken genügt. Auch der Einfluss der verschiedenen Personen auf die Entscheidung kann unterschiedlich gross sein – solange es um dieselbe Datenbearbeitung geht, d.h. solange zwischen den Datenbearbeitungen der Verantwortlichen ein untrennbares Band besteht, sind sie alle verantwortlich und gelten als **gemeinsame Verantwortliche**.

[14] Beauftragt ein Klient, seinen Dienstleister (z.B. seinen Anwalt) damit, im Rahmen seiner Dienstleistungserbringung eine bestimmte Datenbearbeitung durchzuführen (z.B. dem Gericht eine bestimmte Klage einzureichen), so entscheidet der Klient über den Zweck (und damit die Ausrichtung) der Datenbearbeitung, auch wenn vereinbart ist, dass der Dienstleister über manche der wesentlichen zur Auftragserfüllung zum Einsatz kommenden Mittel selbst entscheidet (z.B. Einsatz welcher Daten, wie bearbeitet, wo beschafft, wem gegeben, wie lange aufbewahrt), weil der Dienstleister diesbezüglich das grössere Wissen hat. Im Beispiel des Anwalts sind Klient und Anwalt mit Bezug auf die Einreichung der Klage «gemeinsame» Verantwortliche (weil die Klage das Ergebnis eines arbeitsteiligen Zusammenwirkens mit Bezug auf Zweck und wesentliche Mittel ist), mit Bezug auf seine eigene Aktenverwaltung ist der Anwalt hingegen ein alleiniger Verantwortlicher (weil er diese für sich vornimmt und selbst organisiert, auch wenn die Akten vom Klienten stammen und er in dessen Auftrag handelt).

[15] Wer hingegen eine Datenbearbeitung mit Bezug auf deren grosse datenschutzrechtliche Linien **lediglich nach Weisung ausführt**, auch wenn er dabei gewisse weniger wichtige Dinge selbst bestimmen kann (z.B. die konkret eingesetzten Abläufe, Auswahl der Programme, Datensicherheitsmassnahmen), gilt als Auftragsbearbeiter. Ein klassisches Beispiel dafür ist der Cloud-Provider, der seinen Kunden seine Computer und Software zur Bearbeitung von Daten zur Verfügung stellt. Dass er dem Kunden gewisse Services vorkonfiguriert anbietet, ändert nichts daran, dass es der Kunde ist, der die Wahl der Bearbeitungsmittel trifft – so wie der Gast im Restaurant auf der Speisekarte das vordefinierte Menü auswählt oder es eben bleiben lässt, wenn ihm nichts passt.

[16] In der EU gibt es bereits mehrere höchstrichterliche Entscheide zu den **Abgrenzungsfragen**, die in der Praxis viel schwieriger sein können, als es auf den ersten Blick erscheinen mag. Der Autor dieses Beitrags hat sich bereits in einem anderen Beitrag eingehend mit der Abgrenzungsthematik auseinandergesetzt und diese mit zahlreichen Beispielen aus der Praxis illustriert[14]. Der Europäische Datenschutz-Ausschuss (EDSA) hat kürzlich eine Leitlinie zur Vernehmlassung pu-

14 David Rosenthal: Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019; David Rosenthal/Barbara Epprecht, Banken und ihre datenschutzrechtliche Verantwortlichkeit im Verkehr mit ihren Dienstleistern, in: Susanne Emmenegger (Hrsg.), Banken und Datenschutz, Basel 2019 (http://www.rosenthal.ch/downloads/Rosenthal-Epprecht-ControllerProcessor.pdf [Stand 9. Oktober 2020]).

bliziert, die sich mit dem Thema auseinandersetzt[15]. Manche Konstellationen bleiben nach wie vor unklar, so etwa die Frage, ob derjenige, der nur wesentliche Mittel einer Datenbearbeitung aber nicht den Zweck einer Datenbearbeitung festlegt trotzdem (gemeinsamer) Verantwortlicher sein kann[16].

[17] Wer einen Auftragsbearbeiter einsetzt, muss wie im bisherigen Recht typischerweise **mittels Vertrag** dafür sorgen, dass dieser die Datenbearbeitung nur so durchführt, wie dies der Verantwortlich selbst tun darf und riskiert ansonsten neu eine Busse (Art. 9 revDSG, N 57 ff.). Anders als unter Art. 26 DSGVO sieht das revidierte DSG im privaten Bereich dagegen keine pauschale Pflicht zur Regelung der Zuständigkeiten unter gemeinsamen Verantwortlichen vor. Eine solche Regelung kann sich jedoch aus Art. 7 Abs. 1 und 2 revDSG ergeben (N 44)[17].

[18] An der **zivilrechtlichen Haftung für Datenschutzverstösse** haben die beiden neu eingeführten Begriffe nichts geändert: Ins Recht gefasst werden kann weiterhin jeder, der an einer persönlichkeitsverletzenden Datenbearbeitung *mitwirkt*. Dies betrifft übrigens auch die Mitarbeiter oder anderweitig in den Betrieb integrierte natürliche Personen, die weder als Auftragsbearbeiter, noch als Verantwortliche gelten, sofern ihnen die Verletzung zugerechnet werden kann (eine Bestimmung analog zu Art. 29 DSGVO, wonach Daten nur auf Weisung des Verantwortlichen bearbeitet werden dürfen, kennt das revidierte DSG nicht, vgl. auch N 58).

2. Personendaten

[19] Auch der Begriff der **Personendaten** (Art. 5 Bst. a revDSG) wird insofern von der DSGVO übernommen, als dass der bisher in der Schweiz bestehende Schutz juristischer Personen wegfällt. Letztere bleiben jedoch über Art. 28 ZGB geschützt, und es ist davon auszugehen, dass bei einem Streit über eine konkrete Datenbearbeitung, die Bearbeitungsgrundsätze und Rechtfertigungsgründe des DSG analog zur Anwendung gelangen. Ein Auskunftsrecht hat eine juristische Person aber zum Beispiel nicht mehr. Ansonsten ändert sich das Verständnis, was als Personendaten gilt, mit dem neuen Recht nichts: In der Schweiz gilt weiterhin die bundesgerichtlich bestätigte «relative Methode» mit einer Unterscheidung nach der **objektiven und subjektiven Bestimmbarkeit**: Es wird jeweils aus der Sicht desjenigen, der Zugang zu einer Information hat, beurteilt, ob dieser (a) in der Lage ist herauszufinden, auf welche natürliche Person sich die Information bezieht und (b) ob er auch bereit ist, den für die Identifikation erforderlichen Aufwand zu betreiben[18].

[20] Genetische Daten sind somit zum Beispiel erst dann Personendaten, wenn derjenige, der Zugang zu ihnen hat, auch Zugang zu einer Gendatenbank oder einer anderen Informationsquelle hat, welche ihm die Identifikation der Person erlaubt. **Pseudonymisierte Daten**, also codierte

15 European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 1.0), 2. September 2020, (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en [Stand 9. Oktober 2020]).

16 Was im Hinblick auf den Sinn und Zweck der Legaldefinition, all jene ins Recht fassen zu können, die datenschutzrechtlich wesentliche Aspekte einer Datenbearbeitung festlegen, nach der hier vertretenen Ansicht der Fall ist (*a.M.* offenbar David Vasella, Verantwortliche und Auftragsverarbeiter: Zu den Leitlinien des EDSA (Entwurf) zum «Controller» und «Processor», in: datenrecht.ch, 14. September 2020, Ziff. 1.2.1 (https://datenrecht.ch/edsa-entwurf-von-leitlinien-zum-verantwortlichen-und-zum-auftragsverarbeiter) (Stand 9. Oktober 2020).

17 Weiter sieht Art. 33 revDSG vor, dass der *Bundesrat* Regelungen trifft, wenn ein Bundesorgan Personendaten gemeinsam mit einem anderen Bundesorgan, kantonalen Organen oder Privaten bearbeitet. Kantonale Datenschutzgesetze sehen teilweise für ihren Bereich ähnliche Regelungen wie Art. 25 DSGVO 26 vor (z.B. Art. 5 Abs. 1 IDG ZH).

18 BGE 136 II 508, E. 3.2.

oder sonst verschlüsselte Daten, sind wiederum nur für denjenigen noch Personendaten, der Zugang zum Code hat, mit welchem der Personenbezug wiederhergestellt werden kann. Dementsprechend stellen «singularisierte» Daten[19] auch unter dem revidierten DSG noch keine Personendaten dar, obwohl sie sich auf eine einzige Person beziehen. Das gilt an sich auch unter der DSGVO, doch wird dort von Datenschutzbehörden – meist ohne erkennbar vertiefte Erwägungen – immer wieder vertreten, dass eine Singularisierung zur Annahme von Personendaten genügen soll. So werden Cookies und IP-Adressen von ihnen regelmässig pauschal als Personendaten qualifiziert, obwohl der EuGH bisher in beiden Fällen eine differenzierte Ansicht vertrat[20].

3. Besonders schützenswerte Personendaten

[21] Nicht aus der DSGVO übernommen hat der Schweizer Gesetzgeber die Legaldefinition der **besonders schützenswerten Personendaten**. Sie sind zwar ähnlich definiert wie die «besonderen Kategorien von Personendaten», welche in Art. 9 DSGVO geregelt sind, weil ihre Bearbeitung einen besonderen Rechtsgrund erfordert. Sie weichen jedoch in verschiedener Hinsicht vom europäischen Begriff ab. Der Schweizer Begriff ist breiter definiert und umfasst – wie schon im bisherigen Recht – insbesondere auch Personendaten bezüglich verwaltungs- und strafrechtlicher Verfolgungen und Sanktionen (welche in der DSGVO teilweise in Art. 10 geregelt sind), Daten über die Massnahmen der sozialen Hilfe und Daten über die Intimsphäre. Bezüglich letzteren Daten umfasst der Begriff in der DSGVO lediglich Daten zum Sexualleben und zur sexuellen Orientierung.

[22] Erweitert wurde der abschliessende Katalog von Art. 5 Bst. c revDSG um **«genetische Daten»** und **«biometrische Daten, die eine natürliche Person eindeutig identifizieren»**. Auch wenn der Zusatz «die eine natürliche Person eindeutig identifizieren» trotz entsprechenden Versuchen des Nationalrats nicht auch betreffend die genetischen Daten eingeführt wurde, bleiben aus systematischen und teleologischen Gründen nur solche genetische Daten vom DSG erfasst, welche die Anforderungen an Personendaten nach Art. 5 Bst. a revDSG erfüllen. Mit anderen Worten, auch die Bearbeitung von genetischen Daten fällt nur in den Anwendungsbereich des DSG, wenn die genetischen Daten Rückschlüsse auf die Identität einer natürlichen Person zulassen. In der DSGVO ist dies ausdrücklich festgehalten[21]. Zwar lässt die parlamentarische Diskussion darauf schliessen, dass gewisse Parlamentarier genetische Daten *per se* als Personendaten erachteten, aber diese (und auch andere) Aussagen erscheinen primär als Ausdruck mangelnder Sachkenntnis, und nicht als Willen des Gesetzgebers, genetische Daten *per se* zu Personendaten zu erklären[22]. Es ist nicht ersichtlich, dass der Gesetzgeber Sachdaten auf dem Weg der Legaldefinition

19 Also Daten, die wie ein Fingerabdruck so individuell oder eben «singulär» sind, dass sie sich nur auf eine einzige Person beziehen können, obwohl diese damit noch nicht identifiziert wird.

20 Vgl. David Rosenthal, Personendaten ohne Identifizierbarkeit?, in: Digma Dezember 2017, Heft 4 (http://www.rosenthal.ch/downloads/digma_2017_4_Rosenthal.pdf) [Stand 9. Oktober 2020]); Urteil des EuGH vom 19. Oktober 2016, C-582/14 («Breyer»), Rz. 44–49 sowie Urteil des EuGH vom 1. Oktober 2019, C-673/17 («Planet49»), Rz. 71.

21 Als genetische Daten gelten dort «*personenbezogene* Daten zu den ererbten oder erworbenen Eigenschaften einer natürlichen Person (...)» (Art. 4 Nr. 13 DSGVO).

22 Die pauschale Unterschutzstellung von genetischen Daten müsste systematisch an einem anderen Ort erfolgen, denn die Definition der besonders schützenswerten Personendaten besagt nur, welche *Personendaten* besonders schützenswert sind. Eine Klassifizierung von genetischen Daten als besonders schützenswerte Personendaten setzt aber voraus, dass sich aus dem DSG ergibt, dass es sich bei genetischen Daten überhaupt um Personendaten handelt. Ebenso ist nicht ersichtlich, dass die Schweiz über den Schutzumfang genetischer Daten gemäss der DSGVO hinausgehen wollte. Auch der weggelassene Zusatz besagt diesbezüglich nichts: Er hätte lediglich genetische *Perso-*

besonders schützenswerter Personendaten zu Personendaten erklären wollte. Eine andere Frage ist, wieviel Raum nach dem aktuellen Stand der Wissenschaft überhaupt noch bleibt, dass genetische Daten in einem bestimmten Kontext keine Rückschlüsse auf eine bestimmte Person erlauben. Der Zusatz bei den biometrischen Daten ist deshalb nötig, weil sonst beispielsweise auch «normale» Fotos von Gesichtern oder anderen Körperteilen besonders schützenswerte Personendaten wären.

[23] Der Begriff der «besonders schützenswerten Personendaten» ist weiterhin leicht irreführend. Der Katalog ist abschliessend, doch bedeutet das weder, dass die darin bezeichneten Personendaten im Einzelfall auch besonders heikel sein müssen (z.B. politische Aussagen eines Politikers) noch, dass andere Personendaten nicht sensibel sein können (z.B. Angaben zum Einkommen oder ein Bewegungsprofil). Die Schweiz war und ist jedoch aufgrund der Europaratskonvention verpflichtet, für diese Kategorien von Personendaten im DSG einzelne zusätzliche Schutzregeln vorzusehen. Das Vorliegen von Personendaten mit dem Prädikat «besonders schützenswert» ist immerhin ein klares Indiz dafür, dass es sich dabei um sensible Daten handelt. Generell galt und gilt im DSG aber sowieso das Prinzip **der risikobasierten Anwendung der Normen**, die eine Wertung des Einzelfalls zulassen und erfordern: Je sensibler Daten oder ein Bearbeitungsvorgang im Hinblick auf die Verletzung der Persönlichkeit der betroffenen Personen ist, desto mehr Vorkehrungen müssen getroffen werden, damit es nicht zur Verletzung kommt (vgl. Art. 7 und 8 revDSG).

4. Profiling mit und ohne «hohem Risiko»

[24] Auf den ersten Blick aufgegeben hat die Schweiz ihre Eigenschöpfung des «Persönlichkeitsprofils», für welche bisher dieselben Regelungen galten, wie für besonders schützenswerte Personendaten. Stattdessen wurde neu der Begriff des **«Profilings»** eingeführt (Art. 5 Bst. f revDSG). Entgegen dem Vorschlag des Bundesrates übernahm das Parlament hierfür die Legaldefinition der DSGVO. Das Profiling beginnt quasi dort, wo das Persönlichkeitsprofil aufhört: Letzteres ist die *Sammlung* der Daten, die die Beurteilung wesentlicher Aspekte einer Person *erlaubt*, während das Profiling den Vorgang *der Bewertung* solcher Aspekte erfasst, also weder den Input, noch den Output. Der Begriff der «Bewertung» umfasst zudem nur solche Bearbeitungen, die eine *Interpretation* des Inputs erfordern, d.h. eine **Wertung verlangen**, eine subjektive Komponente enthalten wie z.B. eine Prognose. Kein Profiling ist die objektive Feststellung eines Sachverhalts.

[25] Die Interpretation muss **automatisiert** erfolgen, d.h. nicht manuell durch einen Menschen, und sie muss sich auf eine individuell betroffene Person (nicht auf eine Gruppe von Menschen) beziehen. Darum ist ein automatisierter HIV-Test kein Profiling im Sinne des DSG (die Antwort auf die simple Ja/Nein-Frage, ob Virus-Antikörper vorliegen, muss immer dieselbe sein, egal, wer oder was den Test durchführt) während die Analyse eines Cervix-Abstriches bei einer Frau im Hinblick auf das Krebsrisiko ein Profiling darstellt, sobald sie automatisiert erfolgt (da die Analyse der Gewebeprobe einer Interpretation bedarf, ob es sich um eine gutartige oder bösartige Wucherung handelt, was heute automatisiert möglich ist).

[26] Darin zeigt sich auch das besondere Risiko beim Profiling: Eine Person bzw. ein Aspekt von ihr wird durch eine Maschine *bewertet*, und nicht mehr durch einen Menschen. Auch wenn die

*nen*daten (die als Personendaten gelten, weil sie dazu fähig sind, eine Person zu identifizieren) als besonders schützenswert erklärt.

Bewertung der Maschine auf einen menschlichen Befehl zurückgeht, so erfolgt sie doch schematisch. Damit ein Vorgang als Profiling gilt, muss dies das Ziel bzw. Motiv der Bearbeitung sein: Erstellt ein Weinhändler eine Statistik, welcher Kunde welche Sorte von Weinen gekauft hat, um sein Sortiment besser zu gestalten, ist dies kein Profiling. Zieht er aus derselben Datenbank eine Liste von pauschal allen Käufern von spanischen Weinen, um diese anzuschreiben, weil er glaubt, sie seien am ehesten an einer neuen Lieferung solcher Weine *interessiert* (automatische Bewertung), ist dies ein Profiling. Wählt er jeden Kunden von Hand aus, ist es keins. Ein manuelles Profiling im Sinne des DSG gibt es schon begriffslogisch nicht.

[27] Beim **Profiling «mit hohem Risiko»** (Art. 5 Bst. g revDSG) konnten sich die Räte erst zum Schluss einigen. In der Debatte war allen klar geworden, dass nicht jedes Profiling wirklich heikel ist, wie auch das vorangehende Beispiel des Weinhändlers zeigt. Um das Problem zu lösen, wurde der Begriff des Persönlichkeitsprofils durch die Hintertüre wieder eingeführt: Als Profiling mit hohem Risiko kommt jenes Profiling in Frage, das zu einer Verknüpfung von Daten führt und dadurch eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Das ist nichts anderes, als das altbekannte Persönlichkeitsprofil. Ein Beispiel ist die Firma, welche das Persönlichkeitsprofil des idealen Stellenbewerbers definiert und dann vom Computer beurteilen lässt, wer diesem am besten entspricht. Die neue Regelung ist allerdings zumindest dem Wortlaut nach strenger geraten als das heutige Recht: Selbst wenn ein Computer eigenständig ein Persönlichkeitsprofil erzeugt, liegt trotzdem nur dann ein Profiling mit hohem Risiko vor, wenn die Erzeugung des Persönlichkeitsprofils zu einem hohen Risiko für die betroffene Person führt («ein hohes Risiko [...] mit sich bringt, *indem* es zu einer Verknüpfung von Daten führt [...]»). Ob tatsächlich ein hohes Risiko der Verletzung von Persönlichkeitsrechten vorliegt, hängt in der Tat von den konkret getroffenen Schutzmassnahmen ab. Die alternative, im Parlament teilweise vertretene Ansicht, wonach aus dem Vorliegen eines Persönlichkeitsprofils *per se* ein hohes Risiko resultiert, erscheint problematisch und zieht Folgeprobleme nach sich[23] (vgl. dazu die Ausführungen zur Datenschutz-Folgenabschätzung, N 148 ff.). Umgekehrt kann ein Profiling auch ohne Persönlichkeitsprofil zu einem hohen Risiko führen. Es ist also sinnvollerweise eine von der Legaldefinition unabhängige Beurteilung nötig. Die Streichung des Persönlichkeitsprofils wird dort, wo es in einer Gesetzesbestimmung durch «Profiling mit hohem Risiko» ersetzt wurde nur teilweise kompensiert weil neu mindestens eine Automatisierung der Bewertung nötig ist. Wo stattdessen lediglich auf «Profiling» verwiesen wird, was namentlich bei wichtigen Bestimmungen für Bundesorgane der Fall ist[24], wurde das neue DSG verschärft, weil neu mehr erfasst wird als bisher, nämlich sämtliche Verknüpfungen von Daten, die eine Beurteilung von (auch unwesentlichen) Persönlichkeitsaspekten einer natürlichen Person erlauben.

[28] Über das Profiling wurde im Parlament und auch in der breiten Öffentlichkeit viel diskutiert. Die **rechtliche Relevanz des Begriffs** ist jedoch beschränkt. Ausser bei den Anforderungen an eine gültige Einwilligung (N 30 ff.) und beim Rechtfertigungsgrund der Kreditwürdigkeitsprüfung

23 Eine Fiktion des hohen Risikos würde die *tatsächlichen* Auswirkungen der Verwendung eines Persönlichkeitsprofils völlig ausser Acht lassen. Jegliche Verwendung eines Persönlichkeitsprofils würde *per se* als hochrisikoreich eingestuft und müsste immer dem EDÖB vorgelegt werden (Art. 23 revDSG). Es gibt keinen Hinweis darauf, dass der Gesetzgeber einen solchen, weit über das Profiling und das bisherige Recht hinausgehenden Persönlichkeitsschutz durch die Hintertür der Legaldefinition des «Profiling mit hohem Risiko» beabsichtigte. Letztere ist doch lediglich ein Kompromiss in letzter Minute im Streit um den Umfang des Schutzes der betroffenen Personen vor Profiling. Im Fokus hatten die Räte nur die Frage der Einwilligung und Kreditwürdigkeitsprüfung. Das hohe Risiko gemäss Legaldefinition müsste also ein anderes sein als in Art. 23 revDSG.

24 Beispielsweise Art. 34 revDSG.

(N 42), kommt das Profiling in den für die Privatwirtschaft relevanten Regelungen des DSG gar nicht vor. Bei den automatisierten Einzelentscheiden (N 106 ff.) hat das Parlament das Profiling aus der Bestimmung gestrichen, ebenso bei der Datenschutz-Folgenabschätzung (N 148 ff.). Mit anderen Worten: Das Parlament hat über eine Legaldefinition ohne wirkliche Rechtsfolgen gestritten, jedenfalls im Hinblick auf die privaten Datenbearbeiter. Ein spezielles Widerspruchsrecht zum Profiling, welches die Ratslinke einführen wollte, kam nicht durch. Das Profiling wird durch das DSG nicht mehr und nicht weniger eingeschränkt, als jede andere Datenbearbeitung. Es gilt auch hier der risikobasierte Ansatz, d.h. es muss zum Beispiel geprüft werden, ob ein Profiling verhältnismässig ist oder ob die Bewertung einer Person lieber einem Menschen überlassen werden soll, der die Bewertung im Einzelfall vornimmt. Es muss geprüft werden, ob die Grundsätze der Zweckbindung und der Transparenz eingehalten sind, die sowieso für jede Datenbearbeitung gelten. Viele Profilings werden absolut harmlos sein, und zwar viel harmloser als ein Persönlichkeitsprofil. Darum ist es unglücklich, dass von Bundesorganen neu verlangt wird, dass sie für jedes Profiling eine formalgesetzliche Grundlage haben müssen (Art. 34 Abs. 2 Bst. b revDSG). Das neue DSG sieht somit kein grundsätzliches Einwilligungserfordernis beim Profiling vor, auch nicht bei hohem Risiko[25].

5. Verletzung der Datensicherheit

[29] Vgl. hierzu die Ausführungen unter N 161.

C. Einwilligung

[30] An der Legaldefinition der Einwilligung hat sich – richtigerweise – materiell nichts geändert. Die vom Bundesrat noch vorgeschlagene Klarstellung, wonach eine Einwilligung eindeutig erfolgen muss, wurde vom Parlament gestrichen. Damit ist klar, dass auch im Datenschutzrecht **kein anderer Standard für Einwilligungen** gilt, wie bisher und sonst im Schweizer Recht für Willenserklärungen. Die Einheit der Rechtsmaterie bleibt damit gewahrt. Notabene war schon bisher klar, dass je mehr Risiken eine Datenbearbeitung für die betroffene Person birgt, umso höher die Anforderungen an die Gültigkeit der Einwilligung sind. Kästchen dürfen auf einem elektronischen Formular daher anders als unter der DSGVO[26] grundsätzlich weiterhin vorangekreuzt sein[27], die Gültigkeit der Einwilligung setzt keine Information über das Widerrufsrecht

25 So auch David Vasella, Neues DSG: kein grundsätzliches Einwilligungserfordernis beim Profiling, auch nicht bei hohem Risiko, in: datenrecht.ch, 25. September 2020 (https://datenrecht.ch/neues-dsg-kein-grundsaetzliches-einwilligungserfordernis-beim-profiling-auch-nicht-bei-hohem-risiko/ [Stand 9. Oktober 2020]).

26 Vgl. Urteil des EuGH vom 1. Oktober 2019, C-673/17 («Planet49»), Rz. 62, mit Hinweis auf den Erwägungsgrund 32 der DSGVO, wonach bereits angekreuzte Kästchen keine Einwilligung darstellen.

27 Entscheidend ist, dass das angekreuzte Kästchen bei der Bestätigung des Formulars durch die betroffene Person Teil ihrer Willenserklärung wird, was üblicherweise der Fall ist, wenn es für die betroffene Person als solches vor der Bestätigung erkennbar ist. Das gilt auch im Falle einer ausdrücklichen Einwilligung: Wer auf einem Anmeldeformular seine Adresse angibt, ein ebenfalls darauf enthaltenes Kästchen, welches die Einwilligung in eine bestimmte, auf dem Formular umschriebene Datenbearbeitung signalisiert, angekreuzt lässt und dann durch Knopfdruck das gesamte Formular als Inhalt seiner Willenserklärung bestätigt, nimmt mit diesem Knopfdruck das zur Ausdrücklichkeit erforderliche aktive Verhalten vor (N 31). Würde zusätzlich das aktive Anklicken der Box verlangt, würden im Ergebnis zur Gültigkeit zwei Willenserklärungen für dieselbe Einwilligung verlangt. Auch bei einem Papierformular käme im Schweizer Recht niemand auf die Idee, das Ankreuzen einer Box zu verlangen, damit eine im Formular wiedergegebene Einwilligungserklärung als ausdrücklich erteilt gilt, wenn das Formular überdies unterschrieben wird. Anders wäre es höchstens dann, wenn die Einwilligungserklärung so auf dem Formular

voraus und ein Koppelungsverbot im strengen Sinne von Art. 7 Abs. 4 DSGVO gibt es im Schweizer Recht auch nicht[28] (vgl. auch N 51). Auch Einwilligungen von Kindern sind im Schweizer Recht weniger starr geregelt als nach Art. 8 DSGVO[29].

[31] Nichts geändert wurde auch am Konzept, dass Art. 6 Abs. 6 und 7 revDSG lediglich definieren, unter welchen Voraussetzungen eine Einwilligung im Kontext des DSG gültig ist. Sie besagen weder, *dass* eine Einwilligung grundsätzlich erforderlich ist, noch in welchen Fällen eine Einwilligung notwendig ist[30]. In welchen Fällen eine Einwilligung erforderlich ist bzw. als Rechtfertigungsgrund dient, legt das DSG anderswo fest, nämlich in Art. 17 Abs. 1 Bst. a revDSG (Datenexport), Art. 21 Abs. 3 Bst. b revDSG (automatisierte Einzelfallentscheide), Art. 25 Abs. 3 revDSG (Auskunftsrecht betreffend Gesundheitsdaten), Art. 31 Abs. 1 revDSG (Rechtfertigungsgründe), Art. 34 Abs. 4 Bst. b revDSG (Bearbeitung ohne hinreichende Rechtsgrundlage durch Bundesorgane) und Art. 36 Abs. 2 Bst. b revDSG (Bekanntgabe von Personendaten durch Bundesorgane). Bezüglich der Frage, wann eine Einwilligung eingeholt werden muss, herrscht in der Praxis nach wie vor eine gewisse Unsicherheit. Doch das DSG ist in dieser Hinsicht klar: Es gibt **gegenüber der bisherigen Rechtslage keine Veränderungen**. Es bestand seitens des Gesetzgebers auch keine Absicht, die bisherige Handhabung zu ändern. Dies wäre auch konzeptwidrig (N 40). Anträge, eine Pflicht zum Einholen einer Einwilligung für bestimmte Datenbearbeitungen festzuschreiben, wurden in der parlamentarischen Diskussion abgelehnt[31].

[32] Keine Pflicht eine Einwilligung einzuholen gilt auch für Art. 6 Abs. 7 revDSG, welcher sich auf die Bearbeitung von besonders schützenswerten Daten und Profiling mit oder ohne hohem Risiko bezieht (je nachdem, ob es um ein Bundesorgan geht oder nicht). Auch hier besagt die Bestimmung nur, dass – falls für solche Fälle auf eine Einwilligung abgestellt werden soll – die Einwilligung eine ausdrückliche zu sein hat. Verwirrung herrscht teils immer noch hinsichtlich der Frage, was **«ausdrücklich»** bedeutet. Es bedeutet nicht, dass eine Einwilligung schriftlich erfolgen muss. Ausdrücklich ist das Gegenteil von konkludent, und so ist der Begriff auch zu verstehen: Eine Einwilligung ist dann ausdrücklich, wenn ein (i) aktives Verhalten oder ein solches Verhalten vorliegt, das als affirmativ vereinbart wurde (z.B. mittels einer AGB-Klausel, wonach ein Schweigen auf eine AGB-Änderung hin als Zustimmung gilt) und (ii) die Bedeutung dieses affirmativen Verhaltens sich direkt auf die betreffende Datenbearbeitung bezieht[32]. Konkludent wäre eine Einwilligung dagegen, wenn sich das affirmative Verhalten nicht auf die Datenbearbeitung bezieht, sondern lediglich auf die Handlung, welche die Datenbearbeitung zur Folge hat.

«versteckt» wäre, dass nicht damit gerechnet werden kann, dass der Benutzer sie zur Kenntnis nimmt und selbst dann stellt sich die Frage, ob sie wie bei AGB in Anwendung der Globalübernahme vorbehältlich der Ungewöhnlichkeitsregel konsequenterweise nicht doch gelten müsste.

28 Auch in der Schweiz kann der Abschluss einer Vereinbarung nicht beliebig von der Erteilung einer Einwilligung in eine bestimmte Datenbearbeitung abhängig gemacht werden, da eine solche Koppelung die Freiwilligkeit der Einwilligung tangieren kann. Die Hürden sind im Schweizer Recht allerdings wesentlich höher als unter der DSGVO – ist eine Koppelung nicht sachfremd und wird auch sonst kein unzulässiger Zwang ausgeübt, so ist sie zulässig (vgl. dazu das Urteil des BVerwG vom 19. März 2019, A-3548/2018 «Helsana+», E. 4.7).

29 Die Gültigkeit von Einwilligungen nach DSG richtet sich bei Minderjährigen grundsätzlich nach Art. 19c ZGB, wonach urteilsfähige Minderjährige selbst entscheiden können. Urteilsfähigkeit wird typischerweise ab einem Alter von 13 Jahren angenommen.

30 So auch David Vasella, Neues DSG: kein grundsätzliches Einwilligungserfordernis beim Profiling, auch nicht bei hohem Risiko, in: datenrecht.ch, 25. September 2020 (https://datenrecht.ch/neues-dsg-kein-grundsaetzliches-einwilligungserfordernis-beim-profiling-auch-nicht-bei-hohem-risiko/ [Stand 9. Oktober 2020]).

31 Ständerat, AB 2019, S. 1246 f., Wintersession 2019, 18. Dezember 2019.

32 Vgl. David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, Rz. 31 f.

Wer also beispielsweise in den Erhalt personalisierter Werbung einwilligt, hat nicht gleichzeitig auch ausdrücklich in die Vornahme des dieser Werbung zugrundeliegenden Profilings mit hohem Risiko eingewilligt, und zwar egal, ob die Einwilligung in den Erhalt der Werbung ausdrücklich erfolgte. Die Datenbearbeitung muss also im Ergebnis *beim Namen genannt* werden.

D. Grundsätze der Datenbearbeitung

1. Die Bearbeitungsgrundsätze

[33] Die Bearbeitungsgrundsätze finden sich neu in Art. 6 revDSG und sind sprachlich etwas umgestaltet worden, **entsprechen aber materiell dem bisherigen Recht**. So jedenfalls will es die Botschaft verstanden wissen[33], und in der Sache macht dies auch Sinn. Für die Praxis bedeutet dies, dass Datenbearbeitungen, die bisher erlaubt waren, grundsätzlich auch mit dem Inkrafttreten des neuen DSG weiterhin erlaubt sein werden. Die Änderungen in Art. 6 revDSG haben vor allem mit einer sprachlichen Angleichung an das europäische Umfeld zu tun. Aus dogmatischer Sicht hat der Gesetzgeber jedoch gewurstelt: Der Grundsatz der (inhaltlichen) Richtigkeit der Daten fällt mit seiner überlangen Formulierung völlig aus dem Rahmen, der Grundsatz der Verhältnismässigkeit kommt neu doppelt vor (Art. 6 Abs. 2 und 4 revDSG) und der Grundsatz der Transparenz wurde trotz seiner Wichtigkeit als ausdrückliche Regelung ohne Not aus dem Wortlaut von Art. 6 revDSG gestrichen.

[34] Gemäss Art. 6 revDSG dürfen Personendaten weiterhin nur **rechtmässig** bearbeitet werden (Abs. 1), also nicht in Verletzung einer anderen Norm des Schweizer Rechts, welche direkt oder indirekt den Schutz der Persönlichkeit bezweckt[34], wie beispielsweise das Recht am eigenen Bild. Die Bearbeitung hat nach Treu und Glauben zu erfolgen und in jeder Hinsicht **verhältnismässig** zu sein (Abs. 2). Letzteres bedeutet, dass die Datenbearbeitung nur so weit gehen darf, wie dies für den verfolgten Zweck nötig, geeignet und verhältnismässig im engeren Sinn – d.h. für die betroffene Person zumutbar – ist. Wenn Abs. 4 neu verlangt, dass Daten vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind, wird lediglich wiederholt, was Abs. 2 bereits verlangt. Die Formulierung «vernichtet» ist nicht wörtlich zu nehmen: Selbstverständlich genügt bereits die datenschutzkonforme Löschung der Daten[35]; vernichtet werden müssen sie nicht, denn Vernichtung impliziert die Zerstörung des Datenträgers. Es reicht aus sicherzustellen, dass keine Personendaten mehr vorliegen, weshalb Abs. 4 auch die Anonymisierung erwähnt. Sogar die Pseudonymisierung genügt, wenn derjenige, der die Daten nicht mehr braucht, keinen Schlüssel zur Entschlüsselung der Daten mehr hat (und unbefugte Personen auch nicht). Abs. 4 umschreibt freilich nur einen Aspekt der Verhältnismässigkeit. Andere Aspekte, wie etwa den Grundsatz der Datensparsamkeit, ergeben sich daher nur aus Abs. 2, wie dies schon bisher der Fall war.

[35] Neu formuliert ist der **Zweckbindungsgrundsatz** in Art. 6 Abs. 3 revDSG. Inhaltlich bleibt es beim Alten, mit einer Einschränkung (N 36). Personendaten dürfen wie bisher nur für diejenigen Zwecke bearbeitet werden, die der betroffenen Person im Zeitpunkt der Datenbeschaffung

33 BBl 2017 7024 ff.

34 Urteil des BVerwG vom 19. März 2019, A-3548/2018, E. 5.4.4.

35 Zur Frage, wann Daten gelöscht sind, vgl. David Rosenthal, Löschen und doch nicht löschen, in: Digma, Dezember 2019, Heft 4 (http://www.rosenthal.ch/downloads/digma_2019_4_Rosenthal.pdf [Stand 9. Oktober 2020]).

erkennbar waren. Dies ist (weiterhin) dann der Fall, wenn die betroffene Person vor der Beschaffung informiert wurde, die Bearbeitung im Schweizer Recht so vorgesehen ist oder sie aus den Umständen erkennbar war[36]. Damit soll zugleich dem Grundsatz der Transparenz Rechnung getragen werden, was aber nur halbrichtig ist: Art. 6 Abs. 3 revDSG verlangt zwar, dass die Beschaffung der Personendaten als solche erkennbar ist (d.h. keine heimliche Beschaffung) und die Zwecke, zu welchen die Personendaten bearbeitet werden sollen, der betroffenen Person kommuniziert werden müssen, aber weitere Parameter der Datenbearbeitung müssen demnach nicht erkennbar sein. Damit ergeben sich rein aus dem Wortlaut im Revisionstext weniger umfassende Aufklärungspflichten als aus der bisherigen Regelung des **Grundsatzes der Erkennbarkeit** nach Art. 4 Abs. 4 DSG. Dogmatisch muss daher auf den Grundsatz der Bearbeitung nach Treu und Glauben in Art. 6 Abs. 2 revDSG zurückgegriffen werden, der schon vor Einführung des Grundsatzes der Erkennbarkeit im Jahre 2008 verlangte, dass Datenbearbeitungen transparent zu erfolgen haben. Mit anderen Worten: Art. 6 Abs. 3 revDSG verlangt, dass die Beschaffung und deren Zwecke offengelegt werden, während Abs. 2 verlangt, dass auch weitere je nach Einzelfall wichtige Parameter der Datenbearbeitung erkennbar sind; jedenfalls soweit an ihnen ein besonderes Interesse bestehen dürfte. Ein besonderes Interesse kann beispielsweise daran bestehen, welche Daten beschafft werden (z.B. Erkennbarkeit des Blickwinkels einer Sicherheitskamera im Gebäude) oder wem die Daten allenfalls mitgeteilt werden (z.B. Behörden). Zwar sieht auch Art. 19 revDSG eine Informationspflicht vor. Aber diese dient lediglich dazu, den betroffenen Personen auf Wunsch weitergehende Informationen zur Datenbearbeitung mitzuteilen. Die Informationspflicht gemäss Art. 19 revDSG ist öffentlich-rechtlicher Natur, während der Bearbeitungsgrundsatz in Art. 6 revDSG eine Konkretisierung von Art. 28 ZGB darstellt. Das ist so wie bei Lebensmitteln: Für den Konsumenten muss sofort erkennbar sein, worum es sich beim Lebensmittel handelt (Erdbeerkonfitüre), während aus dem Kleingedruckten die detaillierte Zusammensetzung hervorgeht. Ersteres entspricht der Erfüllung des Transparenzgrundsatzes nach Art. 6 revDSG, letzteres der Erfüllung der Informationspflicht nach Art. 19 revDSG.

[36] Neu eingeführt wird in Art. 6 Abs. 3 revDSG auch das Konzept der **«Vereinbarkeit» eines Bearbeitungszwecks**. Die DSGVO kennt dieses System bereits und führt es in Art. 6 Abs. 4 DSGVO näher aus. Es weitet den Kreis der zulässigen Zwecke über die für die betroffene Person erkennbaren Zwecke hinaus aus. Erhebt ein Online-Shop die Daten seiner Kunden für die Abwicklung von Bestellungen, so ist dieser Zweck erkennbar und daher vom (engen) Zweckbindungsgrundsatz gedeckt. Beginnt der Online-Shop nun, diese Daten auch für die Betrugsbekämpfung zu analysieren, so benutzt er die Daten nicht mehr zum Zweck, für den sie beschafft wurden. Bisher war dieser Fall eine Verletzung des Zweckbindungsgrundsatzes, der eine Rechtfertigung nach Art. 13 DSG erforderte. Neu ist dies nicht mehr der Fall: Der Sekundärzweck ist mit dem Primärzweck «vereinbar» und daher ebenfalls gedeckt. Nicht vereinbar mit dem Bearbeitungszweck wäre es hingegen, wenn der Online-Shop aus diesen Daten Profile mit den Konsumgewohnheiten seiner Kunden erstellen würde, um diesen individuell zugeschnittene Werbeangebote unterbreiten zu können[37]. Wenn der Online-Shop dies tun will, braucht er dafür zwar keine Einwilligung, aber er müsste die Kunden vorgängig in seiner Datenschutzerklärung darüber informieren, dass er ihre Daten auch für diese Zwecke (personalisierte Werbung, nicht Betrugsbekämpfung) verwendet, und nicht nur zur Abwicklung der Bestellungen, sofern dies nicht sonst aus den Umständen er-

36 BBl 2017 7025.

37 Vgl. BBl 2017 7025 (ähnliches Beispiel).

kennbar ist. Es ist dann ein offiziell kommunizierter weiterer Zweck, der mit dem ursprünglichen Zweck (Vertragsabwicklung) auch nicht mehr vereinbar sein muss. Ein weiteres klassisches Beispiel für eine Bearbeitung, die mit dem ursprünglich angegeben Zweck normalerweise vereinbar ist, ist die Pseudonymisierung oder **Anonymisierung von Daten, um sie für irgendeinen anderen Zweck zu verwenden** (z.B. um sie einem Dritten mitzuteilen, für den sie keine Personendaten mehr sind). Bisher war dies streng genommen ebenfalls eine Verletzung des Zweckbindungsgrundsatzes, es sei denn, der Verantwortliche verfügte selbst über keine Kopie mehr (in diesem Fall kommt die Anonymisierung einer Löschung gleich und darauf folgend findet das DSG keine Anwendung mehr). Wann jedoch ein Sekundärzweck mit dem Primärzweck «vereinbar» ist, definiert das Gesetz nicht wirklich und gibt – anders als die DSGVO – auch keine Hinweise[38]. Die Botschaft erachtet jeden Sekundärzweck als nicht vereinbar, der angesichts des Primärzwecks als «unerwartet, unangebracht oder beanstandbar» erachtet würde[39] und erwähnt als Beispiele das Beschaffen von E-Mail-Adressen im Internet zwecks Versendung von unverlangter Werbung oder die Weiterverwendung von Adressen zu kommerziellen Werbezwecken, die beim Unterschriftensammeln für eine politische Kampagne erfasst wurden[40]. Mindestens das erstgenannte Beispiel (Beschaffen von E-Mail-Adressen im Internet) ist allerdings fehl am Platz, weil bei von einer Person selbst veröffentlichten Daten ohnehin eine andere Regelung greift[41]. Im Ergebnis wird sich jedenfalls für private Verantwortliche durch das Kriterium der «Vereinbarkeit» in den meisten Fällen kaum etwas ändern. Dogmatisch wird es vor allem bei Sekundärnutzungen ein Thema sein.

[37] Die langen Ausführungen zur **Datenrichtigkeit** in Art. 6 Abs. 5 revDSG ändern ebenfalls nichts am bisherigen Grundsatz. Schon bisher war es so, dass Daten immer «nur» im Hinblick auf ihren Zweck richtig sein mussten: Wer Geschäftskorrespondenz mit falschen Anschuldigungen über eine Person erhält, muss diese nicht vernichten, wenn er sie als falsch erkennt, denn ihre Aufbewahrung dient nicht dazu, die Richtigkeit des Inhalts zu dokumentieren, sondern nur die Tatsache, dass die Anschuldigungen gemacht wurden. Neu wird in Abs. 5 klargestellt, dass der Verantwortliche von sich aus tätig werden muss, wenn er bei sich gespeicherte Personendaten als falsch erkennt, d.h. er muss bzw. darf nicht darauf warten, bis sich jemand beschwert. Allerdings hat das Parlament durch den erst im Rahmen der Beratungen eingefügten Satz 2 ebenfalls klargestellt, dass auch Berichtigungsmassnahmen oder – falls solche nicht möglich sind – die Datenlöschung nur dort erforderlich sind, wo dies auch verhältnismässig erscheint. Wer also beim Weihnachtskartenversand feststellt, dass gewisse Briefe unzustellbar zurückkommen, darf die Adressen in seinem Verteiler belassen, wenn er möchte, da die inkorrekten Adressen keinen Schaden anrichten. Der Anspruch auf Berichtigung ist übrigens neu korrekterweise nicht mehr bei den Bearbeitungsgrundsätzen kodifiziert, sondern in einer separaten Bestimmung in Art. 32 Abs. 1 revDSG geregelt (dazu N 137 ff.).

38 Dort: Art. 6 Abs. 4 DSGVO.

39 BBl 2017 7025.

40 BBl 2017 7025.

41 Art. 30 Abs. 3 revDSG.

2. Weitere Grundsätze, Persönlichkeitsverletzungen

[38] Nebst dem in Art. 8 revDSG festgeschriebenen Bearbeitungsgrundsatz der Datensicherheit (N 53) finden sich (wie bisher in Art. 12 DSG) in Art. 30 revDSG noch zwei weitere Grundsätze, welche ihrer Natur nach ebenfalls Bearbeitungsgrundsätze sind:

a) **Besonders schützenswerte Personendaten** dürfen **nicht Dritten bekanntgegeben** werden (Abs. 2 Bst. c), wobei der Begriff der «Dritten» eigenständige Verantwortliche meint, also nicht etwa Auftragsbearbeiter oder gemeinsame Verantwortliche im Rahmen der gemeinsamen Datenbearbeitung. Dieser (schon im bisherigen Recht existierende) Grundsatz lässt sich nicht direkt aus Art. 28 ZGB und den allgemeinen Prinzipien des Persönlichkeitsschutzes ableiten, sondern ist ein bewusster Entscheid des Gesetzgebers in Umsetzung europarechtlicher Vorgaben. Der Grundsatz geht weniger weit als bisher, weil er bisher als schweizerische Spezialität auch die Weitergabe von Persönlichkeitsprofilen erfasste. Das fällt nun weg, weil der Begriff der Persönlichkeitsprofile ersatzlos aufgegeben wurde. Dass der Begriff indirekt wieder über das Profiling mit hohem Risiko eingeführt wurde, ändert nichts daran. Hier geht das revidierte DSG also weniger weit als das bisherige.

b) Personendaten dürfen **nicht gegen den ausdrücklichen Willen** der betroffenen Person bearbeitet werden. Dies ist ein besonders zentraler Grundsatz im Schweizer Datenschutzrecht, denn anders als unter der DSGVO, verlangt auch das neue DSG keinen Rechtsgrund für die Bearbeitung von Personendaten, sondern setzt auf das **«Opt-out»-Prinzip**: Wenn die betroffene Person eine Datenbearbeitung nicht will, muss sie ihr ganz oder teilweise widersprechen. Einen Grund braucht sie dafür nicht; ein solcher spielt erst auf der Ebene der Rechtfertigung (dazu N 40 ff.) eine Rolle. Dies bedeutet umgekehrt, dass wenn eine private Person (also keine Behörde) Personendaten zu einem bestimmten Zweck bearbeiten will und die Bearbeitungsgrundsätze einhält, sie das darf, solange die betroffene Person nicht widerspricht. Eine Einwilligung braucht es *nicht*, nicht einmal bei besonders schützenswerten Personendaten, obwohl der EDÖB teilweise das Gegenteil vertreten hat. Denn nur die *Bekanntgabe* an Dritte erfordert eine Rechtfertigung, nicht schon die Bearbeitung. Das «Opt-out»-Prinzip gilt selbst für das Profiling; jedenfalls solange es verhältnismässig ist und es insbesondere der betroffenen Person zugemutet werden kann. Wie weit der betroffenen Person ein Profiling ihrer Daten zugemutet werden kann, darüber scheiden sich die Geister. Handelt es sich um ein Profiling ohne hohes Risiko, wird normalerweise keine Rechtfertigung nötig sein. Art. 30 Abs. 2 Bst. b revDSG ist auch die Schweizer Implementation des **«Rechts auf Vergessen»**: Die betroffene Person kann sich gegen jeden Aspekt einer Datenbearbeitung aussprechen, auch gegen die weitere Aufbewahrung ihrer Daten. Sie kann damit – indirekt – die Löschung ihrer Daten verlangen (vgl. auch N 138). Mit diesem Argument wurde im Parlament letztlich auch das vorgeschlagene spezielle Widerspruchsrecht gegen das Profiling mit hohem Risiko abgelehnt: Das «Opt-out»-Prinzip erlaubt einer betroffenen Person bereits, sich gegen ein solches Profiling auszusprechen. Viele Unternehmen erlauben es ihren Kunden heute schon ausdrücklich, sich gegen eine Profilbildung für Marketingzwecke auszusprechen. Dies dürfte in den nächsten Jahren Standard werden.

[39] Werden diese beiden Grundsätze in Art. 30 revDSG oder die Bearbeitungsgrundsätze in Art. 6 und 8 revDSG durch einen privaten Datenbearbeiter verletzt, so ist damit gemäss Art. 30 Abs. 2 revDSG – wie schon bisher – die **Persönlichkeit der betroffenen Person *per se* verletzt** und die Datenbearbeitung unzulässig, sofern kein Rechtfertigungsgrund vorliegt. Für Bundesorgane gilt dies nicht; dort kommt nicht das System der Rechtfertigung zur Anwendung, sondern der Grundsatz der Gesetzmässigkeit. Wer als Bundesorgan Personendaten bearbeiten will, muss sich nicht nur an die Bearbeitungsgrundsätze halten, soweit das Gesetz nichts anderes vorsieht. Er braucht darüber hinaus normalerweise auch eine gesetzliche Grundlage (Art. 32 Abs. 1 revDSG), die in gewissen Fällen – wie etwa dem Profiling oder der Bearbeitung von besonders schützenswerten Personendaten – sogar in einem formellen Gesetz festgehalten sein muss (Art. 34 Abs. 2 revDSG). Nur ausnahmsweise geht es ohne eine solche, zum Beispiel im Einzelfall mit einer Einwilligung oder bei öffentlich zugänglichen Daten (Art. 34 Abs. 4 revDSG).

3. Rechtfertigungsgründe

[40] Die Rechtfertigungsgründe, auf die sich ein privater Datenbearbeiter berufen kann, sind grösstenteils unverändert geblieben. Wie bisher kommen eine Einwilligung, eine Grundlage im Schweizer Recht und ein überwiegendes privates oder öffentliches Interesse in Frage (Art. 31 Abs. 1 revDSG), wobei in der Praxis das **überwiegende private Interesse** die meisten Fragen aufwirft. Darum sind in Art. 31 Abs. 2 revDSG einige Beispiele aufgeführt, in denen normalerweise von einem überwiegenden privaten Interesse des Verantwortlichen auszugehen ist. Diese Liste ist aber nicht abschliessend und sie ist nicht identisch mit den Fällen in Art. 17 revDSG zur Rechtfertigung von Datenexporten in Länder ohne angemessenen Datenschutz. Die in Art. 17 revDSG aufgeführten Fälle geben immerhin weitere Indizien, in welchen Fällen ein überwiegendes Interesse (ebenfalls) vorliegen kann[42]. Schon aus der Liste in Art. 31 revDSG wird klar, dass auch wirtschaftliche Interessen angeführt werden können, was die Rechtsprechung bereits vor Jahren bestätigt hat. Zudem können für die Behauptung des überwiegenden privaten Interesses die Interessen *jeder Person* an der Bearbeitung angeführt werden.

[41] Die Interessen an der Bearbeitung werden im Rahmen einer Abwägung den Datenschutzinteressen der betroffenen Person *gegen* die Datenbearbeitung gegenübergestellt, d.h. dem Interesse, dass die Datenbearbeitung aufgrund ihrer Konsequenzen für die betroffene Person nicht in der vorgesehenen Weise stattfindet. An diesem Punkt kann es wichtig werden, warum eine betroffene Person der Datenbearbeitung widerspricht und ihre Daten beispielsweise gelöscht haben möchte. Die Abwägung der Interessen bedeutet letztlich oftmals, dass nach einem **datenschutzverträglichen Kompromiss** gesucht wird. Ein Löschanspruch ist daher nie absolut, auch wenn es Fälle gibt, in denen es kaum Gründe gegen eine Löschung geben wird (z.B. bei gewissen Verwendungen von Daten für Marketingzwecke). Zwar gibt es Rechtsprechung dazu, dass ein überwiegen-

42 Dies kann in der Praxis z.B. bei ausländischen Gerichts- und Verwaltungsverfahren von Relevanz sein, weil in diesen Fällen sehr häufig Personendaten bekanntgegeben werden müssen, ohne dass die betroffene Person vorgängig informiert worden ist. Die Bekanntgabe der Daten kann aber anerkanntermassen einem überwiegenden Interesse des Verantwortlichen entsprechen, wenn Massnahmen zum Schutz der betroffenen Personen getroffen wurden (vgl. Art. 17 Abs. 1 Bst. c Ziff. 2 revDSG). Ein weiteres, analog anwendbares Beispiel aus Art. 17 revDSG ist die Rechtfertigung der Bearbeitung von Daten zur Abwicklung eines Vertrags, in welchem nicht die Daten des Vertragspartners bearbeitet werden müssen, sondern solcher einer weiteren Person, in deren Interesse die Vertragsabwicklung ist (z.B. Empfänger eines Geschenks) und genau genommen von Art. 31 Abs. 2 Bst. a revDSG nicht erfasst ist, während in Art. 17 Abs. 1 Bst. b revDSG dieser Fall abgedeckt ist.

des privates Interesse nicht leichtfertig angenommen werden soll, doch die Rechtsprechung zeigt ebenso, dass Interessenabwägungen auch von Richtern in der Regel reine Bauchentscheide über «Gut und Böse» im Einzelfall sind. Konzeptionell hat eine Interessenabwägung ohne prinzipielle Überbeachtung der Interessen der betroffenen Person zu erfolgen, denn keine der Auslegungsmethoden rechtfertigt einen solchen «bias».

[42] Bei den exemplarischen Rechtfertigungsgründen in Art. 31 Abs. 2 revDSG gab es vier Änderungen:

> a) Die wichtigste Änderung betrifft den Rechtfertigungsgrund der **nicht personenbezogenen Datenbearbeitung** (Bst. e). Es geht um Fälle, in welchen zwar Personendaten bearbeitet werden, es aber nicht um die einzelne betroffene Person geht. Folglich geht es um eine Bearbeitung von Personendaten zu einem nicht personenbezogenen Zweck. Statistische Zwecke sind ein klassisches Beispiel. In den Beratungen spielte klinische Forschung mit Patientendaten häufig eine Rolle; für die Anpassungen der Bestimmung gegenüber dem Bundesratsentwurf machte sich insbesondere die Pharmabranche stark. Dies war insofern müssig, als dass im Bereich der Humanforschung und – speziell für die Sekundärnutzung von Gesundheitsdaten – das Humanforschungsgesetz (HFG)[43] dem DSG als *lex specialis* vorgeht.
>
> Bearbeitungen mit nicht personenbezogenen Zwecken können nach der Regelung von Art. 31 Abs. 2 Bst. e revDSG auch ohne Einwilligung gerechtfertigt sein, wenn sichergestellt ist, dass die Personendaten entweder *so rasch wie möglich* anonymisiert werden oder aber anderweitig sichergestellt ist, dass die Bestimmbarkeit der Personen verhindert wird. Dies kann beispielsweise dadurch erreicht werden, dass nur einem beschränkten Kreis zugängliche Codes statt Klarnamen eingesetzt werden (Pseudonymisierung). Dieses Erfordernis der Unkenntlichkeit der Identität der Person hinter den Daten ist gegenüber der heutigen Rechtslage neu, da gegenwärtig eine Bearbeitung zu nicht personenbezogenen Zwecken in der Regel noch gerechtfertigt ist, solange die Daten höchstens anonym publiziert werden. Neu ist auch das zweite Erfordernis, dass *besonders schützenswerte Personendaten* Dritten nur bekanntgegeben werden dürfen, wenn die Daten *vorher* anonymisiert oder pseudonymisiert wurden. Weil das aber nicht immer möglich ist (z.B., weil Forschungspartner als eigenständige Verantwortliche und damit als Dritte gelten), genügt es auch, die Dritten dazu zu verpflichten dafür zu sorgen, dass die Daten nicht für personenbezogene Zwecke bearbeitet werden. Das dritte Erfordernis schliesslich ist nicht neu: In den veröffentlichten Ergebnissen der Bearbeitung dürfen keine Personendaten mehr enthalten sein; die publizierte Forschungsarbeit darf also keine Daten enthalten, anhand derer die einzelnen Personen identifiziert werden könnten. Soll dies geschehen, braucht es normalerweise deren Zustimmung. Dieser Rechtfertigungsgrund ist vor allem für Zweitnutzungen von Personendaten wichtig, solange die Personendaten nicht im Hinblick auf die einzelne betroffene Person bearbeitet werden. Wenn also ein Unternehmen herausfinden will, warum seine Kunden welche Produkte kaufen, greift dieser Rechtfertigungsgrund.

43 Bundesgesetz über die Forschung am Menschen (Humanforschungsgesetz, HFG) vom 30. September 2011, SR 810.30.

Will es spezifisch jene Kunden ansprechen, die geneigt sein könnten, bestimmte Produkte zu kaufen, greift er nicht.

b) Am meisten zu diskutieren gab der Rechtfertigungsgrund der Bearbeitung zur **Prüfung der Kreditwürdigkeit** (Bst. c), weil hier drei neue Einschränkungen eingeführt wurden, damit der Rechtfertigungsgrund greift: *Erstens* dürfen nur noch Daten von volljährigen Personen bearbeitet werden, d.h. Kreditauskunfteien dürfen in ihren Datenbanken Minderjährige neu nicht mehr als solche identifizieren. *Zweitens* dürfen die Daten, welche den Kreditwürdigkeitsberichten der Auskunfteien zugrunde liegen, nicht mehr älter als zehn Jahre sein. Bisher gab es keine feste Grenze, sondern es galt (richtigerweise) nur der Grundsatz der Verhältnismässigkeit, der eine unterschiedliche Maximaldauer je nach Art der Information zuliess[44]. Auf den zweiten Blick ist die Tragweite der neuen Einschränkung geringer als sie erscheinen mag. Die zeitliche Schranke bezieht sich nur auf Tatsachen, die mehr als zehn Jahre zurückliegen. Der Umstand, dass eine Person im VR einer Gesellschaft sitzt oder gegen diese noch immer ein unverjährter Verlustschein vorliegt, ist aktuell, auch wenn die Person diese Position seit 30 Jahren innehat oder der Verlustschein schon vor 15 Jahren ausgestellt worden ist. Die Information, dass eine Person Konkurs gemacht hatte, darf jedoch nach zehn Jahren nicht mehr bearbeitet werden; bisher wurde diese Information bis zu 20 Jahre lang aufbewahrt. Die Kreditauskunftei wird zudem bei ihr verzeichnete Bonitätsfaktoren nach spätestens zehn Jahren darauf überprüfen müssen, ob sie (wie im Beispiel des Verlustscheins oder der VR-Position) noch bestehen. *Drittens* dürfen den Kreditwürdigkeitsberichten keine Profilings mit hohem Risiko oder besonders schützenswerte Personendaten zugrunde liegen – die Erstellung der Berichte selbst darf ein Profiling sein, d.h. es ist weiterhin möglich, dass sie je nach Datenlage betreffend eine Person z.B. eine grüne, gelbe oder rote Ampel anzeigen. Die *vierte* Anforderung, dass solche Kreditwürdigkeitsberichte nur solchen Personen zugänglich sein dürfen, die mit der betroffenen Person einen Vertrag abschliessen wollen oder einen Vertrag mit ihr abwickeln, ändert sich nicht. Sie galt schon bisher.

Zwei weitere Punkte werden in der Praxis oft übersehen: Der Rechtfertigungsgrund ist nur für jenen Verantwortlichen relevant, der Bonitätsinformationen für Dritte bearbeitet, d.h. für Kreditauskunfteien und dergleichen. Deren Kunden (d.h. jene Unternehmen, die die Auskunft nutzen, um darüber zu entscheiden, ob sie einem Konsumenten Kredit gewähren oder nicht) werden nicht eingeschränkt, denn sie können sich auf den Rechtfertigungsgrund des Vertragsabschlusses berufen (Art. 31 Abs. 2 Bst. a revDSG). Weiter kommt der Rechtfertigungsgrund nur und erst dann zum Zug, wenn eine Persönlichkeitsverletzung vorliegt. Es kann mit guten Gründen vertreten werden, dass dies bei gegebener Transparenz erst dann der Fall ist, wenn eine von einer Kreditauskunftei verzeichnete Person der Bearbeitung ihrer Personendaten widerspricht. Das gilt erst recht, wenn die betroffene Person die Daten öffentlich zugänglich gemacht hat, weil dann Art. 30 Abs. 3 revDSG greift. Bis zu einem solchen Widerspruch können nach dieser Argumentation auch über zehn Jahre alte Daten bearbeitet

44 Vgl. hierzu die «Verhaltensregeln» der IG Wirtschaftsauskunfteien, Stand 21. April 2020 (https://bit.ly/3juFcyn [Stand 9. Oktober 2020]).

werden, solange dies verhältnismässig ist und die betroffene Person nicht protestiert hat. Eine Kreditauskunftei muss also eine Person nicht einfach aus ihrer Datenbank löschen, wenn sie seit zehn Jahren nichts von ihr gehört hat.

c) Eine dritte Änderung betrifft die Ergänzung des Rechtfertigungsgrunds der Bearbeitung von **Personendaten von Konkurrenten** (Bst. b), dem nun auch der Datenaustausch im Konzern nicht mehr entgegensteht. Da aber die Daten juristischer Personen ohnehin nicht mehr vom DSG erfasst sind, spielt diese Anpassung keine grosse Rolle in der Praxis.

d) Eine Präzisierung gab es schliesslich beim **Rechtfertigungsgrund der Medien** (Bst. d), wonach nicht nur dann von einem überwiegenden privaten Interesse auszugehen ist, wenn Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines Mediums bearbeitet werden, sondern auch dann, wenn Daten nicht publiziert werden und lediglich als persönliches Arbeitsinstrument dienen; damit wird klargestellt, dass auch Hintergrundrecherchen oder nicht publizierte Daten (z.B. von weiteren Personen, die aber in einem Beitrag nicht erwähnt werden) gedeckt sind – selbst wenn sie in der Redaktion geteilt werden (und daher nicht unter die Ausnahme für den persönlichen Bereich nach Art. 2 Abs. 2 Bst. a revDSG fallen).

E. Massnahmen zur Sicherstellung des Datenschutzes

1. Privacy by Design

[43] In Art. 7 revDSG sind neu die beiden Schlagworte «Privacy by Design» und «Privacy by Default» geregelt, wobei Letzteres in Ersterem enthalten ist. Die zugrundeliegende Theorie leuchtet ein: Alle Datenschutzprobleme wären gelöst, wenn die zur Bearbeitung von Personendaten genutzten Systeme technisch **von Anfang an so ausgestaltet wären, dass der Datenschutz eingehalten werden muss**. Wer dies praktisch umsetzen will, merkt allerdings rasch, dass dies unrealistisch ist, weil die Anforderungen viel zu komplex und mannigfaltig sind. Wird «Privacy by Design» auf das heruntergebrochen, was realistisch ist, so ist letztlich alter Wein in neuen Schläuchen. Datenbearbeiter sind zum Selben verpflichtet wie bisher: Rechtzeitig entsprechende Vorkehrungen zur Einhaltung des Datenschutzes zu treffen, sei es in technischer oder in organisatorischer Hinsicht. Ausser dem Konzept des «Privacy by Default» in Abs. 3 (dazu N 38 ff.), erlegt Art. 7 revDSG den Datenbearbeitern keine neuen Pflichten auf. Bisher war diese Pflicht in Art. 7 DSG enthalten, der neu zu Art. 8 revDSG mutiert ist und sich nur noch auf die Datensicherheit im engeren Sinn beschränkt. Art. 7 revDSG wiederum ist kein Bearbeitungsgrundsatz mehr (er ist nicht in Art. 30 Abs. 2 Bst. a revDSG erwähnt), d.h. das Fehlen von Massnahmen führt nicht mehr – wie bisher – zwingend zu einer Persönlichkeitsverletzung. Eine Verletzung von Art. 7 revDSG kann als gesetzliche Vorgabe an die Sorgfaltspflicht immerhin eine ähnliche Wirkung wie eine milde Kausalhaftung haben, wenn nicht die erforderlichen Massnahmen zur Vermeidung von Persönlichkeitsverletzungen getroffen wurden. Ansonsten kann die Verletzung des Konzepts des «Privacy by Design» nicht sanktioniert werden, ausser indem der EDÖB im konkreten Einzelfall gegen einen Verantwortlichen vorgeht und ihm eine Anordnung erteilt.

[44] Welche **Massnahmen** der Verantwortliche treffen will, ist ihm überlassen. In einem *ersten Schritt* wird er bezüglich der Datenbearbeitung alle wesentlichen datenschutzrechtlichen Parameter der Bearbeitung definieren müssen. In einem *zweiten Schritt* wird er überlegen müssen,

wie er sicherstellen kann, dass die Bearbeitung wie von ihm vorgesehen stattfindet und alle Datenschutzvorschriften eingehalten werden. Die Mittel dazu sind beispielsweise Datenschutzerklärungen, interne Weisungen, die Schaffung von Widerspruchsmöglichkeiten, Self-Service-Angebote für Betroffenenrechte, der Einsatz von Verschlüsselungen, interne Prozesse zur Beschränkung von Nutzungszwecken, Vermeidung von Personendaten beim Applikationsdesign, Automatisierung von Löschungen, Verbote der Re-Identifikation, Zuständigkeitsregeln, dokumentierte Prozesse, Auswertung von Fehlerraten zwecks Qualitätssicherung, Vermeidung von nicht synchronisierten Datenkopien und die Regelungen der Aufbewahrungsdauer von Daten. Auch die nach Art. 26 DSGVO vorgeschriebene Vereinbarung zwischen gemeinsamen Verantwortlichen kann eine nach Art. 7 Abs. 1 und 2 revDSG angezeigte Massnahme sein. In einem *dritten Schritt* wird der Verantwortliche diese Massnahmen umsetzen müssen.

[45] Anders als in der ursprünglichen Konzeption des «Privacy by Design» geht es nicht mehr nur um die Ausgestaltung von Computern, sondern um **alles, was die Datenbearbeitung tangiert** (Abläufe, Zuständigkeiten, weitere Ressourcen, etc.). Verlangt werden nur angemessene Massnahmen, die jedoch dem «Stand der Technik» entsprechen müssen, also dem, was sich in der Praxis als wirksam erwiesen hat. Die Absicherung der «Compliance» muss (logischerweise) ab der Planung durchgängig bis zum Ende der Datenbearbeitung erfolgen, aber anders als unter der DSGVO ist der Verantwortliche nach Art. 7 Abs. 1 und 2 revDSG nicht verpflichtet, seine Tätigkeit zu dokumentieren. Auf ein Pendant zum **Prinzip der Rechenschaft** («accountability») in Art. 5 Abs. 2 DSGVO wurde – anders als noch im Vorentwurf – bewusst verzichtet.

[46] Mit den **«Datenschutzvorschriften»** sind alle Vorschriften gemeint, die den Schutz personenbezogener Daten im Rahmen einer konkreten Datenbearbeitung sicherstellen (z.B. Bearbeitungsgrundsätze, Vorgaben an Auftragsbearbeitung, Regeln zur Bekanntgabe von Personendaten ins Ausland, aber auch das Auskunftsrecht, das Recht auf Datenherausgabe und das Widerspruchsrecht). Nicht gemeint sind die Verzeichnispflicht, die Pflicht zur Meldung von Verletzungen der Datensicherheit und die Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen.

2. Privacy by Default

[47] Die Pflicht zur «Privacy by Default» ist im DSG neu. Ihre Tragweite ist allerdings beschränkt. Sieht ein Verantwortlicher in einem Service, einer Software oder einem Gerät mehrere Möglichkeiten vor, wie Personendaten bearbeitet werden können und kann der Benutzer diese Möglichkeiten über (Datenschutz-)Einstellungen selbst anpassen, so muss die **Standardeinstellung die am wenigsten weitgehende Einstellung** vorsehen. Wo ein Verantwortlicher dem Benutzer keine (technische) Wahlmöglichkeiten zur Eigensteuerung der Datenbearbeitung anbietet, kann es bereits begriffslogisch auch keine *Vor*einstellungen vornehmen und die Pflicht greift nicht.

[48] Der Umstand, dass eine Datenbearbeitung auf der Basis einer Einwilligung durchgeführt wird, führt ebenso wenig zu einer Voreinstellung, wie der Fall, in welchem einer betroffenen Person ein Widerspruchsrecht eingeräumt wird, selbst wenn ein solches in einem Online-Dienst über eine technische Funktion ausgeübt werden kann («Opt-out»-Knopf). Die Pflicht schreibt einem Verantwortlichen auch nicht vor, dass er den Benutzern (beispielsweise seines Online-Dienstes oder Geräts) **Wahlmöglichkeiten** anbieten muss. Wenn er dies aber tut, dann muss eine allfällige Voreinstellung so gesetzt sein, dass sie die Bearbeitung auf das «für den Verwendungszweck nötige Mindestmass» beschränkt.

[49] Mit **«Verwendungszweck»** ist die *Gesamtheit* der Zwecke aller Datenbearbeitungen gemeint, die der Verantwortliche vornehmen oder anbieten will. Nur so macht die Norm überhaupt Sinn. Mit «Mindestmass» ist der geringste Eingriff in die Persönlichkeit gemeint, und nicht nur jene Bearbeitung, in deren Rahmen volumenmässig am wenigsten Daten bearbeitet werden, wie es die Botschaft vertritt[45]. Welches Mindestmass der Verantwortliche anbieten will, ist wiederum ihm überlassen. Dass der geringste Eingriff in die Persönlichkeit voreinzustellen ist, bezieht sich nur auf die Persönlichkeit der Person, welche die Einstellungen vornehmen kann, nicht auf etwaige andere Betroffene.

[50] Die Pflicht zum «Privacy by Default» verbietet auch nicht, dass das Kästchen einer Online-Einwilligungserklärung bereits vorangekreuzt ist. Dies ist im revidierten DSG – anders als unter der DSGVO – grundsätzlich weiterhin zulässig. Die Pflicht zur datenschutzfreundlichen Voreinstellung gilt zudem dann **nicht, wenn der Benutzer «etwas anderes bestimmt»** hat (Art. 7 Abs. 3 a.E. revDSG). Wird er etwa im Rahmen der Registrierung in einem Online-Dienst vor die Wahl gestellt, welche Einstellung er möchte, dürfen ihm auch solche Einstellungen vorgeschlagen werden, die nicht dem Mindestmass entsprechen, d.h. entsprechende Optionen können standardmässig angewählt sein. Kann er die Einstellungen hingegen überspringen ohne eine Wahl getroffen zu haben, so muss die Standardeinstellung dem Mindestmass entsprechen.

[51] Art. 7 Abs. 3 revDSG enthält ferner **kein Koppelungsverbot** (dazu auch N 30): Der Verantwortliche kann bestimmen, dass eine bestimmte Datenbearbeitung nur gewählt werden kann, wenn zugleich auch andere Datenbearbeitungen zugelassen werden. Eingeschränkt wird dies höchstens durch die Grundsätze der Verhältnismässigkeit oder der Freiwilligkeit der Einwilligung. In diesem Sinne ist das in der Botschaft zitierte Beispiel des Online-Shops, welcher dem Benutzer die Wahl lässt, auch ohne Anlegen eines Kundenprofils einzukaufen, falsch[46]: Es fehlt schlicht an der Voreinstellung.

[52] Direkte Rechtsfolgen hat eine Verletzung von Art. 7 Abs. 3 revDSG übrigens nicht. Die Durchsetzung liegt primär in der Hand des EDÖB.

3. Datensicherheit

[53] In Art. 8 revDSG wird im Sinne eines Bearbeitungsgrundsatzes verlangt, dass der Verantwortliche und – anders als im Falle von Art. 7 revDSG – auch der Auftragsbearbeiter mit **technischen und organisatorischen Massnahmen** für angemessene Datensicherheit sorgen. Anders als im bisherigen Recht deckt diese Bestimmung nur noch die Datensicherheit ab, d.h. den Schutz von Personendaten bezüglich ihrer Vertraulichkeit, Integrität und Verfügbarkeit. Vorkehrungen zur Verhinderung anderer Datenschutzverletzungen fallen unter Art. 7 Abs. 1 und 2 revDSG. Ändern tut sich damit gegenüber dem heutigen Recht (und auch gegenüber der DSGVO) mit Bezug auf die Anforderungen an die Datensicherheit nichts.

[54] Typische Massnahmen zur Erreichung angemessener Datensicherheit sind z.B. Zugriffsbeschränkungen, Zugangsbeschränkungen, Filter (z.B. Firewalls), Pseudonymisierung einschliesslich Datenverschlüsselung, Protokollierung, Backups, sichere Entsorgungstechniken, Bewachung, Alarmanlagen, aber auch Reglemente und Weisungen, Schulungen, die Wahl und Beauftragung

45 BBl 2017 7030.

46 BBl 2017 7030.

von Auftragsbearbeitern, Verträge, welche die Datenbearbeitung oder Geheimhaltung regeln, Dokumentation, Kontrollen, *Penetration Tests* und Zuständigkeitsregelungen.

[55] Das Gesetz schreibt keine bestimmten Massnahmen vor. Sie müssen auch **keinen absoluten Schutz** bieten, sondern bei objektivierter Betrachtung in einem vernünftigen Verhältnis zum Risiko einer Verletzung der Datensicherheit stehen (zum Begriff vgl. N 161). Kommt es zu einer Verletzung, sieht das neue Recht eine Meldepflicht vor (N 160 ff.). Eine spezielle Dokumentationspflicht sieht Art. 8 revDSG nicht vor, doch kann sie sich in grösseren Betrieben indirekt ergeben, weil sich die Datensicherheit ohne eine Dokumentation der Schutzmassnahmen möglicherweise nicht vernünftig gewährleisten lässt.

[56] Anders als im bisherigen Recht, kann die vorsätzliche Verletzung von Art. 8 revDSG auch strafrechtlich mit einer **Busse** von bis zu CHF 250'000 sanktioniert werden. Dies allerdings nur, wenn dabei die vom Bundesrat noch konkret zu definierenden «Mindestanforderungen» vorsätzlich missachtet werden (Art. 61 Bst. c revDSG). Es ist zu erwarten, dass solche Bussen nur dort zum Tragen kommen, wo ein Verantwortlicher oder Auftragsbearbeiter es an minimalster Datensicherheit missen lässt. Der Umstand, dass es trotz getroffener Massnahmen zu einer Verletzung der Datensicherheit kommt, ist nicht strafbegründend und muss auch keine Verletzung von Art. 8 revDSG sein – ein Restrisiko gibt es immer.

F. Auftragsbearbeitung

[57] Die «Auftragsbearbeitung» oder die «Auftragsdatenverarbeitung», wie sie in Deutschland heisst, kommt in der heutigen arbeitsteiligen Wirtschaft häufig vor. Im Kern geht es darum, dass ein Verantwortlicher die Durchführung einer *eigenen* Datenbearbeitung von einem Dritten *in seinem Auftrag* durchführen lässt. Dass nicht jeder Auftrag an einen Dritten, der auch die Bearbeitung von Personendaten beinhaltet, automatisch zur Auftragsbearbeitung wird, wurde bereits im Rahmen der Begriffe des «Verantwortlichen» und «Auftragsbearbeiters» erläutert (N 13 ff.). Eine Auftragsbearbeitung – zum Beispiel die Auslagerung von IT-Funktionen an einen Cloud-Provider oder die Durchführung eines Werbeversands – ist unter dem revidierten DSG weiterhin **grundsätzlich ohne Einwilligung der betroffenen Personen zulässig**. Die Anforderungen sind aber leicht verschärft worden.

[58] Die Auslagerung muss selbstverständlich die Bearbeitungsgrundsätze einhalten und namentlich verhältnismässig sein[47]. Auch die Bestimmungen über den Datenexport (N 64 ff.) müssen befolgt werden. Über eine Auftragsbearbeitung im geschäftsüblichen Rahmen muss hingegen **nicht informiert** werden. Eine Ausnahme erfolgt mit der Revision lediglich gemäss Art. 19 Abs. 2 Bst. c revDSG, wonach über etwaige Empfänger der Daten zu informieren ist. Dazu zählen auch Auftragsbearbeiter[48]. Dasselbe gilt im Auskunftsrecht. Die Auftragsbearbeiter müssen aber grundsätzlich nicht namentlich genannt werden. Sind die Voraussetzungen einer Auftragsbearbeitung erfüllt, so wird der Auftragsbearbeiter dem Verantwortlichen datenschutzrechtlich zugerechnet – es liegt keine Bekanntgabe an einen «Dritten» und keine Zweckänderung vor. Der Auftragsbearbeiter kann sich zudem auf etwaige Rechtfertigungsgründe des Verantwortli-

47 In gewissen Fällen wird eine Auslagerung sogar geboten sein, wenn dadurch etwa das nötige Mass an IT-Sicherheit gewährleistet werden kann, wenn dem Verantwortlichen das Fachwissen dazu fehlt.

48 BBl 2017 7051.

chen berufen. Die eigenen Mitarbeiter (einschliesslich der im Betrieb integrierten, unter Weisung und Aufsicht des Verantwortlichen handelnden Dritten wie z.B. Berater) sind technisch keine Auftragsbearbeiter, allerdings gelten die Regeln für Auftragsbearbeiter für sie analog; in der DSGVO sind sie in Art. 29 separat geregelt. Bearbeitet ein Auftragsbearbeiter die Daten des Kunden (auch) **für eigene Zwecke**, wird er zum Verantwortlichen; das kann, wenn richtig aufgesetzt, datenschutzrechtlich zulässig sein.

[59] Die **Voraussetzungen** für eine Auftragsbearbeitung haben sich im revidierten DSG grundsätzlich nicht verändert, allerdings ist eine Anforderung hinzugekommen (N 60). Sie sind in Art. 9 revDSG geregelt. Im Wesentlichen muss der Verantwortliche – typischerweise mittels Vertrag sowie sorgfältiger Auswahl, Instruktion und Kontrolle – sicherstellen, dass der Auftragsbearbeiter nur die von ihm (datenschutzkonform) definierte Datenbearbeitung durchführt und der Verantwortliche seinen Pflichten nach DSG nachkommen kann. Beides wird mittels eines Weisungs- und Kontrollrechts umgesetzt, letzteres überdies mit vertraglichen Unterstützungspflichten. Anders als Art. 28 Abs. 3 DSGVO schreibt Art. 9 revDSG die Regelungspunkte für den Vertrag nicht vor. Unter dem Schweizer Recht wird ein Verantwortlicher sich an den DSGVO-Vorgaben orientieren, um seinen Pflichten nachkommen zu können. Art. 9 revDSG lässt ihm jedoch mehr Freiheit, *wie* er dies sicherstellt (z.B. die Erfüllung von Betroffenenrechten oder die Datenrückgabe am Ende des Auftrags). Gewissen Pflichten, wie etwa der Pflicht zur Datensicherheit nach Art. 8 revDSG (und damit auch zur Geheimhaltung) und der Pflicht zur Meldung von Verletzungen der Datensicherheit (Art. 24 revDSG) unterliegt der Auftragsbearbeiter zwar direkt. Befindet sich der Auftragsbearbeiter im Ausland, ist eine vertragliche Regelung aus Gründen der Durchsetzbarkeit trotzdem oft erforderlich. Der Abschluss von solchen «Auftragsdatenverarbeitungsverträgen» oder kurz «ADVs» mit den gemäss Art. 28 Abs. 3 DSGVO geforderten Punkten ist mittlerweile Standard; diskutiert wird vor allem darüber, wer die Kosten zu tragen hat und wie weit Eingriffe möglich sind bzw. wie weit Weisungen gehen dürfen. Provider standardisierter Cloud-Dienstleistungen lassen z.B. häufig keine Kundenaudits vor Ort zu, sondern verweisen auf in ihrem Auftrag von unabhängigen Prüfgesellschaften durchgeführte Sammelaudits mit entsprechenden Testaten, Zertifikaten oder Prüfberichten. Auch das Weisungsrecht wird «pauschaliert», indem die im Vertrag vereinbarten Vorgaben und die vom Kunden im betreffenden Online-Dienst vorgenommenen Einstellungen und Nutzungen zu den «einzigen und finalen» vom Kunden erteilten Weisungen deklariert werden; andere Weisungen sind nicht möglich. Genügt dies dem Kunden nicht, muss er den Vertrag kündigen. Unter dem DSG sind solche Abmachungen situationsabhängig zulässig und bleiben es. Weiterhin zulässig und durchaus auch üblich ist – wie unter der DSGVO – eine Begrenzung der Haftung des Auftragsbearbeiters. Nicht zulässig ist hingegen eine Verpflichtung des Auftragsbearbeiters zur Übernahme von Bussen gemäss DSG, da diese persönlicher Natur sind und sonst ihr Zweck vereitelt würde (N 191).

[60] Neu ist die Regelung von Art. 9 Abs. 3 revDSG, wonach der Beizug weiterer Auftragsbearbeiter durch den Auftragsbearbeiter (**«Unterauftragsbearbeiter»** oder «sub-processors») nur mit Genehmigung des Verantwortlichen zulässig ist. Die Bestimmung entspricht inhaltlich Art. 28 Abs. 2 DSGVO; eine analoge, wenn auch leicht abgeschwächte Regelung sieht die FINMA in ihrem Outsourcing-Rundschreiben vor[49]. Keine Unterauftragsbearbeitung liegt vor, wenn ein Auftragsbearbeiter Dritte beizieht, die ihrerseits nicht als Auftragsbearbeiter gelten (wie z.B. eigenes

[49] FINMA Rundschreiben 2018/3 zum Outsourcing bei Banken und Versicherer, Rz. 33.

Personal oder Berater)[50]. Genehmigung meint eine – im privaten Bereich formfreie – Zustimmung des Verantwortlichen im Einzelfall (d.h. der Dritte ist ihm namentlich bekannt) oder im Allgemeinen (d.h. die Dritten sind ihm nicht bekannt). In letzterem Fall muss der Verantwortliche vor dem jeweiligen Beizug über den Dritten namentlich (i.d.R. plus Land und Aufgabe) informiert werden und widersprechen können[51]. Eine solche «Genehmigung mit Widerspruchsvorbehalt» wird vor allem von Anbietern standardisierter Dienstleistungen (z.B. Cloud-Services) beansprucht, da eine Einzelgenehmigung für sie logistisch nicht sinnvoll durchführbar wäre. Die Ankündigungsfrist ist nicht definiert; in der Praxis liegt sie zwischen sieben Tagen bis sechs Monaten. Auch wenn Widersprüche normalerweise nicht vorkommen, muss die Frist genügend Zeit zur Beurteilung des Beizugs lassen und ein Widerspruch muss vom Verantwortlichen realistischerweise ausgeübt werden können. Bei standardisierten Dienstleistungen besteht das Widerspruchsrecht typischerweise in Form eines ausserordentlichen Kündigungsrechts. Die Information kann über eine auf der Website publizierten Liste der Unterauftragsbearbeiter mit automatischer Benachrichtigung im Falle von Änderungen erfolgen. Korrekterweise muss auch über weitere Delegationen in der Kette informiert werden (d.h. wenn der beigezogene Dritte seinerseits Dritte beizieht), was in der Praxis häufig missachtet wird. Die Regelung von Art. 9 Abs. 3 revDSG gilt auch beim Beizug von Unterauftragsbearbeitern im eigenen Konzern. Ein Recht zur nachträglichen Abberufung eines Unterauftragsbearbeiters verlangt Art. 9 Abs. 3 revDSG hingegen nicht. Die Bestimmung ist von ihrer Rechtsnatur her ein öffentlich-rechtliches Verbot; eine Verletzung führt zwar nicht direkt, über Art. 6 Abs. 1 revDSG aber indirekt zur Persönlichkeitsverletzung. Aus Art. 9 Abs. 1 und 2 revDSG (und nicht Abs. 3) ergibt sich, dass der Verantwortliche dafür sorgen muss, dass die Vorgaben von Abs. 1 und 2 über die gesamte Kette der Auftragsbearbeitung erfüllt bleiben. Das war schon bisher so und ändert sich nicht. Direkte Weisungs- und Kontrollrechte gegenüber dem Unterauftragsbearbeiter verlangt das revidierte DSG vom Verantwortlichen allerdings nicht (ebenso wenig tut dies die DSGVO).

[61] Neu wird die vorsätzliche Verletzung von Art. 9 Abs. 1 und 2 revDSG (nicht jedoch Abs. 3) seitens des Verantwortlichen mit einer **Busse** bis zu CHF 250'000 bestraft (Art. 61 Bst. b revDSG). Die verantwortlichen Personen haben also jedes Interesse den Auftragsbearbeiter entsprechend zur Einhaltung ihrer Vorgaben zu verpflichten. Die Auftragsbearbeiter haben jedenfalls aus dieser Regelung kein Strafbarkeitsrisiko, auch nicht im Falle einer Unterauftragsbearbeitung. Kein Strafbarkeitsrisiko besteht in den Fällen, in denen Art. 9 revDSG analog angewandt wird. Kommt es zu einer Persönlichkeitsverletzung, so sind Ansprüche gegen jeden möglich, der an ihr mitgewirkt hat. Das kann auch der Auftragsbearbeiter sein. Seitens des Verantwortlichen greift gegenüber der betroffenen Person typischerweise auch die Geschäftsherrenhaftung[52], die allerdings wie üblich eine Exkulpation zulässt; unter der DSGVO gilt Ähnliches[53]. Besteht zwischen dem Verantwortlichen und der betroffenen Person eine Vertragsbeziehung, kann auch eine Hilfspersonenhaftung in Frage kommen[54].

[62] In der Praxis werden Auftragsbearbeiter in der Schweiz häufig mit **ADVs nach Art. 28 DSGVO** konfrontiert. Sie können unter dem künftigen DSG weiterhin übernommen werden, je-

50 BBl 2017 7032.

51 BBl 2017 7032.

52 Art. 55 OR.

53 Art. 82 Abs. 2 und 3 DSGVO.

54 Art. 101 OR.

doch ist es nach wie vor erforderlich, diese an das DSG anzupassen: *Erstens* sind Verweise auf die DSGVO durch entsprechende Verweise auf das DSG (oder «anwendbare Datenschutzrecht») zu ergänzen, *zweitens* ist die Bekanntgabe ins Ausland so anzupassen, dass auch Exporte aus der Schweiz DSG-konform erfasst sind und *drittens* ist in internationalen Verhältnissen der Geltungsbereich so zu formulieren, dass alle Auftragsbearbeitungen nach DSG erfasst sind und nicht nur solche, die der DSGVO unterliegen.

[63] Keine Änderung bringt das revidierte DSG mit Bezug auf den Vorbehalt entgegenstehender **Geheimhaltungspflichten** von Art. 9 Abs. 1 Bst. b revDSG mit sich. Hier enthält der ausführliche Aufsatz des Autors dieses Beitrags weitergehende Hinweise[55].

G. Datenexporte

1. Allgemeines Regelungskonzept

[64] Die Bestimmungen zur **Bekanntgabe von Personendaten ins Ausland** ab Art. 16 revDSG gingen schlank durchs Parlament. Es kam zu einer Streichung im Bereich der Meldepflichten, und ganz generell ist die neue Regelung von Datenexporten gegenüber den bisherigen Bestimmungen etwas liberaler ausgefallen. Mussten Verträge für die grenzüberschreitende Bekanntgabe in unsichere Drittstaaten bisher pro forma dem EDÖB gemeldet werden, ist das neu normalerweise nicht mehr nötig.

[65] Vom Prinzip her ändert sich mit dem neuen DSG nicht viel. Neu liegt es nicht mehr am Datenexporteur zu beurteilen, ob ein Drittstaat ein angemessenes Datenschutzniveau bietet oder nicht. Dies wird stattdessen **vom Bundesrat autoritativ entschieden** – so wie das im EWR die Europäische Kommission tut[56]. Die Schweiz wartet derzeit selbst auf den Beschluss über ihre Angemessenheit durch die Europäische Kommission. Im Sinne eines autonomen Nachvollzugs von EU-Recht und um keine Hintertür für Datenexporte aus dem EWR zu schaffen, ist davon auszugehen, dass der Bundesrat nur solche Länder als angemessen anerkennen wird, die es auch nach Ansicht der Europäischen Kommission sind. Die kürzliche Streichung von *Privacy Shield* (N 74) als Grundlage zur Annahme der Angemessenheit der USA auf der bisher vom EDÖB geführten Länderliste erfolgte aus genau diesem Grund[57].

[66] Die Bestimmungen von Art. 16 f. revDSG spielen (weiterhin) nur dann eine Rolle, wenn aus der Schweiz heraus Personendaten an einen Empfänger im Ausland bekanntgegeben werden. Das «Bekanntgeben» erfordert begriffslogisch, dass der Kreis der Personen, die über die betreffende Information verfügen, erweitert wird. Wer also auf sein eigenes E-Mail-Postfach aus dem Ausland zugreift oder Daten auf dem Notebook auf einer Reise ins Ausland mitnimmt, gibt damit noch keine Personendaten bekannt. Das würde er erst dann tun, wenn er die Personendaten im Ausland jemandem zeigt. Als Bekanntgabe gilt dabei **auch der Fernzugriff**: Wer also einer Person die Personendaten auf einem Server in der Schweiz per Remote Access zur Verfügung stellt, gibt ihr

55 David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020.

56 Der Bundesrat wird vermutlich die Länderliste des EDÖB übernehmen: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html (Stand 9. Oktober 2020).

57 EDÖB: Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG, 8. September 2020.

damit Personendaten bekannt. Kraft spezieller gesetzlicher Regelung gilt immerhin die Online-Publikation von Personendaten nicht als Bekanntgeben, auch wenn die Daten vom Ausland her zugänglich sind (Art. 18 revDSG). Das war schon bisher so. Der Umstand, dass Personendaten innerhalb desselben Betriebs weitergegeben werden, schliesst eine Anwendung von Art. 16 ff. revDSG hingegen nicht aus. Wer also Personendaten aus der Schweiz seiner eigenen Zweigniederlassung im Ausland zugänglich macht, muss sich an Art. 16 f. revDSG halten.

[67] Mit seinem Konzept weicht das DSG (weiterhin) etwas von der DSGVO ab, welches nach herrschender Auffassung an die Übermittlung von Daten zwecks deren nachfolgende Verarbeitung in einem Drittland anknüpft, nicht nur an die grenzüberschreitende Bekanntgabe aus dem Inland. In den meisten Fällen spielt die Unterscheidung keine Rolle. Eine Rolle spielt sie dann, wenn Daten **im Ausland weiterübermittelt** werden: Art. 44 ff. DSGVO sind auch in diesen Fällen zu beachten, während Art. 16 revDSG nur an die Bekanntgabe *aus dem Territorium* der Schweiz heraus anknüpft. Wenn also ein Schweizer Unternehmen Personendaten in Deutschland erhebt und ohne Umweg über die Schweiz nach Indien übermittelt, greift Art. 16 revDSG jedenfalls nach dem bisherigen Verständnis nicht[58]. Wenn hingegen ein Schweizer Unternehmen in der Schweiz Daten bearbeitet und nach Indien übermittelt, findet die Parallelnorm in Art. 44 DSGVO auch dann Anwendung, wenn die Daten nie aus dem Territorium des EWR übermittelt worden sind – vorausgesetzt, die Datenbearbeitung unterliegt der DSGVO.

[68] Vom Grundsatz her läuft es daher weiterhin so, dass Personendaten ohne Weiteres in all jene Länder bekanntgegeben werden dürfen, die über einen **angemessenen gesetzlichen Datenschutz** verfügen – nunmehr gemäss der Liste des Bundesrates. Von den Angemessenheitsentscheiden der Europäischen Kommission wird es dort Abweichungen geben, wo das Datenschutzrecht eines Drittlands Daten von Personen aus dem EWR, nicht aber der Schweiz bevorzugt behandelt[59]. Die Länder des EWR bieten in jedem Fall ein angemessenes Schutzniveau, und Grossbritannien wird dies nach dem Vollzug des Brexit tun, da es das Datenschutzrecht der EU übernommen hat[60]. Als Minimalstandard, um als angemessen zu gelten, gelten – inoffiziell – die Vorgaben der revidierten Datenschutzkonvention 108 des Europarats.

[69] Ein Sonderfall war bis vor kurzem die USA: Auch sie galt als Land mit angemessenem Datenschutz, aber nur mit Bezug auf jene Unternehmen, die sich unter dem «Privacy Shield Framework» selbstzertifiziert hatten[61]. Dies haben beispielsweise die grossen US-Online-Anbieter wie Google, Amazon, Facebook und Microsoft getan. Die Selbstzertifizierung entspricht insofern einem gesetzlichen Datenschutz, als diese Unternehmen quasi ein öffentliches Versprechen abgeben, sich an die Grundsätze des europäischen Datenschutzes zu halten und darum im Falle eines Verstosses wegen Verletzung ihrer Zusage lauterkeitsrechtlich belangt werden können. Ob Datenbekanntgaben in Fällen analog dem Privacy Shield (sollte es sie überhaupt noch geben, N 74) inskünftig wie bisher als Fall von Art. 16 Abs. 1 revDSG gelten oder systematisch unter die Ausnahmeregelung nach Art. 16 Abs. 3 revDSG gefasst werden (N 67), wird der Bundesrat entscheiden müssen.

---

58 Wohl aber kann ein sog. *onward transfer* durch den erforderlichen Datenschutzvertrag oder durch lokales Datenschutzrecht (z.B. DSGVO) untersagt sein, weil es auch von Auftragsbearbeitern zu beachten ist.

59 So beispielsweise bisher im Falle von Japan.

60 Aus Sicht des EWR werden Datenexporte nach Grossbritannien allerdings formal einen Angemessenheitsbeschluss der Europäischen Kommission benötigen, der zum Zeitpunkt dieses Beitrags noch nicht vorlag.

61 Privacy Shield List, https://www.privacyshield.gov/list (Stand 9. Oktober 2020).

[70] In der Praxis ist bei der Übernahme von den Datenschutz betreffenden, für die DSGVO formulierten Vereinbarungen und Datenschutzerklärungen darauf zu achten, dass die Formulierungen so ausgeweitet werden, dass einerseits Exporte auch aus der Schweiz erfasst sind, und andererseits Regelungen auch für Daten aus der Schweiz gelten. Die DSGVO arbeitet mit dem Begriff des «Drittlands» und meint damit alle Staaten ausserhalb des EWR. Auch die Schweiz ist aus der Sicht des EWR ein Drittland. Aus Sicht der Schweiz sind wiederum alle anderen Staaten als die Schweiz Drittländer. Das ist im Rahmen von Datenschutzerklärungen schon deshalb zu berücksichtigen, weil nach Art. 19 Abs. 4 revDSG neu alle Länder (oder Regionen) aufgeführt werden müssen, in welche Personendaten aus der Schweiz exportiert werden.

2. Ausnahmeregelungen

[71] Verfügt ein Land nicht über ein angemessenes gesetzliches Datenschutzniveau, so war dies in der Praxis bisher kein Problem, solange mit den Empfängern der Daten ein passender Vertrag abgeschlossen werden konnte, mit welchem der Datenschutz vertraglich soweit wie erforderlich sichergestellt ist. Die in der Praxis hierzu am häufigsten verwendeten Verträge sind die **Standardklauseln der Europäischen Kommission**, die es für Auftragsbearbeiter wie auch für Verantwortliche als Empfänger gibt[62]. Sie können auch für Schweizer Verhältnisse verwendet werden. Eine Anpassung der Verweise auf das DSG und seine Definitionen ist sinnvoll, aber nicht zwingend, sofern aus den Anhängen klar genug hervorgeht, dass auch die Datentransfers aus der Schweiz erfasst sind. Solange diese Standardklauseln vom EDÖB anerkannt, ausgestellt oder genehmigt werden – was bei den Klauseln der Europäischen Kommission bisher der Fall war – muss weiter nichts unternommen werden. Unter dem revidierten DSG entfällt die bisherige Meldepflicht (Art. 16 Abs. 2 Bst. d revDSG). Dies entspricht den Regelungen unter der DSGVO.

[72] Die Standardklauseln genügen für die meisten Fälle, dürfen aber in ihren datenschutzrechtlich relevanten Aspekten nicht verändert werden. Passen sie nicht, gibt es zwei Alternativen: Entweder wird ein individueller Vertrag ausgearbeitet, der einen angemessenen Datenschutz vertraglich sicherstellt oder es wird mit ***Binding Corporate Rules*** (BCR) gearbeitet:

> a) Die erste Variante ist eine Schweizer Freiheit, welche die DSGVO so nicht kennt. Sie setzt weiterhin voraus, dass der Vertrag dem EDÖB mitgeteilt wird, damit er ihn sich anschauen und Stellung dazu nehmen kann. Eine formelle Genehmigung durch den EDÖB ist aber nicht nötig.
>
> b) BCR hingegen kennt auch die DSGVO. Gemeint sind konzerninterne Regelungen des Datenschutzes, so dass auch Konzerneinheiten in unsicheren Drittstaaten einen angemessenen Datenschutz sicherstellen. Diese Regelungen können umfassend sein oder sich auf bestimmte Bereiche beschränken. Normalerweise wird dazu ein Vertrag zwischen allen Konzerneinheiten abgeschlossen, welcher den Datenschutz – ähnlich den Standardvertragsklauseln – regelt. Der Vorteil der BCR liegt darin, dass sie einerseits Abweichungen von den vom EDÖB anerkannten Standardklauseln zulassen und andererseits generischer für eine Vielzahl von Datenbearbeitungen im Konzern

62 Diese sind unter https://bit.ly/3lt6Yvq abrufbar (Stand 9. Oktober 2020); in Kürze wird allerdings mit neuen Standardvertragsklauseln der Europäischen Kommission gerechnet.

abgefasst werden können (und nicht auf spezifische Datenbearbeitungen beschränkt sind, wie das im Falle der Standardklauseln typischerweise der Fall ist). BCR gibt es sowohl für Datentransfers unter Verantwortlichen als auch für Datentransfers unter Auftragsbearbeitern und Unterauftragsbearbeitern (sog. *Processor BCR*)[63]. BCR mussten bisher in der Schweiz dem EDÖB nur gemeldet werden und sind neu – analog der Regelung in Art. 47 DSGVO – genehmigungspflichtig (Art. 16 Abs. 2 Bst. e revDSG), wobei auch unter der DSGVO ergangene Genehmigungen anerkannt werden können. BCR haben in der Schweiz bisher allerdings eine sehr untergeordnete Rolle gespielt, weil sie relativ aufwändig sind und in vielen Fällen keine wirklichen Vorteile mit sich bringen. Viel einfacher sind oft konzernweite Datentransferverträge auf der Basis der EU-Standardvertragsklauseln. So oder so werden mit solchen konzernweiten Datenschutzverträgen regelmässig auch weitere Anforderungen des Datenschutzes, wie etwa die Regelung von Auftragsbearbeitungen und gemeinsamen Verantwortlichkeiten im Konzern, abgedeckt.

[73] Theoretisch kann der Datenschutz in unsicheren Drittstaaten auch auf andere Weise als durch eine vertragliche Absicherung sichergestellt sein; beispielsweise durch technische Beschränkungen oder aber durch **Selbstzertifizierungssysteme**, wie beim bereits erwähnten Privacy Shield[64]. Bisher gab es dazu keine Formvorschriften; neu setzt die Zulassung solcher anderer «Garantien» einen Entscheid des Bundesrats voraus (Art. 16 Abs. 3 revDSG). Die DSGVO sieht Ähnliches für Zertifizierungen vor, bietet aber viel weniger Flexibilität (Art. 46 Abs. 2 Bst. f DSGVO).

[74] War es bisher selbstverständlich, dass Datenexporte in unsichere Drittstaaten mit Verträgen hinreichend abgesichert werden konnten, ist dies seit dem EuGH-Entscheid **«Schrems II»** vom 16. Juli 2020[65] für manche Experten und Behördenvertreter nicht mehr so klar. Der EuGH erinnerte daran, dass Verträge alleine unter Umständen keinen hinreichenden Schutz bieten, weil ausländische Behörden sich nicht an diese halten müssen. Anlass war eine Bestimmung des US-Rechts, welche US-Geheimdiensten den Zugriff auf Personendaten aus dem Ausland auch ohne Gerichtsbeschluss erlaubt, was im Widerspruch zu den Verfassungsgarantien der EU steht. Vor diesem Hintergrund wurde die Anerkennung von Privacy Shield durch die Europäische Kommission aufgehoben. Beim Einsatz der Standardvertragsklauseln der Kommission (und bei BCR) wird jetzt im EWR gerätselt, in welchen Fällen weitere Massnahmen nötig sind, um Personendaten weiterhin legal in die USA bekanntgeben zu dürfen. Verlangt wird teilweise die Analyse des tatsächlichen Risikos eines Behördenzugriffs im Ausland, der intensivere Einsatz von Verschlüsselung, aber auch die Anpassung der Verträge oder die Verlagerung von Datenbearbeitungen von den USA zurück nach Europa. Die Diskussion ist derzeit noch im Gange, da sich auch die Datenschutzbehörden nicht im Klaren darüber sind, was zu tun ist. Es wird unter anderem erwartet, dass die Kommission in Kürze **neue Standardverträge** vorlegen wird. Die neue Schweizer Regelung von Art. 16 Abs. 2 revDSG lässt alle Möglichkeiten offen: Der Einsatz von Verträgen zur

63 Dies wird gerne von international tätigen Service Providern benutzt, die Verträge mit den Kunden über ihre lokalen Gesellschaften in Europa abschliessen. Die europäischen Gesellschaften transferieren die Kundendaten dann aber im Rahmen der Auftragsbearbeitung in die USA oder in andere unsichere Drittstaaten.

64 BBl 2017 7042.

65 Urteil des EuGH vom 16. Juli 2020, C-3111/18 («Schrems II»), Rz. 126 ff.

Absicherung von Datenexporten in unsichere Drittstaaten wird zwar als Methode vom Gesetzgeber anerkannt, aber der Export wird trotz allem nur erlaubt, wenn dadurch tatsächlich «ein geeigneter Datenschutz gewährleistet» wird. Der EDÖB kann also ohne Weiteres vertreten, dass in gewissen Fällen ein Vertrag oder BCR nicht genügen.

[75] Kommen weder ein Vertrag noch BCR in Frage, bleibt dem Datenexporteur nur übrig, mit einer der **anderen Ausnahmen** aus Art. 17 revDSG zu arbeiten. Auch diese Ausnahmen gab es grösstenteils schon bisher, aber der Katalog wurde im Hinblick auf die Angleichung an die DSGVO etwas ausgeweitet. Weiterhin vorgesehen ist die Ausnahme der Einwilligung, die neu ausdrücklich – und nicht mehr wie bisher «im Einzelfall» – erfolgen muss (Bst. a). In der Praxis wird freilich nicht sehr häufig darauf abgestellt, weil eine Einwilligung typischerweise bedeutet, dass die Personendaten im Ausland nicht mehr geschützt sind, und darauf muss die betroffene Person hingewiesen worden sein. Denkbar sind aber auch Abstufungen, wie zum Beispiel der Einsatz von Vertragsklauseln, die zwar insbesondere im Lichte von «Schrems II» nicht den Anforderungen von Art. 16 revDSG genügen, von den betroffenen Personen aber als hinreichend akzeptiert werden. In der Praxis spielt die Einwilligung meist deshalb keine Rolle, weil es oft nicht möglich ist, von allen betroffenen Personen eine solche einzuholen. Übrigens: **Gibt eine Person ihre Personendaten selbst ins Ausland bekannt** (z.B. indem sie sie auf einer ausländischen Website erfasst), liegt keine Bekanntgabe im Sinne von Art. 16 revDSG vor, und es braucht auch keine Einwilligung für den Datenexport.

[76] Am wichtigsten sind in der Praxis die beiden nächsten Ausnahmen in Art. 17 revDSG:

> a) Personendaten dürfen ohne angemessen Datenschutz ins Ausland bekanntgegeben werden, wenn dies **im unmittelbaren Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags** mit der betroffenen Person steht oder – neu – mit einer Person, in deren Interesse der Vertrag abgeschlossen oder abgewickelt werden soll (Bst. b). Letzteres kann z.B. ein wirtschaftlich Berechtigter oder ein Geldempfänger sein, dessen Personendaten von einer Bank im Rahmen der Abwicklung einer Transaktion ins Ausland bekanntgegeben werden müssen. Bisher wurde die Bekanntgabe von Daten Dritter unter der Ausnahme mitsubsumiert. Die Formulierung der verwandten Bestimmung in Art. 31 Abs. 2 Bst. b revDSG geht nicht ganz so weit, ist aber im Ergebnis gleich zu verstehen; die weitergehende Fassung von Art. 17 Bst. b revDSG ist wohl der Angleichung an Art. 49 Abs. 1 Bst. b und c DSGVO geschuldet (welche dieselben Ausnahmen vorsieht). Der Begriff «im unmittelbaren Zusammenhang» wird nach herrschender Ansicht als «erforderlich» verstanden, also letztlich genau so wie Art. 31 Abs. 2 Bst. b revDSG. Auch die DSGVO verlangt, dass der Datentransfer für den Abschluss oder die Abwicklung des Vertrags *erforderlich* ist und nicht bloss *in dessen Rahmen* geschieht. Zu beachten ist, dass Art. 17 Abs. 1 Bst. b revDSG einen Export in diesen Fällen ohne Einwilligung und ohne Vertrag mit dem Empfänger erlaubt. Die Bestimmung entbindet den exportierenden Verantwortlichen jedoch weder von seiner Transparenzpflicht noch – nach herrschender Ansicht – davor sicherzustellen, dass die Daten nicht für andere Zwecke verwendet werden.
>
> b) Personendaten dürfen ohne angemessenen Datenschutz ins Ausland bekanntgegeben werden, wenn dies für die Feststellung, die Ausübung oder zur Durchsetzung von Rechtsansprüchen **vor einem Gericht oder einer anderen zuständigen ausländischen Behörde notwendig ist** (Art. 17 Abs. 1 Bst. c Ziff. 2 revDSG). In der Revi-

sion hinzugekommen ist die Ausweitung des Anwendungsbereichs dieser Ausnahme auf andere zuständige Behörden, nicht mehr nur Gerichte. Diese Anpassung ist von erheblicher Praxisrelevanz, denn das bisherige Exportregime des DSG stiess an seine Grenzen, wenn Schweizer Unternehmen mit ausländischen Behörden kooperieren wollten, z.B. im Rahmen einer aufsichtsrechtlichen oder strafrechtlichen Untersuchung. Möglich war nur die Bekanntgabe von Personendaten in einem ausländischen *Gerichtsverfahren* (z.B. in Form der Einreichung von Beweismitteln oder einer *pre-trial discovery*). Die meisten gerichtlichen Verbote der Bekanntgabe von Daten von Mitarbeitern oder Drittberatern durch Schweizer Banken im Rahmen des US-Steuerstreits der Schweiz erfolgten auf Basis dieser (historisch bedingten) Regelungslücke im bisherigen DSG.

Die erweiterte Ausnahme von Bst. c Ziff. 2 bedeutet jedoch nicht, dass Personendaten frei an ausländische Behörden geliefert werden dürfen: Erstens gelten weiterhin die Bearbeitungsgrundsätze und weitere Prinzipien des DSG (einschliesslich des Transparenzgrundsatzes und des Widerspruchsrechts) und zweitens muss selbst im Falle einer Bekanntgabe sichergestellt werden, dass danach keine zweckwidrige Verwendung der Personendaten erfolgt. In Gerichtsverfahren wird dies seitens des Gerichts durch die Verfahrensordnungen und die Verschlussanträge sichergestellt und seitens der Gegenparteien dort, wo das Gesetz die Geheimhaltung nicht bereits vorsieht, durch entsprechende Vereinbarungen oder gerichtliche Anordnungen. In den USA hat sich für diese Zwecke beispielsweise die Verwendung von auf Personendaten erweiterte *protective orders* für *pre-trial discoveries* eingespielt, d.h. gerichtlich bestätigte Geheimhaltungsvereinbarungen mit Verwendungsbeschränkungen.

[77] Art. 17 revDSG sieht noch andere Ausnahmen vor, so namentlich für die Wahrung **überwiegender öffentlicher Interessen** (die Hürden sind gemäss der Gerichtspraxis hier sehr hoch), im Bereich des Schutzes der **körperlichen Unversehrtheit**, bezüglich den von der betroffenen Person selbst **allgemein zugänglich gemachten Daten** und für Daten in einem gesetzlich vorgesehenen **Register**. In Art. 17 revDSG nicht vorgesehen ist der Export gestützt auf eine gesetzliche Pflicht. Sollte jedoch eine Bestimmung des Schweizer Rechts tatsächlich eine Bekanntgabe von Personendaten in ein unsicheres Drittland erlauben oder erfordern, dürfte sie Art. 16 f. revDSG in der Regel als *lex specialis* vorgehen.

[78] In der Parlamentsberatung richtigerweise gestrichen wurde das Erfordernis, wonach der Verantwortliche oder Auftragsbearbeiter den EDÖB über das Abstellen auf gewisse Ausnahmen hätte informieren müssen. Schon heute geht die Pflicht nach Art. 19 revDSG, die betroffene Person (auch) über die Ausnahmen nach Art. 17 revDSG zu informieren weiter als die DSGVO.

3. Sanktionen

[79] Blieb die Verletzung der Datenexportbestimmungen des DSG bisher meist folgenlos, so kann sie neu strafrechtlich sanktioniert werden. Mit **Busse** bis zu CHF 250'000 bestraft wird diejenige private Person, die vorsätzlich dafür verantwortlich ist, dass Personendaten unter Verstoss gegen Art. 16 und 17 revDSG bekanntgegeben werden. Das umfasst auch eine Verletzung der Melde- und Genehmigungspflicht. Allerdings ist ein Strafantrag erforderlich, d.h. eine betroffene Person muss tätig werden. Der EDÖB selbst kann keinen Strafantrag einreichen.

[80] Die Strafnorm, wie auch Art. 16 und 17 revDSG, gelten nicht nur für Verantwortliche, sondern **auch für Auftragsbearbeiter**. Dies bedeutet, dass der Auftragsbearbeiter in der Schweiz, der seine Dienste einem Verantwortlichen im Ausland anbietet und zu diesem Zweck ihm überreichte Personendaten ins Ausland zurückübermittelt, die Vorschriften von Art. 16 und 17 revDSG ebenfalls beachten muss. Auch dieses Szenario ist bisher meist unter den Tisch gefallen. Normalerweise werden Datenexportverträge nur mit Auftragsbearbeitern als Empfänger von Personendaten abgeschlossen, nicht als Übermittler von solchen. In der Praxis löst sich das Problem unter Schweizer Recht zum einen meist dadurch, dass die Rückübermittlung von Personendaten an den Verantwortlichen nicht als Bekanntgabe gilt, weil die Daten von ihm stammen und somit der Kreis der Empfänger nicht erweitert wird. Zum anderen kann, je nach Situation, davon ausgegangen werden, dass eine betroffene Person darin eingewilligt hat, dass ihre Daten im Land des Verantwortlichen bearbeitet werden, wenn sie ihm ihre Daten dort übergegeben hat – eine Rückübermittlung in dieses Land wäre diesfalls von dieser Einwilligung ebenfalls erfasst. Ob die Einwilligung ausdrücklich im Sinne des DSG erfolgt ist (N 32) ist freilich eine andere Frage. Es wird sich zeigen, ob in Zukunft auch für den Fall, dass der Verantwortliche sich in einem unsicheren Drittstaate befindet, künftig vermehrt auf vertragliche Garantien abgestellt wird.

H. Geltungsbereich des revidierten DSG

1. Persönlicher Geltungsbereich

[81] Der persönliche, sachliche und örtliche Geltungsbereich des DSG wurde nicht wesentlich verändert – vom Wegfall des *Schutzes* von Daten juristischer Personen (N 19) einmal abgesehen. Die Regelungen finden sich in Art. 2 und 3 revDSG. Der persönliche Geltungsbereich umfasst weiterhin private Personen (natürliche und juristische) und Bundesorgane. Es wurde darauf verzichtet, auch kantonale Organe dem DSG zu unterstellen; die bisherige Subsidiaritätsklausel ist sogar entfallen. Die kantonalen Datenschutzgesetze werden derzeit ebenfalls an die neuen europarechtlichen Anforderungen angepasst oder sind es bereits.

2. Sachlicher Geltungsbereich

[82] Der sachliche Geltungsbereich des DSG weicht weiterhin von jenem der DSGVO ab. Grundsätzlich gilt das DSG immer dann, wenn Personendaten bearbeitet werden. Die Ausnahmen sind teilweise enger, teilweise weiter gefasst als unter der DSGVO. Die DSGVO erfasst **manuelle Datenbearbeitungen** nur dann, wenn die Personendaten dabei in einem Dateisystem abgelegt werden. Das DSG kennt diese Einschränkung (weiterhin) nicht.

[83] Unterschiedlich geregelt ist auch die Ausnahme vom sachlichen Geltungsbereich für die Bearbeitung von Daten zum ausschliesslich persönlichen Gebrauch. In der Schweiz bezieht sich die Ausnahme in Art. 2 Abs. 2 Bst. a revDSG auf sämtliche **Datenbearbeitungen im privaten Familien- und Freundeskreis**. Demgegenüber greift die «Haushaltsausnahme» nach Art. 2 Abs. 2 Bst. c DSGVO nur, wenn eine persönliche oder familiäre Tätigkeit keinen Bezug zur beruflichen oder wirtschaftlichen Tätigkeit des Bearbeiters aufweist. Das DSG findet auch auf zu beruflichen Zwecken erstellte persönliche Notizen keine Anwendung, sofern sie nicht mit anderen geteilt werden. Umgekehrt findet die DSGVO auch auf den rein privaten, nicht beruflichen und nicht gewerblichen Austausch zwischen sich unbekannten Privatpersonen – etwa in sozialen Medien –

keine Anwendung, soweit er nicht öffentlich erfolgt. In der Schweiz findet das DSG hingegen auf den Smalltalk an einer Party mit einer nicht-nahestehenden Person (weder Freund noch Familienmitglied) durchaus Anwendung.

[84] Völlig neu formuliert wurde die Ausnahme in Art. 2 Abs. 3 revDSG. Das Konzept, wonach das vor Gerichten und Behörden geltende **Verfahrensrecht grundsätzlich vor dem DSG Vorrang** hat, gilt weiterhin. Die Grenzen haben sich aber verschoben. Erfasst sind alle bundesrechtlichen Verfahrensordnungen, mit Ausnahme des erstinstanzlichen Verwaltungsverfahrens (d.h. auf Verfahren zum Erlass einer Verfügung). Dazu zählen etwa das Verwaltungsverfahrensgesetz (VwVG)[66], die Zivilprozessordnung (ZPO)[67], das Bundesgesetz über Schuldbetreibung und Konkurs (SchKG)[68], die Strafprozessordnung (StPO)[69] oder das Rechtshilfegesetz (IRSG)[70]. In Verfahren vor Schlichtungsbehörden und Sühnebeamten, wie etwa dem Friedensrichter im Sinne von Art. 3 ZPO, gehen deren Verfahrensbestimmungen dem DSG ebenfalls vor. Das Gleiche gilt neuerdings auch für **private Schiedsgerichte** mit Sitz in der Schweiz[71], sofern sie bundesrechtlichen Verfahrensordnungen folgen[72]. Datenschutzrechtlich wirft dies Fragen auf, da die betreffenden Verfahrensordnungen den Datenschutz nicht wirklich regeln; dies ist weitgehend den Parteien oder Schiedsordnungen überlassen[73]. Die DSGVO kennt keine solche Ausnahme für Schiedsgerichte, weshalb im Falle von Schiedsrichtern oder Parteien mit einer Niederlassung im EWR auch vor Schweizer Schiedsgerichten für diese die DSGVO gilt.

[85] Unter dem bisherigen Recht endete der Anwendungsbereich des DSG mit der Hängigkeit des betreffenden Verfahrens, was immer wieder zu Abgrenzungsschwierigkeiten führte. Neu wird stattdessen darauf abgestellt, ob eine bestimmte Datenbearbeitung «in» einem Verfahren stattfindet. Das soll dann gegeben sein, wenn die Datenbearbeitung in einem unmittelbaren, funktionalen Zusammenhang mit dem Verfahren steht[74]. Es muss mit anderen Worten eine Datenbearbeitung sein, die dem betreffenden Verfahren dient, unmittelbar aus diesem folgt oder von der Verfahrensordnung vorgesehen ist. Erfasst sind also etwa Eingaben (inklusive deren Übermittlung an eine andere Partei), Partei- und Zeugenaussagen und deren Bearbeitung, das Bearbeiten von Beweismitteln, deren Beschaffung durch die Behörde sowie das Verfassen und Eröffnen einer Verfügung oder eines Entscheids. Kein unmittelbarer, funktionaler Zusammenhang dürfte hingegen in der Regel bei Recherchen und Arbeiten im Vorfeld eines Verfahrens bestehen. Der unmittelbare, funktionale Zusammenhang fehlt wohl auch im Falle des Entwurfs einer Eingabe, welcher der Gegenpartei im Vorfeld zugestellt wird, bei internen und externen Berichten und Einschätzungen, Medienmitteilungen sowie der Berichterstattung der Presse.

---

66 Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG) vom 20. Dezember 1968, SR 172.021.

67 Schweizerische Zivilprozessordnung (Zivilprozessordnung, ZPO) vom 19. Dezember 2008, SR 272.

68 Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) vom 11. April 1889, SR 281.1.

69 Schweizerische Strafprozessordnung (Strafprozessordnung, StPO) vom 5. Oktober 2007, SR 312.0.

70 Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG) vom 20. März 1981, SR 351.1.

71 BBl 2017 7013.

72 So etwa Internationale Schiedsgerichte mit Sitz nach dem 12. Kapitel des IPRG.

73 Zum ganzen Thema: David Rosenthal, Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance, in: ASA Bulletin December 2019 No 4, Kluwer Law International (http://www.rosenthal.ch/downloads/Rosenthal-ArbitrationGDRP.pdf [Stand 9. Oktober 2020]).

74 BBl 2017 7013.

[86] Die Aussage der Botschaft, wonach die Ausnahme greifen soll, sobald sich ein Gericht oder eine Behörde zum ersten Mal mit einem Fall befasst[75], greift hingegen zu kurz. Entscheidend muss der **Zeitpunkt** sein, zu welchem die Verfahrensordnung ihre Geltung beansprucht. So regelt die ZPO bereits das Einreichen einer Klageschrift[76] und die StPO die Anzeige einer Straftat[77]. Vom Geltungsbereich des DSG ausgenommen sind nur aber immerhin alle Datenbearbeitungen, welche einen unmittelbaren, funktionalen Zusammenhang mit dem Verfahren aufweisen.

[87] Diese Abgrenzungen werden in der Praxis insbesondere bezüglich der Ausübung des **Auskunftsrechts** von Relevanz sein: Wo eine Datenbearbeitung nicht von der Verfahrensordnung erfasst ist, wird sie unabhängig von der Hängigkeit des Verfahrens dem DSG unterliegen – auch bezüglich des Auskunftsrechts. Soll das Auskunftsrecht hingegen dazu benutzt werden, um vorsorglich an Beweismittel für die Geltendmachung von Ansprüchen im Zivilprozess zu gelangen, kann der Verantwortliche die betroffene Person auf das Verfahrensrecht verweisen, weil die vorsorgliche Beweisführung eine von der ZPO geregelte Datenbearbeitung darstellt[78]. Dass das Verfahren zu diesem Zeitpunkt noch nicht hängig ist, spielt unter dem neuen DSG keine Rolle mehr.

3. Örtlicher Geltungsbereich

[88] Der örtliche Geltungsbereich ist teilweise in Art. 3 revDSG geregelt. Diese Bestimmung ist neu, hält aber lediglich fest, was schon bisher gilt. Der Wortlaut von Art. 3 Abs. 1 revDSG entspricht der schon zuvor im Kartellgesetz eingeführten Regelung und hält fest, dass das **Auswirkungsprinzip** als spezielle Ausprägung des Territorialitätsprinzips auch im DSG gilt. Es besagt, dass die öffentlich-rechtlichen Bestimmungen des DSG auf alle Sachverhalte Anwendung finden, die sich zwar im Ausland zutragen, sich aber in ausreichendem Mass auch auf das Territorium der Schweiz auswirken oder auswirken werden. Das Bundesgericht wendete das Auswirkungsprinzip beispielweise im «Street View»-Entscheid an[79]. Was ein ausreichendes Mass ist, ist nicht völlig klar. Es muss sich vernünftigerweise um über Einzelfälle hinausgehende, spürbare Auswirkungen handeln. Mit Auswirkung ist dabei ein potenzieller oder tatsächlicher Eingriff in die Persönlichkeit einer betroffenen Person in der Schweiz gemeint.

[89] Obwohl nicht genannt, gilt das **Territorialitätsprinzip** im DSG auch in seinen anderen Facetten: Findet ein relevanter Teil des von einer öffentlich-rechtlichen Bestimmung des DSG geregelten Sachverhalts (z.B. Beschaffung von Personendaten, Verletzung der Datensicherheit) in der Schweiz statt, so findet die den Sachverhalt ggf. regelnde öffentlich-rechtliche Bestimmung Anwendung. Es muss nicht der gesamte Sachverhalt in der Schweiz stattfinden; eine einzelne, relevante Handlung in der Schweiz (wie z.B. der Betrieb eines Servers, das Erheben von Daten, aber auch die Datenbearbeitung bestimmende oder fördernde Handlungen, wie das Festlegen ihres Zwecks und ihrer wesentlichen Mittel) kann genügen, auch wenn die Datenbearbeitung ansonsten im Ausland stattfindet oder der Verantwortliche sich im Ausland befindet. Kann der tatsächliche Ort der Handlung eines Verantwortlichen oder des Auftragsbearbeiters nicht ermittelt werden, wird in der Regel an dessen Sitz bzw. Wohnsitz angeknüpft werden (im Sinne eines **nor-**

75 BBl 2017 7013.

76 Art. 130 ff. ZPO.

77 Art. 309 StPO.

78 Art. 158 ZPO.

79 BGE 138 II 346, E. 3.3.

mativen Handlungsorts). Bei Zweigniederlassungen greift das Territorialitätsprinzip allerdings nur, wenn ein Bezug zu dieser besteht und die Datenbearbeitung nicht am Ort der Hauptniederlassung vorgenommen wird. Geht es um eine Datenbearbeitung der Zweigniederlassung wird sie ohnehin als eigene Verantwortliche gelten. Das revidierte DSG kann also weiterhin **extraterritorial** Anwendung finden, soweit ein hinreichender Bezug zur Schweiz besteht, und sei es nur, dass sich die betroffenen Personen in der Schweiz befinden und somit eine relevante Auswirkung in der Schweiz erfolgt, die Datenbearbeitung aber im Ausland stattfindet und auch der Verantwortliche seinen Sitz nicht in der Schweiz hat. Die Bestimmung von Art. 3 Abs. 1 revDSG geht damit über Art. 3 Abs. 2 DSGVO hinaus.

[90] Zu den **öffentlich-rechtlichen Bestimmungen** gehören z.B. die Informationspflicht (Art. 19 revDSG), die Pflicht zum Führen eines Verzeichnisses der Bearbeitungstätigkeiten (Art. 12 revDSG), zur Vornahme einer Datenschutz-Folgenabschätzung (Art. 22 f. revDSG) oder die Meldepflicht bei Verletzungen der Datensicherheit (Art. 24 revDSG). Auch die Aufsichtskompetenz des EDÖB ist öffentlich-rechtlicher Natur. Gleicher Natur ist auch die Pflicht gewisser ausländischer Verantwortlicher zur Benennung eines Vertreters in der Schweiz (Art. 14 f. revDSG).

[91] **Privatrechtlicher Natur** hingegen sind die Bearbeitungsgrundsätze (Art. 6 und 8 revDSG), die Regelung zur Auftragsbearbeitung (Art. 9 revDSG), das Auskunftsrecht (Art. 25 ff. revDSG) und die Regelungen zur Persönlichkeitsverletzung und deren Rechtfertigung (Art. 30 f. revDSG). Für diese Regelungen gilt, was schon bisher galt und neu in Art. 3 Abs. 2 revDSG festgehalten wird: Das internationale Privatrecht. Kann ein Gerichtsstand in der Schweiz begründet werden[80], so kann die betroffene Person demnach das auf die Beurteilung anwendbare Recht weitgehend auswählen[81]. Befinden sie oder der Anspruchsgegner sich in der Schweiz, muss mit der Anwendbarkeit des DSG gerechnet werden auch wenn die Datenbearbeitung im Ausland stattfindet.

III. Betroffenenrechte

A. Informationspflicht und automatisierte Einzelentscheide

1. Übersicht

[92] Die Informationspflichten werden im revidierten DSG deutlich ausgebaut, jedenfalls für private Verantwortliche. Mussten diese die betroffene Person bisher nur informieren, wenn sie besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafften, so besteht neu nach Art. 19 revDSG **bei *jeder* Beschaffung von Personendaten** eine Informationspflicht, soweit keine der Ausnahmen in Art. 20 revDSG greift. Der Inhalt der Informationspflichten wurde zudem erweitert. Abgebaut wurde die Informationspflicht hingegen bei Bundesorganen, was aber vermutlich eher einem Versehen des Gesetzgebers zuzuschreiben ist. Dogmatisch handelt es sich bei der Informationspflicht um eine öffentlich-rechtliche Bestimmung, weshalb ihre Verletzung für sich gesehen keine Persönlichkeitsverletzung bewirkt und demzufolge auch *nicht* über Art. 31 revDSG (Rechtfertigungsgründe) gerechtfertigt werden kann. Die vorsätzliche Verletzung ist mit einer **Busse** bis zu CHF 250'000 strafbewehrt. Allerdings kann nur die betroffene Person Antrag stellen, nicht der EDÖB. Er kann immerhin die Vornahme einer rechtskonformen Information

80 Art. 129 IPRG, Art. 5 Ziff. 3 LugÜ.

81 Art. 139 IPRG.

anordnen (nicht jedoch die Einstellung der Datenbearbeitung mangels gemäss Art. 19 revDSG erfolgter Information). Will der EDÖB die Datenbearbeitung unterbinden, so muss er dies mit einer Verletzung des Transparenzgebots von Art. 6 revDSG begründen, das parallel zur Informationspflicht gilt. Das ist auch der Sinn und Zweck von Art. 19 revDSG: Er stellt sicher, dass einer betroffenen Person *zusätzliche* Informationen zur Datenbearbeitung zur Verfügung stehen, falls sie sich dafür interessiert, während Art. 6 revDSG eine «Grundtransparenz» sicherstellt, die generell gegenüber allen betroffenen Personen bestehen muss. Auch die DSGVO kennt diese Unterscheidung: Die Grundtransparenz wird in Art. 5 DSGVO geregelt, die Informationspflicht hingegen in Art. 13 f. DSGVO. Mit wenigen Ausnahmen geht Art. 19 revDSG allerdings weniger weit als Art. 13 f. DSGVO.

[93] Die Informationspflicht nach Art. 19 revDSG gilt nur dann, wenn ein Verantwortlicher Personendaten «beschafft». Dies erfordert eine **Planmässigkeit**. Soweit ein Verantwortlicher ungewollt oder zufällig an Personendaten gelangt, muss er nicht informieren. Planmässig erhebt z.B. der Arbeitgeber die HR-Daten seiner Arbeitnehmer, der Händler die Kontakt- und Transaktionsdaten und Kundendienstanfragen seiner Kunden, die AG die gesetzlich vorgesehenen Daten ihrer Aktionäre. Nicht planmässig ist der gelegentliche Eingang der Anfrage eines Journalisten, die Entgegennahme der Visitenkarte während einer Sitzung oder der Erhalt von Personendaten in Form von Unterschriften unter Verträgen mit anderen Unternehmen. Informiert werden muss dementsprechend nur über die Datenbearbeitung, wie sie der Verantwortliche **zum Zeitpunkt der Beschaffung** plant. Die Information muss wiederum spätestens zu diesem Zeitpunkt geschehen sein, kann aber auch vorgängig erfolgen solange den betroffenen Personen ein Konnex zwischen Information und Beschaffung ihrer Personendaten möglich ist; im Falle einer indirekten Beschaffung gilt eine etwas lockerere Regelung (N 97). Da die Information an die Beschaffung von Personendaten anknüpft, ist es beim Inkrafttreten des revidierten DSG nicht erforderlich, die Bestandskunden proaktiv zu informieren, wie dies teilweise bei Inkrafttreten der DSGVO geschah. Es genügt, wenn diese im Falle der nächsten Beschaffung informiert werden (beim nächsten Einkauf, der nächsten Schadensmeldung, etc.) und die Datenschutzerklärung im Übrigen auf der eigenen Website bereitgehalten sowie in Broschüren, Formularen, AGB, etc. referenziert wird.

[94] Über **spätere Änderungen** (z.B. andere Speicherorte von Daten, weitere Empfängerkategorien) muss nicht informiert werden. Einzige Ausnahme hiervon ist der Fall, in welchem der Verantwortliche die beschafften (oder sonst erhaltenen) Daten einem zusätzlichen Zweck zuführen will. Während die DSGVO diesen Fall ausdrücklich regelt, tut dies Art. 19 revDSG nicht. Die Fallkonstellation ist unter dem DSG dogmatisch als erneute Datenbeschaffung durch den Verantwortlichen einzustufen, auch wenn sie bloss bei ihm selbst, in seinen eigenen Datenbeständen, und nicht mehr bei der betroffenen Person erfolgt. Eine überschiessende Datenschutzerklärung, die solche, in der Zukunft möglichen Zwecke und Bearbeitungen vorwegnimmt, ist auch dann erlaubt, wenn darin von Verwendungszwecken die Rede ist, die noch nicht geplant sind.

2. Inhalt der Information

[95] Während Art. 13 f. DSGVO eine Information der betroffenen Person nach dem Giesskannenprinzip vorschreibt, verlangt Art. 19 revDSG nur relativ wenige Mindestinformationen. In den meisten Fällen wird die Mitteilung der Mindestinformationen auch genügen. Mitgeteilt werden müssen die Identität und die Kontaktdaten des Verantwortlichen (mit einer physischen und einer elektronischen oder telefonischen Kontaktmöglichkeit), wobei bei mehreren gemeinsamen

Verantwortlichen im Normalfall einer genügt (und zwar denjenigen, an den sich die betroffene Person wenden soll; er muss dann ggf. über weitere Verantwortliche Auskunft geben). Des Weiteren müssen auch die Kontaktdaten eines etwaigen Datenschutzberaters (im Sinne von Art. 10 revDSG) angegeben werden und – wo er tatsächlich bestellt werden musste – der Schweizer Vertreter (im Sinne von Art.14 revDSG). Dies ist allerdings nicht in Art 19 revDSG geregelt sondern bei den jeweiligen Bestimmungen. Anzugeben sind die Bearbeitungszwecke, wobei, anders als unter der DSGVO, auch Kurzbezeichnungen wie «Direktmarketing», «Produktentwicklung» oder «Betrugsbekämpfung» zulässig sind. Je knapper der Zweck definiert wird, desto grösser ist letztlich das Risiko des Verantwortlichen, dass die mitgeteilten Bearbeitungszwecke nach dem Vertrauensprinzip und der Unklarheitenregel einschränkend ausgelegt werden.

[96] Anzugeben sind weiter die *Kategorien* der Empfänger, wobei es natürlich auch erlaubt (aber nicht erforderlich) ist, die *einzelnen Empfänger* zu nennen. Zu den Empfängern gehören nicht nur «Dritte», sondern auch etwaige andere gemeinsame Verantwortliche oder Auftragsbearbeiter, nicht aber die eigenen Mitarbeiter, Zweigniederlassungen oder andere Abteilungen. Ist eine **Bekanntgabe ins Ausland** geplant – wozu auch die Speicherung auf ausländischen Systemen (Cloud) gehört – sind die Länder anzugeben, gleichgültig, ob diese einen angemessenen Datenschutz bieten. Hier geht das DSG weiter als die DSGVO. Angaben wie «jedes Land der Welt», «weltweit» oder «Europa» oder «alle Länder, in denen wir vertreten sind» genügen allerdings, da diese Länder bestimmbar sind. Anzugeben ist auch, welche Datenschutzgarantien gegebenenfalls zum Einsatz kommen (z.B. EU-Standardvertragsklauseln) oder auf welche Ausnahmen nach Art. 17 revDSG sich der Verantwortliche allenfalls bezieht; auch hier weicht das DSG von der DSGVO ab. Zu informieren ist schliesslich noch über automatisierte Einzelentscheide (dazu N 106 ff.).

[97] Werden die Daten **nicht bei der betroffenen Person direkt beschafft** (wozu auch die «interne» Datenbeschaffung, beispielsweise zum Zweck einer Sekundärnutzung, zählt; nicht aber das direkte Beobachten der betroffenen Person, auch wenn diese dies nicht bemerkt), so sind auch die Kategorien der beschafften (nicht jedoch die im Rahmen der Datenbearbeitung selbst erzeugten) Personendaten anzugeben. Die Information der betroffenen Person über die Datenbeschaffung muss erfolgen, sobald der Verantwortliche deren Personendaten weitergibt (und sei es nur an einen Auftragsbearbeiter oder anderen gemeinsamen Verantwortlichen), spätestens jedoch innerhalb eines Monats nach der Beschaffung.

[98] Nur ausnahmsweise werden über diese Mindestinformationen **hinausgehende Angaben** nötig sein, so z.B. Angaben zur Dauer der Datenbearbeitung, der Datenquelle, der Rechtsgrundlage, zu einem spezifischen Datenempfänger oder zu den Betroffenenrechten. Art. 19 Abs. 2 revDSG enthält hierzu eine Generalklausel, die Fälle abdecken soll, in welchen aufgrund von besonderen Umständen, wie z.B. einem sehr hohen Risiko einer Persönlichkeitsverletzung, weitere Angaben erforderlich sind, um diese Risiken einzuschätzen oder die Wahrnehmung der Betroffenenrechte sicherzustellen. Ein Beispiel für Letzteres ist, wenn eine Wirtschaftsauskunftei erklärt, wie bei ihr Selbstauskünfte eingeholt und falsche Daten korrigiert werden können (normalerweise ist dies – anders als unter der DSGVO – nicht erforderlich). Auf Zusatzangaben, die die betroffenen Personen typischerweise nicht interessieren, darf verzichtet werden. Umgekehrt werden selbst die Zusatzangaben i.d.R. nicht über das hinausgehen müssen, was unter Art. 13 f. DSGVO erforderlich ist.

3. Form der Information

[99] Für die Mitteilung der Informationen nach Art. 19 revDSG gibt es keine **Formvorschrift**. In der Praxis wird sie allerdings meist in Form einer Datenschutzerklärung erfolgen. Auch Tonbandansagen oder Piktogramme können eingesetzt werden[82]. Eine **mehrstufige Datenschutzerklärung** (d.h. zuerst eine Kurzinformation, dann, auf einer weiteren Stufe, die vollen Informationen) mag benutzerfreundlich sein, ist aber in den meisten Fällen keine Pflicht. Dabei genügt es im Schweizer Recht grundsätzlich, wenn der Verantwortliche die betroffene Person darüber informiert, wo sie die Datenschutzerklärung erhält, soweit es ihr zugemutet werden kann, die Datenschutzerklärung dort abzurufen, einzusehen oder abzuholen. *Un*genügend ist die Angabe einer Kontaktperson für weitere Fragen. Ob die betroffene Person die Datenschutzerklärung anschaut, spielt keine Rolle. Art. 19 revDSG verlangt nur, dass sie ihr zur Verfügung steht.

[100] Anders, als dies manche Datenschutzbehörden unter der DSGVO verlangen, sieht das DSG keine «Basisinformationen» vor, die im Falle mehrstufiger Informationen auf der ersten Stufe der Information auf jeden Fall zu liefern sind (also z.B. welche Angaben über den Link zur Datenschutzerklärung hinaus auf einem Schild sein müssen, welches über die Videoüberwachung informiert). Auch in AGB oder anderen Unterlagen genügt in der Regel der Hinweis auf die Datenschutzerklärung unter Angabe eines **Links im Internet**. Dies führt zwar mitunter zu einem Medienbruch, wenn die betroffene Person die Angaben abrufen will. Aber in den meisten Fällen wird es der betroffenen Person aufgrund der allgegenwärtigen Verfügbarkeit des Internets zuzumuten sein, die Datenschutzerklärung dort abzurufen, falls sie sich für die weitergehenden Angaben von Art. 19 revDSG interessiert[83]. Zu berücksichtigen ist auch das Informationsinteresse der betroffenen Person: Während sie erwarten mag, dass sich in Vertragsunterlagen ein Hinweis auf den Zugang zur Datenschutzerklärung findet, ist dieser auf Visitenkarten, Briefpapier oder der Fusszeile von E-Mails nicht nötig. Sollte sich eine Person ausnahmsweise dafür interessieren, kann ihr zugemutet werden, auf der Website des Unternehmens nachzuschauen. Darum wird es unter dem DSG auch nicht nötig sein, in Alltagssituationen – wie etwa bei einer Terminvereinbarung, am Schalter oder in einer Sitzung – auf die Datenschutzerklärung hinweisen zu müssen. Dies bedeutet aber umgekehrt auch, dass Unternehmen ihre Datenschutzerklärung auf ihrer Website gut zugänglich und erkennbar bereithalten sollten.

[101] Hinsichtlich der **Formulierung** einer Datenschutzerklärung werden dieselben Grundsätze zur Anwendung gelangen, wie sie auch für AGB gelten: Unklarheiten werden zu Lasten des Verfassers ausgelegt. Wenn also nicht klar ist, was mit dem Begriff des «Direktmarketings» gemeint ist, wird er eng ausgelegt. Wer spezielle Formen des Direktmarketings betreiben will, wird diese daher expliziter formuliert aufführen müssen. Auf ungewöhnliche Bestimmungen ist speziell hinzuweisen. Das ergibt sich aber ohnehin auch aus dem Grundsatz der Transparenz nach Art. 6 revDSG.

---

82 Vgl. etwa die Initiative «privacy-icons.ch» der Schweizer Wirtschaft.

83 Immerhin traut die Schweiz dies auch ihren Bürgern zu, wenn diese beispielsweise auf Bundesgesetze zugreifen möchten. Diese und viele weitere amtliche Informationen sind heute nur noch via Internet einfach und rasch zugänglich. Notabene wird der Wegfall der Informationspflicht nach Art. 20 Abs. 1 Bst. b revDSG damit gerechtfertigt, dass die nötigen Informationen sich bereits aus dem Gesetz ergeben – wozu die betroffenen Personen eben das Internet konsultieren müssen. Mutet der Gesetzgeber ihnen diesen Aufwand zu, so muss die Verfügbarkeit auch für private Datenschutzerklärungen genügen.

4. Ausnahmen

[102] Art. 20 revDSG definiert einen Katalog an **Ausnahmen von der Informationspflicht**, der über jenen der DSGVO hinausgeht. Wer sich auf eine Ausnahme beruft, muss dies nicht offenlegen. Nicht informiert werden muss eine betroffene Person zudem über das, was sie schon weiss. Ein Verantwortlicher muss also nicht jedes Mal, wenn er Daten beschafft, von neuem informieren, wenn zwischen der früher erfolgten Information und der aktuellen Beschaffung ein gewisser zeitlicher und inhaltlicher Konnex besteht. Gemäss der Botschaft gelten auch jene Personen als vorinformiert, die ihre Personendaten dem Verantwortlichen ohne dessen Zutun zugänglich machen[84]. Wird die dem zugrundeliegende Logik weitergedacht, heisst dies: Wenn aus den Umständen hervorgeht, dass die betroffene Person auf die Informationen nach Art. 19 revDSG verzichtet hat oder sie an der Information nicht interessiert ist, muss die betroffene Person ebenfalls nicht informiert werden. Das macht durchaus Sinn und gilt teilweise sogar unter der DSGVO[85].

[103] Auch bei **gesetzlich vorgesehenen Bearbeitungen** braucht über diese nicht informiert zu werden. Die neue Ausnahme von Art. 20 Abs. 1 Bst. b revDSG hat zur Folge, dass die Informationspflicht bei praktisch allen Datenbearbeitungen von Bundesorganen wegfällt, was erstaunt. Aber auch private Verantwortliche profitieren von der Ausnahme, soweit eine Bestimmung des Schweizer Rechts eine Datenbearbeitung vorschreibt. Das ist nicht nur bei spezialgesetzlichen Pflichten, wie etwa in der Geldwäschereibekämpfung, der Fall, sondern auch bei alltäglichen Datenbearbeitungen, wie etwa der Buchführung oder dem Führen eines Personaldossiers (oder der Falldossiers der Anwälte). Diese Ausnahme von der Informationspflicht aufgrund einer gesetzlichen Bearbeitungspflicht entspricht übrigens der Praxis des EDÖB hinsichtlich der bisherigen Pflicht zur Anmeldung von Datensammlungen[86]. Diese Pflicht gilt auch nach bisheriger Praxis nicht für Personaldossiers.

[104] Weitere Ausnahmen nach Art. 20 revDSG lassen sich mit Berufsgeheimnispflichten und dem Quellenschutz für Medienschaffende begründen. Bei indirekten Datenbeschaffungen kann auf die Information verzichtet werden, wenn der Verantwortliche die betroffene Person nicht informieren kann, weil er sie entweder nur mit **unverhältnismässigem Aufwand** identifizieren und lokalisieren könnte (soweit dies zur Information nötig ist)[87] oder aber der Aufwand zur Information als solche unverhältnismässig wäre. Die Verhältnismässigkeit wird danach beurteilt, wie gross der Aufwand des Verantwortlichen im Verhältnis zur Höhe des Informationsinteresses der Person ist. In diese Betrachtung wird das Interesse der betroffenen Person an der Ausübung ihrer Rechte gegenüber dem Verantwortlichen miteinbezogen. Allerdings sind hier bei Mehrheiten von betroffenen Personen keine Einzelbetrachtungen erforderlich; es darf objektiviert und generalisiert werden.

[105] Schliesslich sieht Art. 20 Abs. 3 revDSG noch vor, dass die Informationspflicht auf Basis einer **Interessenabwägung** ganz oder teilweise aufgehoben oder hinausgeschoben werden darf. Dies ist einerseits der Fall, wenn eine Information Drittinteressen negativ betreffen würde (z.B. weil die Information selbst Personendaten Dritter enthalten müsste oder Geheimhaltungs-

84 BBl 2017 7053.

85 So sieht § 32 Abs. 1 BDSG in Ergänzung der DSGVO für Deutschland vor, dass auf eine Information bei analog gespeicherten Daten dort verzichtet werden kann, wo das Interesse der betroffenen Person an der Informationserteilung nach den Umständen «als gering anzusehen ist».

86 Art. 11a DSG.

87 Die Bestimmung meint diesen Fall, wenn sie davon spricht, dass eine Information «nicht möglich» ist.

interessen Dritter tangieren würde) oder andererseits, wenn eine Information die mit der Datenbearbeitung angestrebte Zielerreichung ernsthaft gefährden würde und dieses Ziel wichtiger erscheint, als die (sofortige) Information (z.B. weil eine zwingend vorgängig anzukündigende Observation durch einen Privatdetektiv den Zweck der Observation vereiteln würde). Auf überwiegende private Interessen kann sich ein Verantwortlicher soweit berufen (z.B. Geheimhaltungsinteressen), als er die Personendaten nicht auch planmässig Dritten (wozu andere eigenständige Verantwortliche – einschliesslich Behörden – nicht aber gemeinsame Verantwortliche, Auftragsbearbeiter oder – gemäss ausdrücklicher Regelung – auch Gruppengesellschaften zählen) bekanntgibt. Bundesorgane können die Information auf Basis überwiegender öffentlicher Interessen oder im Zusammenhang mit der Durchführung eines Verfahrens einschränken, wobei sie meist ohnehin nicht informieren müssen aufgrund ihrer gesetzlichen Vorgaben (und dem Vorrang des Verfahrensrechts nach Art. 2 revDSG).

5. Automatisierte Einzelentscheide

[106] Die Regelung automatisierter Einzelentscheide in Art. 21 revDSG ist neu im Schweizer Datenschutzrecht; im restlichen Europa existiert sie schon seit längerem, spielte in der Praxis bisher aber eine untergeordnete Rolle. Angesichts der derzeit inflationären Schlagzeilen über den Einsatz von «Künstlicher Intelligenz» (KI) liegt sie durchaus im Trend. Ihr liegt die Überlegung zugrunde, dass Maschinen nicht über Menschen entscheiden sollen, jedenfalls nicht wenn es um wichtige Entscheide geht. Das ist an sich kein Datenschutzthema, ist hier aber geregelt, weil jedem solchen Entscheid letztlich sachlogisch ein Vorgang zugrunde liegt, dessen Problematik in der Unvollkommenheit der für den Entscheid nötigen Datenbearbeitung besteht.

[107] Mit «automatisierten Einzelentscheiden» sind – wie beim Profiling – und entgegen dem (weiter gefassten) Wortlaut, vereinfacht gesagt, nur solche Entscheide gemeint, bei denen einer Maschine ein *Ermessensentscheid* übertragen wird[88]. Die Maschine trifft eine Entscheidung aufgrund einer von der Maschine sich antrainierten oder von einem Menschen einprogrammierten Bewertung der der Maschine vorliegenden Personendaten. Die Maschine beurteilt, ob das Zeugnis des Bewerbers das nötige Notenbild aufweist, um im Prozess eine Runde weiterzukommen; oder ob dem Bankkunden die Überziehung des Kontos ausnahmsweise erlaubt wird, obwohl das nicht vereinbart ist. Der «Unwert» liegt dabei darin, dass die Maschine sich dabei immer nur an jene Daten und Faktoren halten wird, die ihr einprogrammiert oder – im Fall einer KI – antrainiert worden sind. Das werden aber nie *alle* Umstände sein. Würde hingegen ein (perfekter) Mensch denselben Bewerber beurteilen, würde er ihm womöglich trotz nicht überzeugendem Notenbild eine Chance geben, weil ein anderer Aspekt seiner Bewerbung ausnahmsweise eine Sonderbehandlung rechtfertigt. Ob die Annahme des Gesetzgebers richtig ist, dass Menschen *per se* bessere Ermessensentscheide treffen und umgekehrt nur Maschinen beim Fällen von Entscheidungen «stur» etwaigen Anweisungen folgen, soll hier nicht erörtert werden. Diese Überlegung liegt jedenfalls der Regel zugrunde.

[108] Dementsprechend sind nur Entscheide erfasst, die **vollständig von einer Maschine** getroffen werden, und dabei nur jene Entscheide, die einen Spielraum zulassen, also eine Bewertung

88 Die Botschaft spricht umgekehrt davon, dass reine «Wenn-Dann-Entscheidungen» nicht vom Begriff erfasst sind (BBl 2017 7057). Als Beispiel für eine solche Wenn-Dann-Entscheidung nennt sie den Entscheid des Bankomaten, Geld auszugeben, wenn eine genügende Kontodeckung vorhanden ist.

oder Interpretation verlangen. Das Zutrittskontrollsystem, das die Türe entsperrt, wenn ein gültiger Badge vorgelegt wird, trifft keinen automatisierten Einzelentscheid, weil kein Interpretationsspielraum besteht. Kein automatisierter Einzelentscheid liegt zudem vor, wenn mit der Bank fest vereinbart ist, dass das Konto bis CHF 1'000 überzogen werden kann und der Geldautomat diese Limite hart durchsetzt[89]. Der Automat trifft keinen Entscheid, er setzt einen solchen lediglich um. Wenn hingegen die Bank ihren Computer für jeden Kunden – anhand seiner Zahlungsein- und ausgänge – eine individuelle Limite bestimmen lässt, ist dies ein automatisierter Einzelentscheid. Kein automatisierter Einzelentscheid liegt dort vor, wo ein Computer einem Bankmitarbeiter individuelle Überzugslimiten vorschlägt, diese aber letztlich vom Mitarbeiter abgesegnet werden. Datenschutzrechtlich liegt damit ein Profiling vor (der Computer bewertet die Kreditwürdigkeit des jeweiligen Kunden vollautomatisch), aber es kommt nicht zum automatisierten Entscheid (hier weicht das revidierte DSG von der DSGVO ab)[90]. Ob ein von einer Maschine gefällter Entscheid von der Maschine oder einem Menschen mitgeteilt wird (und der Mensch den Entscheid nicht mehr beeinflussen kann bzw. soll), spielt hingegen keine Rolle.

[109] Ausserdem sind nicht alle automatisierten Einzelentscheide erfasst, sondern nur solche, die mit einer **Rechtsfolge** für die betroffene Person verbunden sind oder die diese **erheblich beeinträchtigen**. Eine Rechtsfolge kann zum Beispiel der automatisierte Abschluss eines Vertrags zu bestimmten Konditionen sein oder dessen automatisierte Kündigung[91]. Wird der Vertragsabschluss hingegen automatisiert abgelehnt wie im Beispiel des Bewerbers, so liegt zwar gerade *keine* Rechtsfolge vor, die betroffene Person erleidet – in diesem Beispiel – aber unter Umständen trotzdem eine erhebliche Beeinträchtigung. Hier geschieht dies in ihren wirtschaftlichen Belangen, Beeinträchtigungen sind aber auch in persönlichen Belangen denkbar (z.B. automatisierte Zuteilung einer medizinischen Leistung[92]). Wenn hingegen ein Computer automatisiert entscheidet, welche Werbung dem Besucher einer Website angesichts seines konkreten Profils gezeigt wird, so ist das keine erhebliche Beeinträchtigung. Eine blosse Belästigung reicht nicht, wie auch die Botschaft klarstellt[93].

[110] Entscheidet ein Computer nicht den Fall einer einzelnen Person, sondern wird ihm eine generelle Entscheidung überlassen (z.B. welcher Kundengruppe ein Rabatt angeboten werden soll oder wie Ticketpreise anhand der noch vorhandenen Kapazitäten tagesaktuell angepasst werden sollen), so liegt ebenfalls kein Fall von Art. 21 revDSG vor. Keine Rolle spielt, wie sorgfältig der automatisierte Einzelentscheid stattfindet oder ob ein Mensch versteht, warum der Computer so entschieden hat[94]. Entscheide nach dem Zufallsprinzip sind genauso erfasst wie solche, denen eine komplexe Auswertung grosser Datenmengen zugrunde liegen, ob vom Menschen programmiert oder vom Computer selbst trainiert.

---

89 BBl 2017 7057.

90 Nach Art. 22 Abs. 1 DSGVO gilt auch ein Profiling als automatisierter Einzelentscheid. Das Schweizer Parlament hat den Hinweis hingegen während den Beratungen aus dem Wortlaut von Art. 21 Abs. 1 revDSG gestrichen.

91 BBl 2017 7057; nicht ganz korrekt ist die Ausführung in der Botschaft, wonach die automatisierte Zustellung einer Rechnung kein automatisierter Einzelentscheid mit Rechtsfolge ist, weil sich die *Rechtsfolge* aus dem Vertragsschluss ergibt. Es ist deshalb kein relevanter Einzelentscheid, weil kein Ermessensentscheid vorliegt, soweit der Computer lediglich die vorher in Höhe und Fälligkeit vereinbarten Beträge automatisiert fakturiert. Eine relevante Rechtsfolge hat der Entscheid aber durchaus.

92 BBl 2017 7057.

93 BBl 2017 7057.

94 Wie zum Beispiel bei Mustererkennungssystemen, die trainiert statt programmiert werden (sog. *Deep Learning*).

[111] Findet ein relevanter automatisierter Einzelentscheid statt, so hat dies zwei Rechtsfolgen: Erstens muss die **betroffene Person informiert** werden, und zweitens hat sie das Recht, den Entscheid nach Darlegung ihres Standpunkts von einem Menschen aus Fleisch und Blut überprüfen zu lassen. Die betroffene Person hat also **Anspruch auf «menschliches Gehör»**. Anders als im Falle der ähnlichen Regelung in der DSGVO, wo nicht klar ist, ob automatisierte Einzelentscheide grundsätzlich verboten sind oder sie lediglich einen Anspruch der betroffenen Person auf menschliche Überprüfung begründen, sind automatisierte Einzelentscheide in der Schweiz grundsätzlich zulässig. Immerhin muss geprüft werden, ob sie im Einzelfall unverhältnismässig sind oder andere Bearbeitungsgrundsätze, wie etwa jenen der Datenrichtigkeit, verletzen.

[112] Die Information kann im Rahmen der Mitteilung der Entscheidung erfolgen. Zulässig ist aber ebenso eine vorgängige, allgemeine Information in einer Datenschutzerklärung. Wesentlich ist, dass die betroffene Person im Falle eines solchen Entscheids in die Lage versetzt wird, die Überprüfung durch einen Menschen und Auskunft über die Logik des Entscheids (N 113 ff.) zu verlangen. Dazu muss sie mindestens wissen, **welche Entscheide automatisiert gefällt werden** (wobei nur über im Sinne von Art. 21 revDSG relevante, nicht über alle automatisierten Entscheide zu informieren ist) und wie sie ihr Recht auf «menschliches Gehör» geltend machen kann (wobei diese Information auch erst mit dem Entscheid mitgeteilt werden darf). Weitere Angaben werden normalerweise nicht erforderlich sein, weil der betroffenen Person solche bereits über das Auskunftsrecht zur Verfügung stehen (N 115 ff.).

[113] Übt eine betroffene Person ihr Recht auf «menschliches Gehör» aus, hat sie Anspruch auf Anhörung, und zwar auch zu denjenigen Aspekten, die die Maschine nicht berücksichtigt hat. Anhören muss sich dies jemand, der befugt ist, den Entscheid umzustossen. Dieser Entscheider ist jedoch nicht verpflichtet, Letzteres zu tun, solange er den **Entscheid in guten Treuen wiedererwägt**. In der Entscheidung bleibt der Verantwortliche also frei. Wie lange er «menschliches Gehör» gewähren muss, sagt Art. 21 revDSG nicht. In vielen Fällen werden – analog zur Rechtsmittelfrist in manchen Kantonen – zehn Tage nach Eröffnung des Entscheids genügen. Die Frist wird mit Vorteil kommuniziert. Dem Anspruch auf menschliches Gehör kann z.B. Genüge getan werden, wenn mit dem Entscheid der betroffenen Person mitgeteilt wird, dass der Entscheid maschinell gefällt worden ist und sie, falls sie nicht einverstanden ist, mit einem Vertreter des Verantwortlichen sprechen kann, der den Entscheid nach Anhörung der Person wiedererwägt.

[114] Hat die Maschine im Rahmen eines Vertragsabschlusses oder einer Vertragsabwicklung bereits so entschieden, **wie es die Person verlangt hatte**, kann richtigerweise (aber anders als unter der DSGVO) keine Wiedererwägung verlangt werden (Art. 21 Abs. 3 Bst. a revDSG). Vor allem aber muss sie dann auch nicht informiert werden, d.h. es genügt im Umkehrschluss, erst im Rahmen eines abschlägigen Entscheids zu informieren (falls nicht bereits in der Datenschutzerklärung über die den automatisierten Entscheidprozess informiert wurde). Ein Online-Shop, welcher Verträge automatisch abschliesst, trifft zwar i.d.R. automatisierte Einzelentscheide[95], muss eine Wiedererwägung aber nur dann anbieten, wenn er die Bestellung automatisiert abweist, was kaum vorkommen dürfte. Eine Person kann nach Art. 21 Abs. 3 Bst. b revDSG auch vorab auf das Wiedererwägungsrecht **verzichten**, indem sie ausdrücklich darin einwilligt, dass eine Entscheidung automatisiert erfolgt (z.B. weil solche im Rahmen eines Vertragsverhältnisses regelmässig vorkommen). Hier wird jedoch im Sinne des Erfordernisses einer informierten Einwilligung

95 Soweit die Bestellung des Kunden schuldrechtlich als Vertragsangebot gilt, das vom Shop-Betreiber mit einer Annahmeerklärung angenommen werden muss.

grundsätzlich verlangt werden müssen, dass der Person klargemacht wird, worauf sie verzichtet, nämlich auf das menschliche Gehör. Ohne Information geht es in diesen Fällen also so oder so nicht.

B. Auskunftsrecht

1. Übersicht

[115] Das Auskunftsrecht in Art. 25 revDSG ergänzt die Informationspflicht nach Art. 19 ff. revDSG und ist daher ähnlich aufgebaut. Es geht inhaltlich allerdings weiter, d.h. die betroffene Person kann damit mehr erfahren als der Verantwortliche im Rahmen seiner Datenschutzerklärung offenlegen muss. Die revidierte Norm wurde einerseits um gewisse zu liefernde Informationen erweitert, andererseits aber auch im Hinblick auf die heute übliche **missbräuchliche Nutzung** des Auskunftsrechts zur Beweisbeschaffung eingeschränkt. Das war zu Recht auch in der Vernehmlassung ein grosses Thema[96]. Ferner ist das Auskunftsrecht nicht mehr nur auf Datensammlungen beschränkt, was in der Praxis allerdings von untergeordneter Bedeutung ist: In der EU gab es diese Einschränkung nie und in der Schweiz scheiterten Auskunftsansprüche selten an diesem Kriterium. Ansonsten entspricht das revidierte Auskunftsrecht im Wesentlichen dem bisherigen Recht[97]. Es ist ein höchstpersönliches Recht, auf welches nicht im Voraus verzichtet werden kann (Art. 25 Abs. 5 revDSG). Eine urteilsfähige Person kann und muss es selbst (oder einen in ihrem Auftrag handelnden Rechtsvertreter) geltend machen; bei nicht urteilsfähigen Kindern kann dies der gesetzliche Vertreter tun (z.B. Eltern, die prüfen wollen, ob die Daten ihrer Kinder von der Kinderkrippe richtig bearbeitet werden).

[116] Gewisse Verletzungen des Auskunftsrechts sind **strafbewehrt**. Sie müssen allerdings vorsätzlich erfolgen. Das Bussenrisiko trägt im Ergebnis derjenige, der über die Auskunft entscheidet, was auch eine subalterne Person sein kann. Bestraft wird der Auskunftserteilende aber nur, wenn er vorsätzlich eine falsche oder unvollständige Auskunft erteilt (wie im bisherigen Recht). Wer gar nicht reagiert oder zwar initial reagiert, sich aber zu Recht oder zu Unrecht auf den Standpunkt stellt, er müsse keine Auskunft erteilen, ist nicht strafbar, denn hier kann die betroffene Person bei Bedarf zivilrechtlich vorgehen[98]. Auch die Strafbarkeit bei unvollständiger Auskunft besteht nur, wenn vorsätzlich der Eindruck erweckt wird, sie sei vollständig[99]. Da es keine Pflicht zur Abgabe einer Vollständigkeitserklärung gibt, sollte darauf verzichtet werden.

2. Inhalt, Form und Zeitpunkt der Auskunft

[117] Jede natürliche Person kann mit dem Auskunftsrecht im Kern verlangen, dass der Verantwortliche ihr offenlegt, **ob er Personendaten von ihr bearbeitet und wenn ja, welche**. Weiter muss der Verantwortliche – auf Verlangen – die in Art. 25 Abs. 2 revDSG aufgelisteten Informationen liefern. Diese wurden an die DSGVO angepasst: Angaben zur Identität, Bearbeitungszwecke, Aufbewahrungsdauer (oder deren Kriterien), Datenquelle (soweit verfügbar), automatisierte

96 BBl 2017 7066 f.

97 BBl 2017 7066.

98 BBl 2017 7101.

99 BBl 2017 7101.

Einzelentscheide (und Logik), Kategorien von Empfängern (z.B. Behörden, Konzerngesellschaften; Namen müssen nicht genannt werden), Angaben zum Export analog Art. 19 Abs. 4 revDSG (N 96)[100]. Gewisse wenig sinnvolle Pflichtangaben sind weggefallen (Rechtsgrundlagen, Kategorien der Daten, beteiligte Personen). Das entspricht den Vorgaben der DSGVO, mit Ausnahme der dort noch erforderlichen Angaben über die Betroffenenrechte und das Beschwerderecht. Die Angaben zum Export der Daten unterscheiden sich inhaltlich von jenen, die nach DSGVO erforderlich sind.

[118] Von den Zusatzangaben werden in der Praxis vor allem jene zur Identität des Verantwortlichen und zur Aufbewahrungsdauer eine Herausforderung sein, auch wenn diesbezüglich keine absoluten Angaben nötig sind und nicht jede Ausnahme genannt werden muss. Um klare Aussagen «drücken» sich in diesen Punkten heute die meisten Datenschutzerklärungen, obwohl die DSGVO sie an sich fordert. Bei der **Identität des Verantwortlichen** wird das Hauptproblem darin bestehen, dass in vielen Fällen derjenigen Stelle, die die Auskunft erteilt, erfahrungsgemäss gar nicht klar ist, wer ausser dem «Haupt»-Verantwortlichen sonst noch als (gemeinsamer) Verantwortlicher gilt. Schon in der Datenschutzerklärung sind diese nicht zwingend anzugeben (N 99 ff.). Im Rahmen des Auskunftsrechts sind die Verantwortlichen dann anzugeben, wenn ein besonderer Anlass hierzu besteht, z.B. weil der Haupt-Verantwortliche im Ausland ist und die betroffene Person einen (allfälligen) Mit-Verantwortlichen im Inland möchte, um ihre Ansprüche einfacher durchsetzen zu können. Hier greift die **Generalklausel** in Art. 25 Abs. 2 revDSG, welche eine über die DSGVO hinausgehende Regelung darstellt: Falls für die Geltendmachung von Rechten im Bereich des Datenschutzes nötig, kann eine betroffene Person auch weitere, in Abs. 2 *nicht* aufgelistete Informationen verlangen[101]. Ein Beispiel kann die Auskunft darüber sein, wo bestimmte Betroffenenrechte geltend gemacht werden können oder wer bestimmte Personendaten erhalten hat[102]. Theoretisch können es auch Informationen sein, wie sie die DSGVO nicht vorsieht, so z.B. Angaben zu bestimmten Aspekten von Abreden mit anderen Verantwortlichen, mit denen Daten ausgetauscht werden. Über die gesetzlich vorgesehenen Mindestangaben hinausgehende Zusatzinformationen werden jedoch – analog zur entsprechenden Regelung in Art. 19 revDSG – die Ausnahme und zu begründen sein[103]. Es gibt jedenfalls keinen Hinweis, dass der Gesetzgeber mit dem erweiterten Auskunftsrecht quasi durch die Hintertür ein Auditrecht für betroffene Personen einführen wollte; dazu wäre der Geheimnisschutz des Verantwortlichen auch viel zu lückenhaft ausgestaltet. Verantwortliche werden zusätzliche Informationen zudem grundsätzlich nur auf spezifische Rückfrage liefern müssen. Dies entspricht einem Grundsatz, der sich in der Praxis freilich auch in anderen Fällen eingebürgert hat: Geliefert wird in einer ersten Antwort das, was die betroffenen Personen typischerweise interessiert. Wollen sie mehr, sollen sie spezifisch nachfragen[104].

---

100 Hier enthält der Text der Schlussabstimmung einen redaktionellen Fehler, der vermutlich noch bereinigt werden wird: Der Verweis auf «Artikel 19» wurde versehentlich gestrichen.

101 BBl 2017 7066.

102 Vgl. Art. 19 DSGVO.

103 Etwa durch konkrete Hinweise auf eine Verletzung ihrer Datenschutzrechte und Erläuterungen, warum sie ihre Rechte nur durch den Erhalt der Zusatzinformation im Rahmen des Auskunftsrechts (und nicht etwa im Rahmen der normalen zivilprozessualen Beweisbeschaffung) geltend machen kann. Kann sie das nicht, ist die die Auskunft nach DSG nicht «erforderlich».

104 Das gilt unabhängig von der Formulierung «In jedem Fall» in Art. 25 Abs. 2 revDSG, da dieser Absatz nur besagt, welches die Pflichtinformationen sind, die eine betroffene Person in jedem Fall verlangen kann; ohne Darlegung, warum sie es zur Geltendmachung ihrer Datenschutzrechte braucht.

[119] Bezüglich der **automatisierten Einzelentscheide** muss über die Logik des Resultats nicht im Detail informiert werden. Wie sich bereits unter der DSGVO zeigt, genügen relativ allgemeine Angaben. Bei einer automatisierten Kreditbeurteilung müsste beispielsweise darauf hingewiesen werden, dass ihr ein Scoring der Kreditwürdigkeit des Interessenten zugrunde gelegt wird und woher dieses stammt (z.B. falls es von einer Kreditauskunftei stammt) oder welche Art von Informationen dem Scoring mit welcher Gewichtung zugrunde liegen (z.B. Betreibungsdaten, Zahlungserfahrungen, etc.)[105]. Es muss auch über das Vorliegen einer automatisierten Einzelentscheidung als solche informiert werden. Dies bedeutet aber nicht, dass eine natürliche Person von einem Unternehmen die Herausgabe eines Katalogs aller automatisierten Einzelentscheidungen verlangen kann. Ein Verantwortlicher wird erstens nur über jene Auskunft erteilen müssen, welche die konkrete Person vernünftigerweise betreffen können und er kann zweitens verlangen, dass die Person präzisiert, um welche Bearbeitungsvorgänge es ihr geht (also z.B. bei einer Krankenkasse um die Bearbeitung von Leistungsansprüchen). Diese Einschränkung gilt für das Auskunftsrecht generell: Jedenfalls kann ein Verantwortlicher, wenn er *viele Daten über eine Person* bearbeitet, normalerweise verlangen, dass der Auskunftspflichtige sein **Auskunftsersuchen einschränkt**[106]. Dasselbe muss bei Verantwortlichen mit *vielen Datenbearbeitungen* gelten. Diese Einschränkungen ergeben sich originär aus Art. 25 revDSG und nicht erst aus den Ausnahmebestimmungen nach Art. 26 revDSG.

[120] Kern einer jeden Auskunft wird natürlich die **Aufstellung der bearbeiteten Personendaten** sein. Hier fügte das Parlament die Einschränkung «als solche» hinzu. Damit sollte verdeutlicht werden, dass nicht Dokumente, sondern nur Personendaten verlangt werden können. Das entspricht auch der Praxis des EuGH[107]. Nötig wurde die Präzisierung, weil viele Schweizer Gerichte – einschliesslich das Bundesgericht – die an sich schon bisher geltende Regelung missachtet haben und freizügig Rechtsbegehren stattgaben, welche die Edition von Unterlagen (z.B. E-Mails, Verträge, Berichte) verlangten[108] und nicht nur die Personendaten als solche (also z.B. gewisse in den E-Mails und Berichten enthaltenen Aussagen über eine Person). Das ist einer der Gründe für den grassierenden Missbrauch des Auskunftsrechts.

[121] Dies führt zur Frage, wo ein Personendatum aufhört: Hat eine Person einen Vertrag unterschrieben, ist dann der gesamte Vertrag ihr Personendatum oder nur ihre Unterschrift? Die Frage kann natürlich nicht pauschal beantwortet werden. Aufgrund der Zweckbestimmung des Auskunftsrechts (Abs. 2) wird vorliegend entscheidend sein, wie die Information genutzt wird. Wird sie nicht als Personendatum der betreffenden Person genutzt und besteht auch kein relevantes Risiko, dass dies geschehen wird, so wird die Information auch nicht dem Auskunftsrecht unterliegen. Der CEO, der einen Vertrag seiner Firma unterzeichnet hat, hat dies in seiner Eigenschaft als CEO getan. Den Vertragstext zu erfahren ist für die Geltendmachung seiner Datenschutzrechte in der Regel nicht erforderlich. Der Vertragstext braucht ihm daher nicht mitgeteilt zu werden.

105 BBl 2017 7067.

106 BBl 2017 7067 mit Verweis auf Erwägungsgrund 63 der DSGVO.

107 Urteil des EuGH vom 17. Juli 2014 (C-141/12 und C-372/12), in welchem der EuGH festhält, dass das Auskunftsrecht keinen Anspruch auf Überlassung einer Kopie des gesamten Dokuments gewährt, in welchem Personendaten vorkommen, auch wenn Teile davon geschwärzt werden. Auch den Begriff des Personendatums legt der EuGH darin eng aus. In der Sache versuchte eine betroffene Person die Herausgabe der Entwurfsschrift einer Entscheidung zu bewirken.

108 Vgl. etwa Entscheid des BGer vom 3. Juli 2015, 4A_506/2014, Sachverhalt B.

[122] In diesem Sinne schränkt die neue Generalklausel im Einleitungstext von Art. 25 Abs. 2 revDSG das Auskunftsrecht klar ein: Beim Auskunftsrecht geht es nur darum, einer betroffenen Person dabei zu helfen, ihre Datenschutzrechte (zumindest die einklagbaren Ansprüche) geltend machen zu können und eine (datenschutzrechtlich motivierte) Transparenz der Datenbearbeitung sicherzustellen (z.B. um einer Person die Wahl zu erlauben, ob sie Daten zur Verfügung stellen will oder nicht oder ihr zu ermöglichen – um ihres Seelenfriedens Willen – zu erfahren, über welche Daten ein Unternehmen über sie verfügt). Hingegen bezweckt das Auskunftsrecht nicht die Beweisbeschaffung zur Geltendmachung anderer Ansprüche.

[123] Auskunft muss **grundsätzlich kostenlos** erteilt werden, doch wird der Bundesrat in der Verordnung zum revidierten DSG Ausnahmen für unverhältnismässigen Aufwand vorsehen. Bisher waren die Ausnahmen nicht der Rede wert. Das Parlament hat die Frist zur Auskunftserteilung auf 30 Tage festgesetzt, doch sind hiervon – wie bisher – Ausnahmen möglich, die der Bundesrat wohl ebenfalls in der Verordnung definieren wird. Interessanterweise ist in Art. 25 revDSG nicht mehr vorgeschrieben, dass die Auskunft **schriftlich** erfolgen muss. Die DSGVO hingegen sieht vor, dass betroffene Personen eine Kopie der Personendaten verlangen können. Die neue Regelung könnte dazu führen, dass Verantwortliche bei heiklen oder zahlreichen Daten bestimmen werden, dass nur vor Ort Einsicht genommen werden kann. Hier werden der Verordnungsgeber oder die Rechtsprechung zeigen müssen, inwieweit zukünftig auch ohne explizite gesetzliche Regelung Kopien abgegeben werden müssen.

[124] Im Rahmen der Auskunftspflicht weiterhin zwingend ist (auch wenn es in Art. 25 revDSG nicht erwähnt wird) die zuverlässige **Identifikation** des Auskunftsersuchenden, was heute in der Regel mit einer ID-Kopie erfolgt (aber nicht zwingend muss)[109].

3. Einschränkung der Auskunftspflicht

[125] Bei den allgemeinen Einschränkungsgründen der Auskunftspflicht in Art. 26 revDSG hat der Gesetzgeber im Wesentlichen zwei Anpassungen vorgenommen. Zunächst wird abermals versucht, dem Missbrauch einen Riegel zu schieben: Die Auskunft kann nach Art. 26 Abs. 1 Bst. c revDSG verweigert oder zumindest eingeschränkt oder aufgeschoben werden, wenn das **Gesuch «offensichtlich» unbegründet oder querulatorisch** ist. Der letztere Fall ist der wohl einfachere. Er erfasst unter anderem solche Auskunftsersuche, die offenkundig dazu dienen, den Verantwortlichen zu plagen oder unnötig zu beüben (etwa durch Wiederholungen oder im Wissen um die Nutzlosigkeit der Auskünfte[110])[111]. Offensichtlich unbegründet sind Auskunftsersuchen dann, wenn sie nicht den in Art. 25 Abs. 2 revDSG erwähnten Zwecken dienen, d.h. nicht der Geltendmachung von Datenschutzrechten oder der datenschutzrechtlich motivierten Schaffung von Transparenz. Der Bundesrat war hier zu restriktiv, indem er in seinem Entwurf im Wesent-

109 Unter der DSGVO kann das Verlangen einer ID-Kopie, wo dies nicht zwingend nötig ist, sogar eine Verletzung der DSGVO darstellen.

110 BBl 2017 7069.

111 Internet-Services, mit denen ein Benutzer automatisiert und massenhaft Auskunftsersuchen an Firmen stellen kann, mit denen er nie etwas zu tun hatte, und wo es keine Anhaltspunkte gibt, dass sie über seine Personendaten verfügen, sind ein solches Beispiel. Hier sollte die neue Bestimmung es erlauben, solche Auskunftsersuchen serienmässig abzuweisen. Vgl. dazu David Rosenthal/David Vasella, Erste Erfahrungen mit der DSGVO, in: Digma, Dezember 2018, Heft 4 (http://www.rosenthal.ch/downloads/digma_2018_4_Rosenthal_Vasella.pdf [Stand 9. Oktober 2020]), S. 169, zu «One.Thing.Less», einem Anbieter für automatisierte Auskunftsersuchen aus der Schweiz.

lichen die bisherige Rechtsprechung festigte, welche das Vorschieben von Datenschutzgründen erlaubte[112]. Das Parlament wollte dem einen Riegel schieben: Offensichtlich unbegründet ist ein Auskunftsersuchen nach Art. 26 Abs. 2 Bst. c revDSG bereits dann, «wenn es einen datenschutzwidrigen Zweck verfolgt»[113]. Das ist ein Systemwechsel: Zur Annahme der Missbräuchlichkeit muss nicht mehr gezeigt werden, dass es keinem Datenschutzzweck dient (was praktisch unmöglich war), sondern es genügt zu zeigen, dass ein Auskunftsersuchen offensichtlich in relevanter Weise einem Zweck dient, der *nicht* den Datenschutz betrifft. Das dürfte z.B. der Fall sein, wenn ein Arbeitnehmer nach seiner angeblich ungerechtfertigten Entlassung durch seinen Anwalt, der ihn im arbeitsrechtlichen Streit vertritt, vom ehemaligen Arbeitgeber die Herausgabe aller ihn betreffenden E-Mails und Protokolle verlangt: Es ist offenkundig, dass es hier um die Begründung von arbeitsrechtlichen Ansprüchen geht. Auch der unbedachte bundesgerichtliche Leitentscheid BGE 138 III 425, der den Auftakt zu den Missbräuchen im Auskunftsrecht gab, müsste im Lichte des neuen Rechts gegenteilig entschieden werden.

[126] Die zweite Änderung betrifft (leider nur) eine Erleichterung in Konzernen. Das Parlament stritt darüber, ob ein privater Verantwortlicher die Auskunft bei überwiegenden eigenen Interessen immer entsprechend einschränken, aufschieben oder verweigern kann. Der Nationalrat wollte diese Lösung, da sie sachlogisch richtig wäre: Überwiegt ein Interesse objektiv betrachtet, gibt es an sich keinen Grund, diesem nicht den Vorzug zu geben. So geschieht es auch an anderen Stellen im DSG (Art. 17 Abs. 1 Bst. c Ziff. 1 revDSG, Art. 31 Abs. 1 revDSG). Der Ständerat konnte sich jedoch damit durchsetzen, dass die bisherige Lösung beibehalten wird: Eine Berufung auf **überwiegende eigene Interessen** (z.B. Geschäftsgeheimnisse, Angaben zur internen Meinungsbildung, übermässiger Aufwand) ist weiterhin nur möglich bei Personendaten, die der Verantwortliche (planmässig) keinem Dritten bekannt gibt. Die einzige Einschränkung dieser Regelung in Art. 26 Abs. 2 revDSG gegenüber heute ist, das klargestellt wurde, dass andere Konzerngesellschaften nicht als Dritte gelten (Abs. 3). Nicht als Dritte galten bisher zudem Auftragsbearbeiter und gemeinsame Verantwortliche. Hier ist das revidierte DSG somit schärfer als die DSGVO:

[127] Eine Bank kann sich beispielsweise nicht auf ein (an sich begründetes) Geschäftsgeheimnis berufen, falls sie die betreffenden Personendaten z.B. regelmässig der FINMA mitteilen muss, weil diese als Dritte gilt. Besonders problematisch ist der Entscheid des Parlaments, weil der Auskunftsersuchende aus dem Auskunftsrecht selbst nicht verpflichtet ist, die erhaltene Auskunft geheim zu halten. Es ist davon auszugehen, dass sich das Parlament dieser Folgen nicht bewusst war und es sich daher um ein Versehen handelt. Allerdings gibt es daran aufgrund der klaren Gesetzgebungshistorie wohl nichts zu rütteln. Mögliche Lösungen des Problems in der Praxis könnten sein, dass in solchen Fällen nur vor Ort Einsicht gewährt wird (falls die Verordnung dies zulassen wird) oder die Auskunft, gestützt auf die Regel, massiv beschränkt wird, so dass nur noch die Personendaten «als solche» mitgeteilt werden müssten. Denkbar ist auch, von einem

112 BBl 2017 7069, m.w.H.

113 Die Formulierung «datenschutz*widrig*» ist etwas unglücklich, aber angesichts der Motivation der Anpassung erscheint die Absicht des Gesetzgebers und der Sinn und Zweck der Regelung klar. Zu verlangen, dass ein Auskunftsersuchen nicht nur keinen Datenschutzzweck verfolgt, sondern einen Zweck, der dem Datenschutz entgegenwirkt, beraubt der Anpassung ihres Sinns. Ein Auskunftsersuchen würde dann dem Datenschutz entgegenwirken, wenn es zur Verletzung des Datenschutzes einer anderen Person führt. Dieser Fall ist aber bereits in Art. 26 Abs. 1 Bst. b revDSG abgedeckt.

datenschutzwidrigen Zweck zu sprechen, wenn es dem Auskunftsersuchenden darum geht, an Geschäftsgeheimnisse zu gelangen.

[128] Weiterhin wie bisher eingeschränkt, aufgeschoben oder verweigert werden kann die Auskunft, wenn eine gesetzliche Pflicht dies vorsieht oder überwiegende Interessen Dritter dies erfordern. Ersteres ist – wie jetzt ausdrücklich erwähnt wird – dann der Fall, wenn mit der Auskunftsverweigerung ein **Berufsgeheimnis** geschützt werden muss. Darauf kann sich beispielsweise der Anwalt berufen (obwohl er ja selbst Verantwortlicher und damit auskunftspflichtig wäre), nicht aber sein Klient. Der Klient (z.B. ein Konzern) muss ein überwiegendes eigenes Interesse geltend machen, was er aber wie erwähnt nicht kann, wenn er die Daten zum Beispiel einem anderen Verantwortlichen ausserhalb seines Konzerns mitteilt (z.B. einer Behörde oder einem Geschäftspartner).

[129] Will der Verantwortliche eine dieser Ausnahmen geltend machen, kann er von der betroffenen Person verlangen, dass sie ihr eigenes **Interesse an der Auskunft** darlegt[114]. Ansonsten muss sie ihr Auskunftsgesuch grundsätzlich nicht begründen und braucht auch keinen guten Grund. Neugier reicht, wie auch die Botschaft festhält[115]. Der Verantwortliche wiederum muss begründen, warum er die Auskunft verweigert, einschränkt oder aufschiebt. Er wird im Streitfall auch zeigen müssen, warum die von ihm gewählte «Beschneidung» der Auskunft (z.B. Schwärzung, Totalverweigerung) das mildeste Mittel sei.

C. Recht auf Datenherausgabe und -übertragung

[130] Das in Art. 28 f. revDSG neu vorgesehene **Recht auf Datenherausgabe und -übertragung** (auch bekannt als Recht auf «Datenportabilität») wurde erst im Rahmen der parlamentarischen Beratungen eingeführt. Materialien dazu gibt es nicht. Die Regelung ist derjenigen der DSGVO nachgebildet[116]. Es handelt sich nicht um Datenschutzrecht im eigentlichen Sinne, sondern dient dem **Konsumentenschutz** und soll dem Konsumenten die Verfügungsmacht über seine, einem Dienstleister gegebenen, Daten sichern, um sie anderswo nutzen zu können. In der DSGVO wurde sie wegen *Facebook* eingeführt, um den Onlinekonzern dazu zu zwingen, seinen Nutzern die bei ihm von ihnen gespeicherten Daten zu Beiträgen, Bildern, Followern, Freunden und Likes auf deren Verlangen hin herauszugeben, damit sie einfacher zur Konkurrenz wechseln können. Auf diese Weise – so die gut gemeinte Idee – würde Facebook gezwungen, weniger einseitige Datenschutzbestimmungen zu erlassen, weil sonst die Benutzer einfacher zur Konkurrenz wechseln könnten. Das mutet alles etwas naiv an: Es hat in der Praxis bisher nichts dergleichen bewirkt[117]. Aber die Regel existiert; sie gilt nicht nur für Facebook, sondern für alle und es muss damit gelebt werden.

[131] Rechtlich greift die neue Regel dort, wo ein Verantwortlicher eine Datenbearbeitung zum Abschluss oder zur Abwicklung eines Vertrags mit der betroffenen Person, oder gestützt auf eine Einwilligung von ihr, automatisiert bearbeitet. Was der Verantwortliche dabei an Personendaten

114 BGE 138 III 425, E. 5.4 f.; BGE 123 II 534, E. 2e.

115 BBl 2017 7069.

116 Art. 20 DSGVO.

117 Der für Benutzer in sozialen Medien oft wichtigste Grund zum Verbleiben auf einer Plattform – ihre Follower und Likes – können auch mit einem noch so weitgehenden Recht auf Datenherausgabe *nicht* mitgenommen werden.

von der betroffenen Person erhält (und zwar in seiner Eigenschaft als Verantwortlicher, nicht als Auftragsbearbeiter), muss er ihr jederzeit auf Verlangen hin kostenlos herausgeben, und zwar in **einem gängigen elektronischen Format**. Gemeint ist, aufgrund des Normzwecks, ein Format, welches das automatische Einlesen der Daten in ein Computersystem in strukturierter Form ermöglicht. Akzeptabel wären also ein «csv» oder ein XML-File, nicht jedoch eine PDF-Datei (es sei denn, es handle sich bei den Daten bereits um PDF-Dokumente). Die betroffene Person kann sogar verlangen, dass die Daten nicht ihr, sondern direkt einem anderen Verantwortlichen – also etwa dem Anbieter einer Konkurrenzdienstleistung – zugesendet werden; vorausgesetzt der Konkurrent erlaubt die Annahme solcher Daten. Letzteres ist aber keine Pflicht des Konkurrenten, d.h. es gibt nur eine Pflicht auf Datenherausgabe, nicht auch eine Pflicht auf Datenannahme. Sollte der Aufwand für die Herausgabe oder die Übertragung unverhältnismässig sein (für denjenigen, der die Daten liefert), so greift gegebenenfalls eine vom Bundesrat in der Verordnung noch vorzusehende Ausnahme. Allerdings dürften die Kosten für den Bau einer Datenexportfunktion in der Software des Verantwortlichen an sich grundsätzlich nicht relevant sein, denn die Datenherausgabe und -übertragung ist eine gesetzliche Pflicht – und der Verantwortliche hat seine Systeme von Anfang an so zu konzipieren, dass er ihr nachkommen kann (Art. 7 Abs. 1 und 2 revDSG).

[132] Die **Ausnahmen** von der Übertragungspflicht sind qua Verweis in Art. 29 Abs. 1 revDSG dieselben wie beim Auskunftsrecht, auch wenn es sich beim Recht auf Datenherausgabe und -übertragung – seiner Natur nach – um ein anderes Recht handelt. Das zeigt sich bezüglich der Relevanz der beiden Rechte: Anders als beim Auskunftsrecht, kann beim Übertragungsrecht faktisch nur der Kunde des Verantwortlichen Daten herausverlangen und überdies nur jene, die er dem Verantwortlichen selbst gegeben hat. Eine Berufung auf das Berufsgeheimnis oder auf andere gesetzliche Pflichten dürfte kaum ein Thema sein. Auch die Berufung auf überwiegende Interessen Dritter wird oft nicht greifen: Selbst wenn in den herauszugebenden Daten auch Personendaten Dritter enthalten sind – der Standardfall dieser Ausnahme – dürfte ihr Interesse regelmässig nicht überwiegen, handelt es sich doch per Definition um Daten, die der Verantwortliche vom Kunden selbst erhalten hat, d.h. um Daten, die der Kunde bereits kennt. Die überwiegenden Interessen des Verantwortlichen selbst dürften vor allem im Aufwand liegen, welche eine Datenherausgabe verursacht. Doch es ist zu erwarten, dass die Rechtsprechung diese – von gewissen Ausnahmefällen abgesehen – als unbeachtlich betrachten wird mit dem Argument, die Kostentragung der Herausgabe sei vom Gesetzgeber bereits geregelt. Das Interesse der Wahrung von Geschäftsgeheimnissen dürfte auch kaum greifen, soll die Datenherausgabepflicht doch gerade die Konkurrenz beleben. Zudem greift das Argument überwiegender Interessen nur, wenn der Verantwortliche die Daten keinen Dritten bekanntgibt, was jedoch in vielen Fällen der Fall sein wird (und dem Verantwortlichen folglich die Berufung auf überwiegende Interessen von vornherein verwehrt ist).

[133] Es bleibt schliesslich die Ausnahme der **offensichtlich missbräuchlichen oder querulatorischen** Nutzung. Während letzterer Fall wohl durchaus denkbar ist, bereitet der offensichtliche Missbrauch Mühe angesichts der Tatsache, dass die Datenherausgabe selbst einen datenschutzfremden Zweck verfolgt. Die Ausnahme muss daher so zu verstehen sein, dass die Datenherausgabe dann verweigert werden kann, wenn sie offensichtlich primär einem anderen als dem Normzweck dient (N 125). Wie beim Auskunftsrecht, muss auch im Zusammenhang mit dem Herausgaberecht begründet werden, warum die Datenherausgabe verweigert, eingeschränkt oder aufgeschoben wird.

[134] Welche Bedeutung diesem neuen Betroffenenrecht zukommt, ist daher auch nach zwei Jahren nach dem Inkrafttreten der DSGVO noch alles andere als klar. Die Wahrscheinlichkeit ist hoch, dass das Recht auf Datenportabilität aufgrund seiner Einschränkungen keine grosse Relevanz haben wird. Zunächst können nur Daten herausverlangt werden, die die betroffene Person dem Verantwortlichen «bekanntgegeben» hat. Immerhin erfasst dies gemäss der Legaldefinition[118] nicht nur die mitgeteilten, sondern auch die zugänglich gemachten Daten. Was hingegen aus Drittquellen stammt, ist nicht erfasst. Weiter können nur *Personen*daten herausverlangt werden und zwar nur die Eigenen. Ein klassischer Anwendungsfall neben Facebook ist z.B. der Musikstreaming-Dienst, auf welchem Benutzer ihre Playlists anlegen können. Sie können verlangen, dass die Playlists und Angaben – wie die Namen der Künstler, denen sie folgen – transferiert werden. Erfasst ist auch der Patient, der von einem Spital die von oder an ihm erhobenen medizinischen Daten in elektronischer Form herausverlangt, um sie anderweitig auswerten zu lassen oder um sie der Forschung zur Verfügung zu stellen. Die vom Patienten nicht selbst mitgeteilten Daten gelten als «bekanntgegeben», wenn er sich für die entsprechenden Messungen oder Beobachtungen zur Verfügung gestellt hat, und müssen ebenfalls herausgegeben werden.

[135] Wie aber steht es mit den E-Mails, die ein Mitarbeiter im Rahmen seiner beruflichen Tätigkeit auf dem Server seines Arbeitgebers gespeichert hat? Kann er diese nach seiner Kündigung mitnehmen, weil er sie bei seinem neuen Arbeitgeber oder in seiner eigenen Firma nutzen will? Die Herausgabe ist technisch nicht schwierig, es handelt sich um seine Personendaten und da sie planmässig Dritten bekanntgegeben werden, kann sich der ehemalige Arbeitgeber nicht auf überwiegende eigene Interessen (wie etwa den Schutz seiner Geschäftsgeheimnisse) berufen. Es könnte allenfalls argumentiert werden, dass eine Herausgabeforderung zweckwidrig wäre, weil es sich nicht um einen Konsumenten handelt, aber die Stichhaltigkeit dieses Arguments erscheint ungewiss[119]. Ebenso mangelt es der Berufung auf überwiegende Interessen Dritter an Stichhaltigkeit: Es würde dem betreffenden Mitarbeiter nichts gegeben, dass er vor seinem Austritt nicht schon hatte. Zur Einhaltung des Datenschutzes bleibt er auch nach seinem Austritt verpflichtet, jedenfalls sofern er in einem Land mit angemessenem Datenschutz lebt. Argumentiert werden könnte schliesslich, dass er mit seinen E-Mails mehr als nur seine Personendaten im engeren Sinn verlangt, nämlich den gesamten Inhalt seiner E-Mails. Im Falle von Art. 28 revDSG gilt jedoch die Beschränkung auf Personendaten «als solche» wie beim Auskunftsrecht nicht, und würde der Inhalt der Herausgabepflicht bezüglich der E-Mails so eng ausgelegt, erschiene auch die Pflicht zur Herausgabe des Inhalts einer Playlist fraglich. Solche absehbaren «*unintended consequences*» scheinen das Schweizer Parlament freilich genauso wenig abgeschreckt zu haben wie dasjenige der EU; in der Schweiz war die Einführung der Datenportabilität das Ergebnis eines politischen Zugeständnisses an die Ratslinke, die sich eine wesentliche Verschärfung des DSG wünschte.

[136] **Strafbewehrt** ist die Verletzung des Rechts auf Datenherausgabe übrigens nicht (auch nicht die vorsätzliche Lieferung unvollständiger oder falscher Daten). Da sie nicht dem Persönlichkeitsschutz dient, führt eine Verletzung auch nicht zur Rechtswidrigkeit der Datenbearbeitung, auf die sie sich bezieht. Durchgesetzt werden kann sie nur auf dem Zivilweg oder vom EDÖB mittels Verfügung.

---

118 Art. 5 Bst. e revDSG.

119 Deutlicher wäre die Zweckwidrigkeit wohl dort, wo der Mitarbeiter eines Unternehmens die Daten sämtlicher über seinen Badge registrierten Ein- und Austritte haben möchte. Es ist nicht ersichtlich, wie er diese Daten für den ursprünglichen Zweck der Daten weiter nutzen könnte oder durch die Herausgabe der Sinn und Zweck der Norm sonst verwirklicht werden könnte.

D. Berichtigungsrecht und «Recht auf Vergessen»

[137] Das bisher in Art. 5 Abs. 2 DSG festgehaltene Berichtigungsrecht wurde in Art. 32 revDSG verschoben, wo auch die klageweise Geltendmachung von Rechtsansprüchen abgedeckt werden. Hingegen findet sich das Widerspruchsrecht wie bisher in Art. 30 Abs. 2 Bst. b revDSG (und Art. 30 Abs. 3 revDSG; vgl. auch N 38).

[138] Das **Widerspruchsrecht** gab es schon bisher und wurde in der Revision nicht angepasst. Damit hatte die Schweiz allen Unkenrufen zum Trotz[120] schon seit je her auch ein «Recht auf Vergessen». Es gilt nicht absolut, sondern wird im privaten Bereich durch die Rechtfertigungsgründe von Art. 31 revDSG beschränkt. Anders als die DSGVO, welche zwischen sehr kompliziert ausgestalteten Widerspruchs-, Beschränkungs- und Löschrechten unterscheidet[121], ist die Schweizer Konzeption simpel und einfach: Die betroffene Person kann sich nicht nur gegen eine Bearbeitung ihrer Personendaten als Ganzes wehren (also die Einstellung der Bearbeitung oder die Löschung ihrer Daten verlangen), sondern auch gegen einzelne Aspekte oder Ausprägungen. Das gibt ihr wesentlich mehr Freiheiten und erlaubt sehr viel mehr Einzelfallgerechtigkeit, weil sich die Wirksamkeit des Widerspruchs im Falle eines Streits auf jene Aspekte einer Datenbearbeitung beschränken lassen, die sich nicht nach Art. 31 revDSG rechtfertigen lassen. Verlangt jemand z.B. die Löschung aller seiner Daten für alle Zwecke, kann sich der Verantwortliche darauf beschränken, die Daten lediglich für gewisse Zwecke zu löschen, wenn er für die Weiterbearbeitung für andere Zwecke gute Gründe (wie z.B. eine gesetzliche Pflicht) hat.

[139] Im Rahmen des **Berichtigungsrechts** kann verlangt werden, dass falsche Daten gelöscht oder korrigiert werden. Die Regelung hat es in sich, weshalb es erstaunt, dass sie im Parlament nicht wirklich diskutiert worden ist. Denn anders als beim Widerspruchsrecht gilt das Korrekturrecht dem Wortlaut nach wesentlich absoluter. Will sich ein Verantwortlicher gegen eine Berichtigungsforderung wehren, kann er nur die beiden in Art. 32 Abs. 1 revDSG aufgeführten Gründe geltend machen, nämlich dass das Gesetz die Änderung verbietet (z.B. bei Aufbewahrungsvorschriften) oder dass die Personendaten zu Archivzwecken im öffentlichen Interesse bearbeitet werden (was im privaten Bereich selten vorkommen wird). Die in Art. 31 revDSG aufgeführten Rechtfertigungsgründe greifen nicht[122], d.h. der Verantwortliche kann beispielsweise nicht geltend machen, dass die Anpassung viel zu aufwändig sei oder sonst ein überwiegendes Interesse daran bestehe, die falschen Daten so zu belassen, wie sie sind. Letzteres erscheint auf den ersten Blick zwar widersinnig, aber es ist dabei zu bedenken, dass eine Verletzung des Grundsatzes der Datenrichtigkeit nach Art. 6 Abs. 5 revDSG durchaus über Art. 31 revDSG gerechtfertigt werden kann. Mit anderen Worten: Der Gesetzgeber sieht vor, dass ein Verantwortlicher, wenn er gute Gründe hat, falsche Daten weiterhin bearbeiten darf, während derselbe Gesetzgeber ihn zwingt, diese Daten zu korrigieren, wenn die betroffene Person es verlangt. Man denke an den Fall, dass ein Kunde eines Unternehmens verlangt, dass sein falsch geschriebener Name nicht nur in der Kundenkartei korrigiert werde (was das Unternehmen sicher tun wird), sondern auch in allen Backups, welche dasselbe Unternehmen noch aufbewahrt (was das Unternehmen nach Art. 6 Abs. 5 revDSG i.V.m. Art. 31 revDSG nicht tun müsste, weil der Aufwand in keinem Verhältnis zum Nutzen steht und daher ein überwiegendes Interesse des Verantwortlichen begründet).

120 Vgl. etwa das Postulat NR 12.3152 von Jean Christophe Schwaab.

121 Art. 17, 18, 21 und 22 DSGVO.

122 BBl 2017 7076.

Nach dem Wortlaut von Art. 32 Abs. 1 revDSG soll die betroffene Person das Unternehmen trotzdem dazu zwingen können. Die Botschaft hält sogar fest, dass der Korrekturanspruch auch dann bestehen soll, wenn keine Persönlichkeitsverletzung vorliegt[123], der Datenschutz also gar nicht verletzt ist. Es darf bezweifelt werden, dass diese Aussage zu Ende gedacht – und ihre Folge wirklich gewollt – war.

[140] In der Praxis werden diese Fehlkonzeption und der Widerspruch im revidierten DSG auf zwei Wegen bereinigt werden müssen: *Erstens* wird sich der Verantwortliche auf **Rechtsmissbrauch** berufen können müssen, wenn die Ausübung des Korrekturrechts eine Schikane darstellt oder wenn sie so weit geht, dass sie nichtmehr ernsthaft dem Schutz der Persönlichkeit (Art. 1 revDSG) dient und damit zweckwidrig erfolgt. *Zweitens* wird die Frage der Datenrichtigkeit – entgegen dem, was die Botschaft suggeriert – nach dem in Art. 6 Abs. 5 revDSG vorgesehenen Grundsatz beurteilt werden müssen. Das entspricht auch der Regelung von Art. 16 DSGVO. Unrichtig sind Daten nach Art. 32 Abs. 1 revDSG demnach nur, wenn sie dies **im Hinblick auf den Zweck ihrer Bearbeitung** sind. Sinn und Zweck von Daten auf Backups ist es, den früheren Datenstand zu sichern, und zwar so, wie er war. Eine Korrektur kann daher nicht verlangt werden, solange sichergestellt wird, dass – im Falle einer etwaigen Wiederherstellung von Daten – die zwischenzeitlich im operativen System vorgenommenen Änderungen nachgeführt werden.

[141] Mit der Revision nicht verändert wurden die Möglichkeit, ein **Bestreitungsvermerk** zu verlangen, solange unklar ist, ob die Daten falsch sind (eine Schweizer Besonderheit) und der Anspruch, dass eine Korrektur, ein Bestreitungsvermerk, eine Löschung oder ein Bearbeitungsverbot Dritten mitgeteilt wird. Die Mitteilung an Dritte kann aber nur im Rahmen einer Klage verlangt werden. Hier geht die Schweiz weniger weit als Art. 19 DSGVO, wonach Berichtungen und Einschränkungen in der Bearbeitung auf Verlangen hin auch früheren **Empfängern der Daten mitgeteilt** werden muss. In der Schweiz gilt dies in dieser Form nicht.

IV. Flankierende Massnahmen

A. Verzeichnis der Bearbeitungstätigkeiten

[142] Künftig muss nach Art. 12 revDSG jeder private Verantwortliche und jeder Auftragsbearbeiter ein **Verzeichnis seiner Bearbeitungstätigkeiten** führen, d.h. es müssen für jede Bearbeitungstätigkeit die im Gesetz vorgesehenen Angaben verzeichnet werden. Diese Regelung wurde von der DSGVO übernommen[124]. Verzeichnisse, welche für die DSGVO erstellt wurden, können dementsprechend übernommen werden; ergänzt werden müssen diesbezüglich lediglich die Angaben bezüglich der Länder (oder Regionen; dazu N 96), in welche Personendaten exportiert werden (dazu zählen auch etwaige Staaten des EWR[125]) und etwaige Garantien, auf welche sich der Verantwortliche im Falle von unsicheren Drittstaaten abstützt[126]. Eine allgemeine Dokumentationspflicht analog zu Art. 5 Abs. 2 DSGVO kennt das revidierte DSG jedoch nicht; sie war im Vorentwurf noch vorgesehen, wurde dann aber fallengelassen. Immerhin kann eine solche Pflicht

123 BBl 2017 7076.

124 Art. 30 DSGVO.

125 Aus Sicht der DSGVO sind hingegen Exporte in andere EWR-Länder keine Exporte in Drittstaaten.

126 Art. 12 Abs. 2 Bst. g revDSG.

sich aus Art. 7 f. revDSG ergeben. Die in Art. 12 Abs. 5 revDSG vorgesehene **Ausnahme für KMU** dürfte aufgrund der restriktiven Voraussetzungen in der Praxis kaum eine Rolle spielen.

[143] Abgeschafft wurde hingegen die Registrierungspflicht für Datensammlungen nach Art. 11a DSG; sie fand in der Praxis ohnehin kaum Beachtung. Damit gibt es im revidierten DSG keine Bestimmungen mehr, wonach sich Verantwortliche bzw. ihre Datenbearbeitungen zu registrieren haben. Es bestehen für private Verantwortliche somit nur noch die fallabhängigen Meldepflichten im Bereich Bekanntgaben ins Ausland (N 65 ff.), Datenschutzberater (N 168 ff.), Vertreter ausländischer Verantwortlicher (N 172 f.) und Verletzungen der Datensicherheit (N 160 ff.) sowie die Konsultationspflicht des EDÖB im Falle von Vorhaben mit hohem Risiko nach erfolgter Datenschutz-Folgenabschätzung (N 148 ff.).

[144] Es gibt keine feste Regel, wie die Gesamtheit aller Datenbearbeitungen eines Betriebs für die Zwecke des Verzeichnisses aufgesplittet wird. Bewährt hat es sich, **sachlich zusammenhängende Bearbeitungen** zusammenzufassen, soweit sie über dasselbe datenschutzrechtliche Profil verfügen. Das Verzeichnis ist nicht Selbstzweck, sondern soll bei der Datenschutz-Compliance helfen und dem Verantwortlichen und Auftragsbearbeiter einen Überblick über die datenschutzrelevanten Aktivitäten in seinem Betrieb verschaffen. Untersucht der EDÖB einen Fall, wird er als erstes eben dieses Verzeichnis verlangen. Die Erfahrung mit der DSGVO zeigt, dass viele Verzeichnisse tendenziell zu detailliert sind. Beispiele für Bearbeitungstätigkeiten eines Verantwortlichen sind: Personaladministration, Rekrutierung, Kundendatenverwaltung, Kundendienst, Onlineshop, Newsletter, Produktentwicklung, Lieferantenverwaltung, Finanz- und Rechnungswesen, Website, Videoüberwachung, Gebäudemanagement, E-Mail-System, Rechtswesen und interne Untersuchungen.

[145] Eine **Formvorschrift** gibt es nicht; ein Excel oder Word-Dokument genügen ebenso, wie eine ausgefeilte IT-Lösung, wie sie einige Firmen anbieten. Das Verzeichnis kann dezentral geführt werden, wobei dessen Führung sogar delegiert werden kann (z.B. an einen Mitverantwortlichen oder einen Dienstleister). Das Verzeichnis muss aber *alle* Bearbeitungstätigkeiten enthalten und aktuell sein. Wird die Verzeichnispflicht verletzt, hat dies keine unmittelbaren Sanktionen zur Folge. Der EDÖB kann Einblick verlangen, nicht aber die betroffenen Personen. Sie können jedoch mittels Auskunftsrecht vergleichbare Informationen erhalten. Auch Datenschutzerklärungen enthalten häufig ähnliche Informationen, wie die Bearbeitungsverzeichnisse; sie werden auch oft zusammen erstellt.

[146] Das Verzeichnis enthält die **datenschutzrechtlich wesentlichen Eckwerte** der diversen Datenbearbeitungen, aber keine Personendaten und es ist auch kein Journal der Datenbearbeitungen. Was mindestens ins Verzeichnis gehört, zählen Art. 12 Abs. 2 und 3 revDSG auf. Mit der Identität des Verantwortlichen sind nicht die internen Verantwortlichen, sondern typischerweise die juristische Person gemeint. Bei mehreren Verantwortlichen sind alle aufzuführen. Der Bearbeitungszweck meint den Zweck, dem die Bearbeitungstätigkeit dient (z.B. Arbeitszeiterfassung, Lohnabrechnung, Kundenbetreuung, Beschaffung, Reisemanagement, etc.). Zweitnutzungen (z.B. über ein Datawarehouse) sind typischerweise eigene Bearbeitungstätigkeiten. Bei der Beschreibung der Kategorien von Personendaten kann zusammenfassend formuliert werden (z.B. Kontaktdaten, Bankdaten, Beurteilungen, Korrespondenz, E-Mails, Projektdokumente, Arbeitszeiten, Vertragsdaten). Dasselbe gilt für die betroffenen Personen (z.B. Kunden, Mitarbeiter) und die Empfänger (z.B. Gruppengesellschaften, Dienstleister, Behörden, Medien, Öffentlichkeit). Gemeinsame Verantwortliche sind gleichzeitig auch Empfänger. Die Aufbewahrungsdauer ist direkt (z.B. solange Kundenkonto besteht, zehn Jahre nach Vertragsende) oder mittels der sie

bestimmenden Kriterien anzugeben (z.B. handelsrechtliche Aufbewahrungsfristen, Interesse an Beweisführung, Legal Hold). Bezüglich der Datensicherheit empfiehlt es sich, auf die entsprechenden IT-Sicherheitsrichtlinien zu verweisen und gegebenenfalls das zu erwähnen, was über den Grundschutz hinausgeht. Bei Exporten aus der Schweiz sind die Empfangsländer anzugeben, wobei definierte Sammelbegriffe wie «Europa» oder «weltweit» genügen. Beispiele für die zu nennenden Garantien beim Export in unsichere Drittstaaten, sofern sie überhaupt vorkommen, sind «EU-Musterklauseln» oder «Binding Corporate Rules».

[147] **Auftragsbearbeiter** müssen auch ein Verzeichnis führen und darin unter anderem die Namen ihrer Kunden aufnehmen (wobei dies per Verweis auf die Kundendatenbank möglich ist und überdies gemeinsame Verantwortliche nicht erfasst werden müssen). Bei den Kategorien von Bearbeitungen genügen generische Umschreibungen (z.B. IT-Betriebsleistungen, Registrierung von Besuchern des Werkgeländes und Betrieb einer Versandstrasse).

B. Datenschutz-Folgenabschätzung

[148] Die Datenschutz-Folgenabschätzung – kurz «DSFA» – erfreut sich als Compliance-Instrument in den letzten Jahren einer wachsenden Beliebtheit. Sie ist bei heikleren Datenbearbeitungen heute das Mittel der Wahl, um eine solche aus Sicht der Datenschutz-Compliance zu validieren und rechtfertigen. Soll ein Projekt dem EDÖB zur Beurteilung vorgelegt werden, wünscht er sich bereits heute regelmässig eine DSFA. Im Kern geht es um eine **datenschutzrechtliche Selbstbeurteilung** von Vorhaben, die aus Sicht des Datenschutzes etwas heikler erscheinen. Sie ist neu in Art. 22 revDSG in gewissen Fällen vorgeschrieben.

[149] In einer DSFA wird zunächst das Vorhaben aus der Sicht der Datenbearbeitung beschrieben (welche Daten von wem wozu, wie und wo bearbeitet und gegebenenfalls weitergeben werden). Dann wird das «Risiko für die Persönlichkeit» analysiert und beschrieben. Die Botschaft bleibt diesbezüglich vage und abstrakt[127]. In der Praxis werden jedoch regelmässig nicht die Persönlichkeitsverletzungen als solche beurteilt, sondern es wird dargelegt, **welche negativen Folgen** die Datenbearbeitung für die betroffene Person mit einer gewissen Wahrscheinlichkeit haben könnte. Das können physische Auswirkungen (fehlerhafte Daten führen zu einer falschen medizinischen Behandlung; das Bekanntwerden von Daten zur politischen Gesinnung einer Person kann dazu führen, dass sie gestalkt oder bedroht wird; Angstzustände aufgrund Vertraulichkeitsverlust; etc.) oder materielle Auswirkungen (eine Person erhält einen Job nicht; es wird ihre Kreditkarte missbraucht; Erpressung; Verfälschung oder Verlust von Beweismitteln; ungerechtfertigte Gebühren; zusätzliche Aufwände, um Fehler zu bereinigen; etc.) oder immaterielle Auswirkungen sein (gesellschaftliche Nachteile; die «unheimliche Erfahrung» der Schädigung der Privatsphäre oder derartige Einschüchterung; dass betroffene Personen gewisse Dinge nicht mehr ausüben; etc.)[128].

[150] Schliesslich wird dargelegt, mit welchen bereits getroffenen und noch zu treffenden technischen und organisatorischen **Massnahmen diese negativen Auswirkungen verhindert** oder zumindest eingeschränkt werden können. Viele dieser Massnahmen werden bereits durch die

127 BBl 2017 7060.

128 Weitere Beispiele: Fraunhofer Institut für System- und Innovationsforschung ISI, Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, Ein Handbuch für die Praxis, Fraunhofer Verlag 2020, S. 39 ff. (abrufbar unter http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-5863941.pdf [Stand 9. Oktober 2020]).

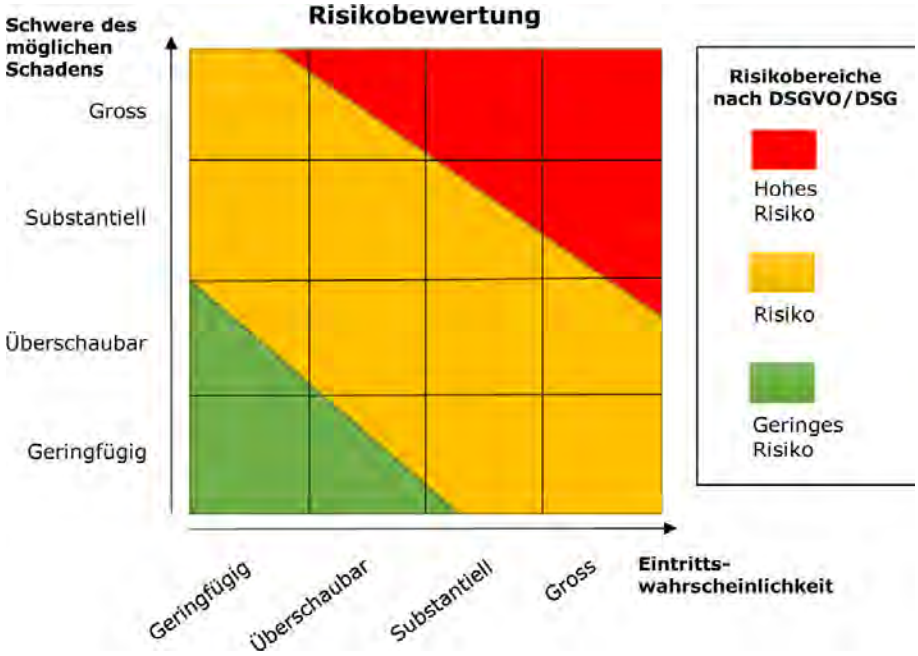
Einhaltung des DSG indiziert sein, wie zum Beispiel die Beschränkung des Zugangs zu den Daten auf einer «*need to know*»-Basis, die Beschränkung der Aufbewahrungsfrist, die Sicherstellung der Datensicherheit, die frühzeitige Pseudonymisierung, die Überprüfung von Daten auf ihre Richtigkeit, das Vier-Augen-Prinzip bei wichtigen Entscheiden, die klaren Vorschriften zur Datenbearbeitung sowie die Schulung des Personals und dessen Überwachung.

[151] In einem einfachen Fall (z.B. beim Aufstellen einer Überwachungskamera) kann eine DSFA sehr kurz und schematisch sein, während sie bei grösseren Vorhaben sehr komplex werden kann. Sie muss zudem nicht für jede Datenbearbeitung separat durchgeführt werden; eine DSFA kann für mehrere Vorhaben mit derselben Risikolage gemeinsam durchgeführt werden (z.B. eine DSFA für alle Sicherheitskameras, in welcher festgehalten wird, wo und wie Kameras aufgestellt werden sollen). Wenngleich die **«Rechtfertigung» einer Datenbearbeitung** formal nicht zum Mindestinhalt einer DSFA gehört, wird sie trotzdem häufig erforderlich sein, weil konzeptionell nur negative Wirkungen zu berücksichtigen sind, die ungewollt oder gar *ungerechtfertigt* sind. Im Beispiel der Sicherheitskamera: Für den Vandalen, der mit Hilfe ihrer Aufzeichnungen geschnappt wird, hat sie zwar eine negative Auswirkung, sie führt aber nicht zu einem hohen Risiko. Werden mit ihr jedoch unbescholtene Arbeitnehmer bezüglich ihres Verhaltens am Arbeitsplatz dauerbeobachtet, ist sie ein Problem. Umgekehrt liegt ein hohes Risiko nicht erst vor, wenn es tatsächlich zur Persönlichkeitsverletzung mit gravierenden Folgen kommt. Es genügt eine hinreichend hohe Eintrittswahrscheinlichkeit. Ob das hohe Risiko zur Unzulässigkeit der Datenbearbeitung führt, ist eine andere Frage, die im privaten Bereich nach den Voraussetzungen von Art. 6, 7, 16, 17, 30 und 31 revDSG beurteilt wird.

[152] Eine DSFA ist konzeptionell **vom Verantwortlichen selbst vorzunehmen**. Sie ist weder ein Audit, noch ein Datenschutz-Konformitätsgutachten durch einen Dritten. Der interne oder externe Datenschutzexperte kann trotzdem helfen: Während der Inhalt einer DSFA vom «Business» kommen muss, da es den Sachverhalt am besten kennt, sorgt der Experte dafür, dass die richtigen Fragen gestellt und die Erkenntnisse passend (d.h. aus der Optik des Datenschutzes) formuliert werden. Eine DSFA beinhaltet regelmässig auch eine Analyse der Einhaltung des DSG (oder der DSGVO, welche die DSFA auch kennt[129]).

[153] Eine DSFA beantwortet im Ergebnis die Frage, ob das Vorhaben trotz aller umgesetzten oder noch umzusetzenden Massnahmen ein **«hohes Risiko»** für die Persönlichkeit der betroffenen Personen mit sich bringt. Das Risiko ist dabei die Verknüpfung von Eintrittswahrscheinlichkeit und Schadensschwere (vgl. Grafik). Haben genügend schwere unerwünschte Folgen eine genügend hohe Eintrittswahrscheinlichkeit, ist von einem hohen Risiko auszugehen.

129 Art. 35 DSGVO.



[154] Erfahrungsgemäss werden die wenigsten Unternehmen nach Durchführung einer DSFA zum Schluss kommen, dass aller Massnahmen zum Trotz ein hohes Risiko vorliegt. Üblich ist, dass ein Vorhaben so gestaltet wird, dass die DSFA am Ende zum Ergebnis kommt, dass *kein* hohes Risiko (mehr) vorliegt und der Verantwortliche sich daher entscheidet, das Vorhaben umzusetzen oder weiterzuführen. Mit Bezug auf das Inkrafttreten des revidierten DSG gibt es keine Regel, wonach alle potenziell heiklen Datenbearbeitungen zum Inkrafttreten überprüft werden müssten. Eine DSFA sollte gemäss Daumenregel jedoch etwa alle drei Jahre wiederholt werden[130] oder wenn die Datenbearbeitung in wesentlichen Punkten angepasst wird oder sich die Umstände wesentlich geändert haben.

[155] Kann ein hohes Risiko wider Erwarten nicht wegdiskutiert werden, muss das Vorhaben **dem EDÖB zur Konsultation vorgelegt** werden, der es dann innerhalb von zwei oder ggf. sogar drei Monaten beurteilt und, sofern nötig, weitere Massnahmen oder den Abbruch der Übung vorschlägt (Art. 23 revDSG). Diese Pflicht zur Konsultation ist einer der Gründe, warum Unternehmen alles tun werden, um diesen Schritt zu vermeiden. Lässt sich das «hohe Risiko» nicht vermeiden, ist es daher wahrscheinlicher, dass sie einen sogenannten «Datenschutz-Berater» nach Art. 10 revDSG bestellen (N 168 ff.), der das Vorhaben anstelle des EDÖB beurteilt (Art. 23 Abs. 4 revDSG). Mit dem Datenschutz-Berater können wesentlich kürzere Fristen vereinbart werden und er wird unter Umständen auch weniger kritisch sein. Eine andere Möglichkeit, die DSFA selbst zu vermeiden, ist die Zertifizierung nach Art. 13 revDSG (was aber gemäss den bisherigen Erfahrungen mit Zertifizierungen kaum praxisrelevant sein wird) oder aber das Abstellen auf ei-

130 Empfehlung gemäss der Art. 29 Datenschutz-Gruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 «wahrscheinlich ein hohes Risiko mit sich bringt» (WP 248), Stand 4. April 2017, S. 12 (in der späteren Version vom 4. Oktober 2017 wurde dieser Hinweis allerdings gestrichen) (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 [Stand 9. Oktober 2020]).

nen vom EDÖB beurteilten Verhaltenskodex (N 175 ff.), was für gewisse Branchenanwendungen von Interesse sein könnte.

[156] Stellt sich somit die Frage, **wann eine DSFA vorgeschrieben** ist. Hier ist der Text von Art. 22 Abs. 1 und 2 revDSG nicht auf den ersten Blick verständlich, was an einer dogmatischen Fehlannahme liegt[131]. Eine DSFA ist zwingend, wenn eine Datenbearbeitung ihrer Natur nach ein hohes Risiko für die betroffene Person mit sich bringen kann[132]. Ob das Vorhaben ungeachtet der getroffenen oder noch zu treffenden Massnahmen tatsächlich ein hohes Risiko mit sich bringt, zeigt erst das Ergebnis der DSFA. In diesem Sinne zählt Abs. 2 lediglich zwei Fälle auf, in welchen ein solcher *Verdachtsfall* vorliegt (im Sinne einer Fiktion) und daher zwingend eine DSFA vorgenommen werden muss. Abs. 2 besagt jedoch entgegen dem Wortlaut *nicht*, dass die beiden Fälle – eine umfangreiche Bearbeitung besonders schützenswerter Personendaten oder eine systematische umfangreiche Überwachung öffentlicher Bereiche – *per se* ein besonders hohes Risiko mit sich bringen. Man denke an eine Datenbank mit zahlreichen öffentlichen Zitaten von Politikern (Daten über «politische Ansichten»): Sie erfordert zwar zwingend eine DSFA, aber sie wird grundsätzlich kein hohes Risiko mit sich bringen.

[157] Liegt keiner der beiden Fälle von Abs. 2 vor, muss anhand der Art und Weise der Datenbearbeitung beurteilt werden, ob sie – werden die zu treffenden Einschränkungen und weiteren Massnahmen weggedacht – ein hohes Risiko für die betroffenen Personen mit sich bringen kann (also das «Bruttorisiko» ermittelt wird, während das Ergebnis der DSFA das «Nettorisiko» ist). Mit anderen Worten: Eine DSFA ist nötig, wenn es um eine an sich aus Sicht des Datenschutzes ***heikle*** **Datenbearbeitung** geht. Die Artikel-29-Datenschutzgruppe der EU hat hierzu für das EU-Recht, welches mit Art. 35 DSGVO eine vergleichbare Regelung kennt, einen Katalog von Risikofaktoren entwickelt[133]. Liegen zwei der **Risikofaktoren** vor – so die Daumenregel – sollte eine DSFA durchgeführt werden. Zu diesen Risikofaktoren gehören: Systematische Überwachung, Bearbeitung von vertraulichen oder höchst persönlichen Daten, Bewertungen persönlicher Aspekte einer Person, umfangreiche Datenbearbeitungen, Abgleiche oder Zusammenführen von verschiedenen Datenquellen, innovative Nutzung von Technik, die Hinderung der Inanspruchnahme eine Dienstleistung oder des Abschlusses eines Vertrags, Bearbeitung von Daten schutzbedürftiger Personen und automatisierte Einzelentscheide. In der EU publizieren die Datenschutzbehörden jeweils weitere schwarze und weisse Listen mit Fällen, in denen *per se* eine DSFA durchgeführt oder nicht durchgeführt werden muss: In der Schweiz wird der EDÖB dies möglicherweise auch tun oder die Verordnung wird solches vorsehen.

[158] In der parlamentarischen Beratung wurde in Art. 22 Abs. 2 revDSG das **Profiling** gestrichen, weil es viele Profilings gibt, die nicht heikel sind. Was aber, wenn ein Profiling «mit hohem

131 Die Norm geht von der Annahme aus, dass Datenbearbeitungen vor einer DSFA noch keine Massnahmen zum Schutz der betroffenen Personen kennen und mit der DSFA die zu treffenden Massnahmen erst ermittelt werden. Entsprechend gibt es ein Risiko *vor* und eins *nach* der DSFA. Die Realität ist jedoch eine andere: Datenbearbeitungen werden heute – entsprechend Art. 7 revDSG – nicht selten von vorherein so konzipiert, dass die Risiken genügend klein sind. In diesen Fällen bestätigt eine DSFA lediglich, dass das Risiko nicht hoch ist. Durchgeführt werden muss sie trotzdem.

132 Genau genommen geht es um eine doppelte Wahrscheinlichkeit: Eine DSFA ist nötig, wenn es wahrscheinlich ist, dass es wahrscheinlich ist, dass die Datenbearbeitung eine schwere Folge für die betroffene Person hat (vgl. BBl 2017 7059, FN 150).

133 Empfehlungen gemäss der Art. 29 Datenschutz-Gruppe: Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 «wahrscheinlich ein hohes Risiko mit sich bringt» (WP248 rev. 01), Stand 4. Oktober 2017, S. 9 ff. (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 [Stand 9. Oktober 2020]).

Risiko» vorliegt? Hier ist zu differenzieren: Führt ein Profiling zu einem Persönlichkeitsprofil (N 24 ff.), so wird typischerweise eine DSFA gemacht werden müssen. Kommt diese aber zum Ergebnis, dass angesichts der Massnahmen kein hohes Risiko vorliegt, so gibt es zwei Möglichkeiten: Entweder muss konsequenterweise auch vom Fehlen eines Profiling «mit hohem Risiko» ausgegangen werden. Denn ein solches liegt gemäss einer Auslegung der Legaldefinition von Art. 5 Bst. g revDSG nach Wortlaut und Systematik nur dann vor, wenn der Umstand, dass ein Profiling zu einem Persönlichkeitsprofil führt, ein hohes Risiko für die betroffene Person mit sich bringt (N 27 f.). Ein computergeneriertes Persönlichkeitsprofil alleine genügt dann also nicht. Die Unternehmen werden also mit geeigneten Massnahmen alles daransetzen, dass ein Profiling «mit hohem Risiko» in der Praxis nicht vorkommt, weil sonst der EDÖB konsultiert oder an dessen Stelle ein Datenschutzberater bestellt werden müsste. Alternativ kann vertreten werden, dass zwar ein Profiling mit hohem Risiko vorliegt, sobald es zu einem Persönlichkeitsprofil führt, es aber nur Teil einer Datenbearbeitung ist, bei welcher dieses Risiko dank Massnahmen netto minimiert ist und daher ebenfalls keine Konsultation nötig ist.

[159] Die Verletzung der Pflicht zur Durchführung einer DSFA ist im revidierten DSG, anders als unter der DSGVO, **nicht mit einer Busse sanktioniert**. Sie kann von betroffenen Personen auch nicht eingeklagt werden. Nur der EDÖB kann ihre Durchführung anordnen.

C. Meldepflicht für Verletzungen der Datensicherheit

[160] Mit dem revidierten DSG wird in der Schweiz erstmals eine Pflicht zur Vornahme von sog. *Data Breach Notifications* eingeführt: Kommt es künftig zu einem Datenverlust, einer falsch versandten E-Mail oder einem anderen Datensicherheitsvorfall, muss dies neu unter Umständen **dem EDÖB gemeldet** werden. Die DSGVO kennt eine solche Meldepflicht schon[134] und sie führt auch bereits zu sehr vielen Meldungen[135]. Die Schweiz entschied sich zu einer etwas milderen Regelung, die aber trotzdem alle Betriebe zwingen wird, entsprechende Zuständigkeiten und Prozesse vorzusehen.

[161] Eine **Verletzung der Datensicherheit** liegt gemäss Art. 5 Bst. h revDSG im Wesentlichen dann vor, wenn im Rahmen einer Datenbearbeitung in unvorhergesehener Weise die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten[136] beeinträchtigt wird und dies dazu führt, dass Personendaten verloren gehen, gelöscht, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden. Das kann durch einen Hackerangriff von aussen oder einen ausländischen Behördenzugriff auf in der Cloud gespeicherte Daten ebenso verursacht sein, wie durch eine interne Fehlmanipulation, die dazu führt, dass vertrauliche Kundendaten dem falschen Kunden offengelegt, Personendaten wegen einer *Ransomware* oder einem Systemfehler verloren gehen oder ein Mitarbeiter mit fremden Personendaten weisungswidrig ein «eigenes Ding» dreht. Geht der Verantwortliche in seinen Vorhaben mit Bezug auf Personendaten jedoch schlicht zu weit, etwa indem er sie zweckentfremdet oder sie unverhältnismässig lange aufbewahrt, verletzt dies

134 Art. 33 f. DSGVO.

135 DLA Piper GDPR Data Breach Survey 2020, https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020 (Stand 9. Oktober 2020).

136 Diese drei Elemente sind das, was nach allgemeinem Verständnis unter «Sicherheit» verstanden wird.

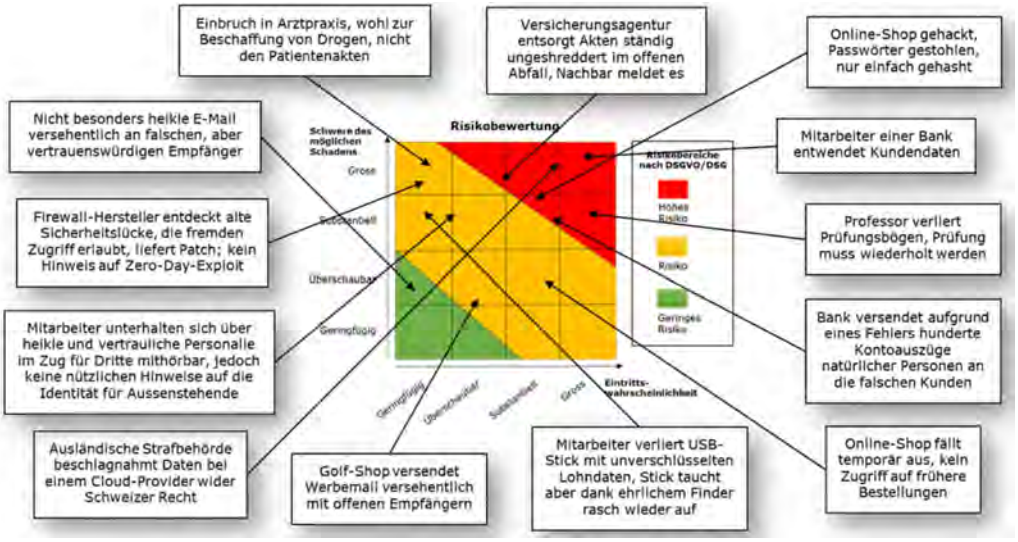
zwar den Datenschutz, doch ist dies keine Verletzung der Datensicherheit. Der Begriff entspricht demjenigen der DSGVO[137].

[162] Gemeldet werden müssen solche Verletzungen der Datensicherheit nur, wenn deswegen **ein «hohes Risiko» für negative Folgen** für die betroffene Person besteht. Natürlich ist hier eine Beurteilung im Einzelfall nötig. Aber als Daumenregel mag folgende Fragestellung helfen: Wie wahrscheinlich ist es, dass die Verletzung eine bestimmte negative Folge[138] für die betroffene Person mit sich bringt (wenig, mittel, sehr) und wie wäre diese negative Folge zu qualifizieren (leicht, mittelmässige, schwer)? Ist eine schwere negative Folge mindestens wahrscheinlich oder eine mittelmässige negative Folge sehr wahrscheinlich, ist das Risiko hoch.[139] Eine ***de-minimis*-Regel gibt es nicht**. Auch bei nur einer betroffenen Person kann eine Meldung erforderlich sein. Aber mit steigender Anzahl an potenziellen Opfern nimmt auch das Risiko erfahrungsgemäss zu. Art. 24 revDSG verlangt jedoch keine Spekulationen über das, was alles passieren könnte. Nur Gefahren, die aufgrund der konkreten Umstände und der allgemeinen Lebenserfahrung als realistisch und konkret erscheinen, kommen überhaupt in Betracht. Wird z.B. eine vertrauliche E-Mail versehentlich falsch versendet, aber der Empfänger ist bekannt und einigermassen vertrauenswürdig und anständig, so ist in der Regel nicht von einem hohen Risiko auszugehen. Ebenso wenig, wenn ein Notebook mit verschlüsselter Festplatte gestohlen wird. Verliert hingegen der Mitarbeiter einer mittelgrossen Firma auf der Strasse einen Memorystick mit den privaten Daten und Gehältern aller Mitarbeiter im Klartext und taucht er nicht mehr auf, so besteht wohl ein hohes Risiko für die Persönlichkeit der betroffenen Personen und eine Meldung ist erforderlich. Findet ein Unternehmen aufgrund des Hinweises eines Mitarbeiters heraus, dass für eine unbestimmte Zeit bestimmte heikle Mitarbeiterdaten für alle Mitarbeiter über einen versehentlich ungeschützten Unterordner der HR-Abteilung im internen Netzwerk zugänglich waren, so liegt in der Regel auch dann kein hohes Risiko vor, wenn keine Zugriffsprotokolle bestehen, sofern keine Hinweise auf einen Missbrauch vorliegen und – wie üblich – nicht davon ausgegangen werden muss, dass die Mitarbeiter ihr internes Netz nach solchen Datenlecks absuchen. Waren die Daten über das Internet zugänglich, ist die Wahrscheinlichkeit solcher Suchläufe viel höher. Und greift ein Hacker bewusst auf die Passwörter eines Online-Shops zu, muss auch dann von einem hohen Risiko ausgegangen werden, wenn die Passwörter zwar verschlüsselt sind, sich die simpleren Passwörter aber mit entsprechenden Hilfsmitteln knacken lassen. Hacker werden dies nach der allgemeinen Lebenserfahrung versuchen. Weitere Fälle (hier am Beispiel einer Schadens- und Wahrscheinlichkeitseinstufung mit jeweils vier Stufen, wobei nach DSG nur die Fälle im roten Bereich gemeldet werden müssen, während unter der DSGVO auch die Fälle im gelben Bereich zur Meldepflicht führen):

137 Art. 4 Ziff. 12 DSGVO.

138 Z.B. Rufschädigung, Blossstellung, Jobverlust, wirtschaftliche Einbusse, Diskriminierung oder körperliche Folgen.

139 Im Allgemeinen wird Risiko als Produkt aus Eintrittswahrscheinlichkeit und Schadenshöhe verstanden.



[163] Das «hohe Risiko» im Rahmen von Art. 24 revDSG unterscheidet sich vom «hohen Risiko» im Zusammenhang mit einer DSFA (N 153) dadurch, dass im ersteren Fall eine Verletzung der Datensicherheit tatsächlich vorliegt und nur deren Auswirkungen beurteilt werden, während im Rahmen einer DSFA beurteilt wird, wie wahrscheinlich eine Verletzung der Datensicherheit oder andere Umstände mit entsprechend schweren negativen Folgen für die betroffenen Personen ist. Die Methodik der Risikoberechnung (Eintrittswahrscheinlichkeit x Schadenshöhe) ist somit grundsätzlich dieselbe (und es kann daher für die Zwecke vom Art. 24 revDSG auch das Beurteilungsgitter in der vorstehenden Grafik verwendet werden), der Bezug jedoch ein anderer. Die Schwelle zur Annahme eines hohen Risikos ist bei der DSFA *tiefer*.

[164] Besteht eine Meldepflicht, so muss **dem EDÖB rasch möglichst Meldung erstattet** werden. Eine Frist von 72 Stunden, wie unter der DSGVO, gibt es nicht. Gemeldet werden muss, sobald die vom Gesetz vorgeschriebenen Mindestinformationen einigermassen beisammen sind: Was ist passiert? Wer und was ist betroffen? Und was sind die möglichen Folgen? Welche Massnahmen sind unternommen worden oder noch geplant, um die Datensicherheit wiederherzustellen und die Folgen für die Betroffenen zu verhindern oder abzumildern? Der Verantwortliche muss nicht in alle Details gehen; ist die Meldung nicht vollständig, weil noch Abklärungen laufen, ist dies kein Problem. Es geht einzig darum, dass der EDÖB beurteilen kann, ob der Verantwortliche die Situation *prima vista* so gut es geht im Griff hat und die nötigen Schritte unternimmt. Ist dies nicht der Fall, wird der EDÖB eingreifen müssen; reicht ihm die erste Meldung nicht, kann und wird er nachhaken. Besonders wichtig wird es sein, den EDÖB darüber zu informieren, ob eine Information der betroffenen Personen geplant ist. Entdeckt der Verantwortliche später ein neues hohes Risiko, wird er es nachmelden müssen. Keine Meldung ist nötig, wenn die betroffenen Personen ihr Desinteresse an einer Meldung erklärt haben. Dann liegt kein hohes Risiko mehr vor. Die primäre Verantwortung für den richtigen Umgang mit der Verletzung bleibt beim Verantwortlichen. Anders als unter der DSGVO muss er im Schweizer Recht allerdings keine Aufstellung der aufgetretenen Verletzungen der Datensicherheit führen.

[165] Die beschriebene Meldepflicht obliegt nur dem Verantwortlichen. Ein etwaiger **Auftragsbearbeiter** hat allerdings eine eigene Meldepflicht. Diese besteht gegenüber dem Verantwortlichen und geht viel weiter: Der Auftragsbearbeiter muss jede Verletzung der Datensicherheit,

die ihm zur Kenntnis gelangt, so rasch als möglich melden. Das gilt unabhängig davon, ob die Verletzung ein Risiko mit sich bringt. Das ist insofern unangenehm für Auftragsbearbeiter wie etwa IT-Provider, weil sie ihrem Kunden selbst folgenlose Verletzungen ihrer Pflichten rapportieren müssen und dies beispielsweise vertragsrechtliche Konsequenzen haben kann. Der Gesetzgeber wollte es dem Verantwortlichen überlassen zu beurteilen, ob allenfalls eine Meldung an den EDÖB erforderlich ist. Es handelt sich um eine *gesetzliche* Pflicht, d.h. selbst wenn sie vertraglich nicht vereinbart ist, muss der Auftragsbearbeiter sie erfüllen. Sie kann auch vertraglich nicht eingeschränkt werden. Die Einhaltung der Datensicherheit obliegt dem Auftragsbearbeiter notabene gesetzlich genauso wie dem Verantwortlichen.

[166] Art. 24 revDSG sieht auch eine **Information der betroffenen Person** vor, doch soll eine solche Information nur ausnahmsweise erforderlich sein[140]. Das Kriterium ist, ob die Information «zu ihrem Schutz erforderlich ist». Es geht nicht primär um Transparenz, sondern es soll dann informiert werden, wenn die betroffene Person *selbst* tätig werden muss, um sich vor den Folgen der Verletzung zu schützen oder diese abzumildern. Das kann z.B. das Wechseln des Passworts oder die Prüfung von Kontoauszügen oder – im Falle einer prominenten Person – die Vorbereitung auf Presseanfragen sein, nachdem pikante private Informationen über sie gestohlen und der Presse weitergegeben wurden. Wo hingegen der Schaden schon angerichtet oder die betroffene Person bereits im Bilde ist oder selbst nichts Relevantes tun kann, besteht keine Informationspflicht. Sie geht auch inhaltlich weniger weit als die Meldepflicht gegenüber dem EDÖB. Die Informationspflicht gibt der betroffenen Person kein Einsichtsrecht in den Vorfall und der Gesetzgeber hat diverse Ausnahmen vorgesehen; etwa wenn es unverhältnismässig aufwändig wäre, die zu informierenden Personen zu identifizieren oder ihnen die Information zukommen zu lassen. Anders als unter der DSGVO ist die öffentliche Bekanntmachung in solchen Fällen keine Pflicht. Allerdings kann sich der Verantwortliche der Informationspflicht nicht mit dem Argument entziehen, er wisse nicht genau, von welchen seiner Kunden die Daten gestohlen wurden. Eine Ausnahme von der Meldeplicht gegenüber der betroffenen Person ist immerhin für überwiegende Drittinteressen vorgesehen, was auch die Interessen der Behörden an einer ungestörten Untersuchung des Vorfalls sein können.

[167] Interessanterweise ist keine der vorgenannten Melde- und Informationspflichten mit **strafrechtlichen Sanktionen** bedroht; unter der DSGVO ist das anders. Die Motivation, jede relevante Verletzung der Datensicherheit tatsächlich zu melden, dürfte daher nicht sehr hoch sein. Das grösste Risiko dürfte dasjenige von Ansprüchen der betroffenen Person sein, wenn diese wegen einer zu spät oder unvollständig erfolgten Information nicht rechtzeitig agieren und sich dadurch nicht oder nicht vollumfänglich vor Schaden bewahren kann. Immerhin können sich aus dem Schweizer Recht noch andere Meldepflichten für Data Breaches ergeben (z.B. Art. 29 Abs. 2 FINMAG, «ad hoc»-Meldepflichten nach Börsenrecht).

D. Datenschutzberater

[168] Im revidierten DSG gibt es neu die Figur des **«Datenschutzberaters».** Sie ist in Art. 10 revDSG geregelt und ähnelt in ihrer Ausgestaltung an den «Datenschutzbeauftragten» gemäss Art. 37 ff. DSGVO. Für viele Experten ist die Regelung allerdings eine verpasste Chance, weil

140 BBl 2017 7065.

die Ernennung eines Datenschutzberaters weder Pflicht ist noch rechtlich praxisrelevante Vorteile bringt. Unter dem bisherigen Recht war es immerhin so, dass durch die Ernennung eines (in seiner Ausgestaltung vergleichbaren) «Datenschutzverantwortlichen» die Unternehmen nicht mehr verpflichtet waren, ihre ansonsten registrierpflichtigen Datensammlungen dem EDÖB zu melden[141].

[169] Der Gesetzgeber sieht im revidierten DSG nur **einen einzigen Anreiz zur Ernennung** eines Datenschutzberaters vor: Ein Datenbearbeitungsvorhaben, das trotz erfolgter DSFA und der Festlegung von Massnahmen noch ein «hohes Risiko» aufweist, muss nicht mehr dem EDÖB vorgelegt werden, wenn der Datenschutzberater es stattdessen prüft (Art. 23 Abs. 4 revDSG). Solche Fälle kommen aber erfahrungsgemäss kaum vor (N 154).

[170] Wer sich als Verantwortlicher trotzdem die Mühe macht, einen solchen Datenschutzberater zu ernennen, muss nach Art. 10 Abs. 2 und 3 revDSG **mehrere Voraussetzungen erfüllen**. Der Verantwortliche muss dem Datenschutzberater: die nötigen Mittel geben, damit dieser einerseits die Schulung und Beratung des Verantwortlichen in Fragen des Datenschutzes sicherstellen kann, er muss ihn in seine Prozesse zur Datenschutz-Compliance einbinden (oder sie ihm im Sinne einer «*second line of defence*»-Funktion übertragen), er muss dafür sorgen, dass er fachlich unabhängig und weisungsungebunden ist, er muss dafür sorgen, dass er keine Interessenkonflikte hat (d.h. der Datenschutzberater kann nicht parallel noch Funktionen ausüben, in denen er selbst über Datenbearbeitungen des Verantwortlichen entscheidet oder an diesen ein Interesse hat[142]) und der Verantwortliche muss selbst über das nötige Fachwissen verfügen (oder auf solches zurückgreifen können). In der Praxis dürfte der Datenschutzberater daher wohl ausser bei grösseren Unternehmen typischerweise ein externer Dienstleister sein, was – analog zur Regelung unter der DSGVO – zulässig ist. Interessenkonflikte lassen sich sonst kaum vermeiden. Auch ein **«Gruppen-Datenschutzbeauftragter»** eines Konzerns kann Datenschutzberater sein. Es gibt – anders als beim Vertreter (N 172 ff.) – keine Pflicht, dass dieser in der Schweiz sein muss. Wird ein Datenschutzberater ernannt, muss er dem EDÖB gemeldet und in der Datenschutzerklärung aufgeführt werden (mit Kontaktdaten; der Name der Person muss allerdings nicht genannt werden).

[171] Es ist zu erwarten, dass viele Unternehmen zwar eine oder mehrere Personen ernennen werden, die sich um Fragen des Datenschutzes kümmern werden, weil es nicht anders geht. Diese gelten jedoch nicht automatisch als Datenschutzberater und müssen daher auch nicht gemeldet werden. Auch die Anforderungen von Art. 10 revDSG gelten für sie nicht. Ohnehin wird die Verletzung von Art. 10 revDSG nicht sanktioniert. Denkbar ist höchstens, dass der EDÖB oder ein Gericht in einem konkreten Fall zum Schluss kommen, dass ein Unternehmen angesichts der konkreten Umstände zur angemessenen Wahrung des Datenschutzes eine für den Datenschutz zuständige Person hätte ernennen müssen, und dies gestützt auf Art. 7 f. revDSG anordnen. Solche Fälle dürften jedoch aussergewöhnlich sein.

141 Art. 11a DSG.

142 Vgl. etwa den Entscheid der belgischen Datenschutzaufsichtsbehörde vom 28. April 2020 (AH-2019-0013), wo der Datenschutzbeauftragte eine zweite Rolle als Compliance-Verantwortlicher hatte, in welcher Eigenschaft er selbst über die Bearbeitung von Daten bestimmte.

E. Schweizer Vertreter

[172] Erst vom Parlament eingeführt ist die Pflicht bestimmter ausländischer privater Verantwortlicher, einen **Vertreter in der Schweiz** zu benennen (Art. 14 f. revDSG). Die Regelung erscheint als eine Mischung von Art. 27 DSGVO (EU-Vertreter) und der Regelung in Art. 3 Abs. 2 DSGVO (extraterritoriale Geltung der DSGVO).

[173] Die Zahl der Unternehmen, die davon erfasst sind, dürfte klein sein. Einen Vertreter in der Schweiz ernennen müssen Verantwortliche mit Sitz oder Wohnsitz im Ausland nur, wenn sie (i) Personendaten von Personen in der Schweiz bearbeiten, (ii) sie diesen Personen Waren oder Dienstleistungen anbieten oder deren Verhalten in der Schweiz beobachten, (iii) eine Bearbeitung solcher Daten umfangreich ist und regelmässig stattfindet und (iv) die Bearbeitung ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich bringt. Bereits letzteres Kriterium werden die meisten Unternehmen als nicht erfüllt ansehen, so wie auch DSFAs in der Praxis regelmässig nicht zur Annahme eines hohen Risikos führen bzw. Datenbearbeitungen so lange angepasst werden, bis kein solches mehr vorliegt. Das zweite Kriterium entspricht weitgehend den Kriterien von Art. 3 Abs. 2 DSGVO und ist wohl auch in diesem Sinne auszulegen. Es braucht also entweder ein eigentliches *Targeting* mit Bezug auf Kunden in der Schweiz oder die Beobachtung muss zu einer eigentlichen Profilbildung bezüglich der betreffenden Person führen; die blosse Aufzeichnung von Zugriffen auf einen Online-Dienst oder eine Website genügt nicht. Im Ergebnis werden hier also Online-Anbieter wie Facebook oder Google erfasst, nicht aber der Betreiber eines ausländischen Online-Shops, der seine Daten für sich behält und die Benutzer für seine eigenen Marketingzwecke im üblichen Ausmass profiliert. Selbstverständlich steht es jedem Verantwortlichen offen, freiwillig einen Schweizer Vertreter zu benennen.

[174] Wird (in Erfüllung von Art. 14 revDSG) ein Vertreter benannt, muss er nicht nur **dem EDÖB gemeldet**, sondern auch in der Datenschutzerklärung aufgeführt werden (Art. 14 Abs. 2 und 3 revDSG). Er dient nicht nur den betroffenen Personen, sondern auch dem EDÖB als Ansprechpartner. Der Vertreter gilt rechtlich als Zustellungsbevollmächtigter. Das ist der Sinn und Zweck der Regelung, die es so übrigens auch in anderen Rechtsgebieten gibt[143]. Der Vertreter muss eine Kopie des Verzeichnisses gemäss Art. 12 revDSG führen und es dem EDÖB auf Verlangen hin offenlegen; für den freiwillig ernannten Vertreter gilt das allerdings nicht. Weitere Pflichten hat der Vertreter nicht. Er ist auch nicht für etwaige vom Verantwortlichen begangene Datenschutzverletzungen verantwortlich. Eine Sanktion für die Verletzung von Art. 14 f. revDSG gibt es auch keine.

F. Verhaltenskodizes

[175] Eine an sich vielversprechende Neuerung im revidierten DSG ist die Möglichkeit von **Verhaltenskodizes**. Sie ist in Art. 11 revDSG geregelt. Art. 40 DSGVO kennt eine ähnliche Regelung, die aber strenger und viel komplizierter ist. Leider hat es der Gesetzgeber auch hier verpasst, die nötigen Anreize für diese Form der Selbstregulierung zu schaffen. War im Vorentwurf noch vorgesehen, dass die Befolgung eines Verhaltenskodexes entsprechenden Rechtsschutz bietet, ist der rechtliche Anreiz neu weitgehend darauf beschränkt, in gewissen Fällen keine DSFA mehr durch-

143 Wie z.B. im Falle ausländischer Fernmeldedienstanbieter, die ab 2021 Schweizer Telefonnummern nutzen wollen.

führen zu müssen. Umgekehrt besteht freilich auch keine Pflicht, dem EDÖB Verhaltenskodizes vorzulegen, obwohl sich dieser das gewünscht hatte[144].

[176] Inhaltlich kann ein Verhaltenskodex («code of conduct») jeden Aspekt des DSG weiter ausführen und damit eine Hilfestellung in dessen Anwendung geben. Beispiele wären Ausführungen, wann ein «hohes Risiko» vorliegt, wie in einer bestimmten Branche hinreichend anonymisiert wird, Mustervorlagen für Datenschutzerklärungen oder DSFAs, eine Auflistung von über Art. 31 Abs. 2 revDSG hinausgehenden Fällen, in denen ein überwiegendes Interesse des Verantwortlichen vorliegt, Aufbewahrungsfristen für bestimmte Daten oder Regeln zur Sicherstellung eines Exports von Personendaten in ein Land ohne angemessenen Datenschutz. Ein Verhaltenskodex muss nicht umfassend sein; er kann sich auf einen Teilaspekt beziehen, was auch wesentlich einfacher zu erreichen sein dürfte. Er muss sich auch nicht auf das DSG beschränken. Er muss jedoch mindestens so streng und zusätzlich konkreter sein, als das DSG (und es nicht bloss wiederholen) und er darf nur die Kreise der Organisation betreffen, welche er dem EDÖB vorlegt. Aussenseiterbetriebe sind jedoch kein Hinderungsgrund.

[177] Ein Verhaltenskodex kann, muss aber nicht dem EDÖB vorgelegt werden. Zur Vorlage berechtigt sind Berufs-, Branche- oder Wirtschaftsverbände. Gemeint ist wohl, analog zu Art. 89 ZPO, jede Organisation, die statutengemäss zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt ist. Aktiengesellschaften und Stiftungen fehlt es hingegen an den Mitgliedern. Konsumentenorganisationen oder Vereine betroffener Personen sind hingegen nicht vorlageberechtigt.

[178] Wird dem EDÖB ein Verhaltenskodex vorgelegt, muss er dazu Stellung beziehen. Massstab ist dabei **einzig die Einhaltung des DSG** und nicht eine – vom EDÖB allenfalls erwünschte – Übererfüllung. Will er selbst eine Alternative vorschlagen, steht ihm dafür sein eigenes Instrument der «Empfehlung der guten Praxis» nach Art. 58 Abs. 1 Bst. g revDSG zur Verfügung. Seine Stellungnahme stellt keine Verfügung dar[145], sondern ein Realakt. Sie ist zu veröffentlichen. Inhaltlich stellt sie nur, aber immerhin, seine gegenwärtige Meinung dar; faktisch kommt ihr freilich erhebliches Gewicht zu. Ein Rechtsunterworfener wird mit der Umsetzung der Empfehlungen die Einhaltung des DSG dokumentieren und die Einhaltung seiner Sorgfaltspflichten nachweisen können. Ist ein Verhaltenskodex parallel als Standarddatenschutzklausel im Sinne von Art. 16 Abs. 2 Bst. d revDSG anerkannt, kann damit auch **der Export gerechtfertigt** werden. Die Einhaltung eines Verhaltenskodex bietet auch einen gewissen Vertrauensschutz gegenüber dem EDÖB, aber die Anforderungen an einen solchen sind sehr hoch und werden daher faktisch selten erfüllt sein (z.B. weil der Kodex nicht hinreichend konkret oder der Sachverhalt leicht anders gelagert ist oder weil sich die Rechts- oder Risikolage geändert hat).

G. Zertifizierungen

[179] Zertifizierungen fristeten schon unter dem heutigen DSG ein Schattendasein und dies dürfte sich trotz einer Erweiterung der Zertifizierungsmöglichkeiten unter Art. 13 revDSG nicht ändern. War es bisher nur möglich, Betriebe mit gewissen oder allen datenschutzrelevanten Abläufen und Massnahmen zu zertifizieren (das ist gemeint, wenn im revidierten DSG von «Systemen»

144 BBl 2017 7035.

145 BBl 2017 7035.

die Rede ist), können neu auch Produkte (namentlich Hard- und Software) und Dienstleistungen hinsichtlich ihrer **Konformität mit dem DSG** zertifiziert werden. In der Praxis spielt dies vor allem dort eine Rolle, wo Rechtsvorschriften eine Zertifizierung verlangen[146], dies im Rahmen von Ausschreibungen verlangt wird oder wo sich ein Anbieter davon verspricht, den eigenen Ruf fördern zu können. Eine generelle Pflicht zur Durchführung einer Zertifizierung, wie sie der EDÖB für Bearbeitungen mit hohem Risiko forderte, wollte der Bundesrat nicht, weil auch die DSGVO sie nicht verlangt[147].

[180] Lässt sich ein Betrieb zertifizieren, bedeutet dies, dass er über ein zur Einhaltung des DSG **angemessenes Datenschutzmanagementsystem** («DSMS») verfügt, d.h. über die zur Einhaltung des DSG nötige Governance. Es bedeutet aber nicht, dass die einzelnen Datenbearbeitungen gesetzeskonform erfolgen. Wie die Anforderungen an die Zertifizierung von Produkten und Dienstleistungen ausgestaltet sein wird, wird sich im Rahmen der noch zu erstellenden Verordnung zeigen. Aus einer Zertifizierung kann wiederum nicht geschlossen werden, dass der Einsatz dieser Produkte oder Dienstleistung automatisch datenschutzkonform ist. In der Praxis wesentlich wichtiger – von Art. 13 revDSG aber nicht erfasst – sind Zertifizierungen im Bereich der Datensicherheit (etwa nach dem ISO 27001-Standard), weil sich mit ihnen, unter gewissen Voraussetzungen, die Angemessenheit der zur Datensicherheit getroffenen Massnahmen dokumentieren lässt. Als Teil solcher Massnahmen, können ISO-Normen Gegenstand einer Zertifizierung nach Art. 13 revDSG sein.

V. Durchsetzung des DSG

A. Durch den EDÖB

[181] Aufgrund europarechtlicher Vorgaben völlig neu gestaltet wurde die Durchsetzung des DSG durch den EDÖB (auch) im privaten Bereich. Der EDÖB operiert nicht mehr mit «Empfehlungen» gegen einzelne Datenbearbeiter, was ihm weitgehende Freiheiten zur «Rosinenpickerei» gab. Neu muss er – wie jede andere Aufsichtsbehörde – ordentliche Verwaltungsverfahren durchführen und entsprechende **Verfügungen erlassen**, wenn er eingreifen will. Das gibt ihm zwar formell mehr «Macht», hat für ihn aber zugleich einen höheren Verfahrensaufwand zur Folge, d.h. für dieselben Resultate benötigt er künftig mehr Ressourcen. Daher ist auch verständlich, dass er sich – anders als seine EU-Amtskollegen – nicht auch noch die Kompetenz wünschte, fehlbare Verantwortliche und Auftragsbearbeiter büssen zu können. Diese Kompetenz (und folglich auch Arbeit) obliegt den Kantonen (N 192).

[182] Verstösse gegen die datenschutzrechtlichen Bestimmungen des DSG muss der EDÖB nach Art. 49 Abs. 1 revDSG künftig **von Amtes wegen** verfolgen. Anzeigen kann ihm solche jedermann; auch eine Meldung in der Presse kann genügen. Damit er nicht in Verfahren ertrinkt, kann er (im Sinne des Opportunitätsprinzips) bei Verletzungen «von geringfügiger Bedeutung» von der Eröffnung einer Untersuchung absehen (Abs. 2). Darauf wird er sich z.B. bei *Data-Breach*-Meldungen berufen, wenn klar ist, dass die Verletzung nicht gravierend ist oder der Verantwort-

146 Nach Art. 59a Abs. 6 der Verordnung über die Krankenversicherung (KVV; SR 832.102) muss jede Datenannahmestelle eines Krankengrundversicherers zertifiziert sein.

147 BBl 2017 7037.

liche sie im Griff hat[148]. Auch überall dort, wo er der Ansicht ist, dass entsprechende «Empfehlungen» an den Datenbearbeiter genügen, um den rechtmässigen Zustand wiederherzustellen, wird er sich auf die Möglichkeit des Verzichts auf eine Untersuchungseröffnung berufen können[149]. Formelle Verfahren kann er in solchen Fällen durch Aussprechen einer **«Verwarnung»** vorzeitig beenden (Art. 51 Abs. 5 revDSG). Dies dürfte der Regelfall werden und dazu beitragen, den Aufwand für alle Beteiligten gering zu halten. Hinzu kommt, dass er ein Verfahren nur dann eröffnen *muss*, wenn «genügend Anzeichen» für eine Datenschutzverletzung vorliegen (Art. 49 Abs. 1 revDSG). In der Botschaft war lediglich von «Anzeichen» die Rede. Dass der EDÖB nach Art. 49 Abs. 1 revDSG nur bei *Datenbearbeitungen*, die gegen Datenschutzvorschriften verstossen, ein Verfahren eröffnen kann, ist weit auszulegen: Auch wer flankierende Massnahmen und Betroffenenrechte verletzt, kann vom EDÖB untersucht werden.

[183] Eine Untersuchung wird sich zwar üblicherweise gegen einen Verantwortlichen oder Auftragsbearbeiter richten; ein Verfahren ist aber auch **gegen jede andere private Person** möglich. Die Formulierung von Art. 49 Abs. 1 revDSG ist diesbezüglich offen. Zu denken ist etwa an den Vertreter nach Art. 14 revDSG. Dritte kann der EDÖB nicht gestützt auf Art. 49 bzw. 50 revDSG zur Mitwirkung zwingen; sie unterliegen jedoch der allgemeinen Zeugnis- und Mitwirkungspflicht nach Art. 15 und 17 Verwaltungsverfahrensgesetz (VwVG)[150].

[184] Bis ein Untersuchungsverfahren eröffnet wird, müssen private Personen dem EDÖB keine Auskunft erteilen. Oft werden sie gut beraten sein, dies trotzdem zu tun, wenn sich eine Angelegenheit so in einem informellen Vorabverfahren klären lässt. Ist das Untersuchungsverfahren eröffnet, gilt das VwVG (Art. 52 Abs. 1 revDSG). Die **Informationsbeschaffung des EDÖB** ist dabei zweistufig geregelt:

> a) Auf einer ersten Stufe erfolgt sie durch blosse Anfrage: Die angefragten privaten Personen – das müssen nicht notwendigerweise Verantwortliche oder Auftragsbearbeiter sein – sind nach Art. 49 Abs. 3 revDSG zur **Mitwirkung** verpflichtet, unter Vorbehalt des Zeugnisverweigerungsrechts. Die Mitwirkung kann formlos verlangt werden. Zu mehr, als zu Auskünften und der Herausgabe von Unterlagen, ist eine Partei in diesem Stadium nicht verpflichtet.
>
> b) Gelingt oder genügt dies nicht, gibt Art. 50 revDSG dem EDÖB die Befugnis, sich die für die Untersuchung nötigen Informationen und Einblicke mittels **Zwangsmassnahmen** zu beschaffen; nötigenfalls unter Mitwirkung der Polizei. Eigentliche «Dawn Raids» – unangekündigte Hausdurchsuchungen – dürfte es keine geben: Die Befugnis zu Zwangsmassnahmen setzt voraus, dass der EDÖB die betreffenden Personen vorgängig erfolglos zur Mitwirkung angehalten hat (Art. 50 Abs. 1 revDSG).

148 Die Botschaft erwähnt selbst das harmlose Beispiel des Versands einer E-Mail mit offener Empfängerliste durch einen Verein an seine Mitglieder (BBl 2017 7090).

149 In diesem Sinne auch BBl 2017 7090.

150 Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG) vom 20. Dezember 1968, SR 172.021.

[185] Die Befugnis des EDÖB **vorsorgliche Massnahmen** zu verfügen, wurde im Parlament aus Art. 50 revDSG gestrichen[151]; das VwVG selbst sieht sie nur für das Beschwerdeverfahren vor. Die Lehre anerkennt die Möglichkeit deren Anordnung auch im Verwaltungsverfahren. Das muss auch vorliegend so gelten – die Streichung dürfte ein Versehen und kein qualifiziertes Schweigen sein.

[186] Hat der EDÖB eine Verletzung der datenschutzrechtlichen Bestimmungen des DSG festgestellt, kann er eine entsprechende Verfügung erlassen (muss es aber nicht). Tut er es, hat er in den Schranken der Verhältnismässigkeit weitgehende Kompetenzen: Er kann die Anpassung, den Unterbruch oder Abbruch einer Datenbearbeitung, die Löschung der bearbeiteten Personendaten sowie die Umsetzung der flankierenden Massnahmen und Betroffenenrechte verlangen (Art. 51 Abs. 1 und 2 revDSG). Da die **Kompetenz zum Erlass von Massnahmen** von der Verletzung der Datenschutzvorschriften abhängig ist, schränkt das DSG die Kompetenz auch entsprechend ein; d.h. der EDÖB kann nur verlangen, was das DSG auch ohne seine Anordnung erfordern würde. Er kann daher weder eine Auskunftserteilung anordnen, soweit Verweigerungsgründe gegeben sind, noch eine DSFA verlangen, falls die Voraussetzungen nach Art. 22 Abs. 1 und 2 revDSG nicht gegeben sind. Will er eine Konsultation nach Art. 23 revDSG oder die Benennung eines Schweizer Vertreters nach Art. 14 revDSG erzwingen, muss er feststellen, dass die betreffende Datenbearbeitung trotz der von Verantwortlichen ergriffenen Massnahmen ein hohes Risiko birgt bzw. die entsprechenden Voraussetzungen nach Art. 14 revDSG gegeben sind. Eine Besonderheit findet sich auf den ersten Blick in Art. 51 Abs. 2 revDSG: Diese Regelung erlaubt es dem EDÖB, eine Bekanntgabe von Personendaten ins Ausland auch gestützt auf Bestimmungen anderer Bundesgesetze zu untersagen. Allerdings muss es sich dabei ebenfalls um eine (auch) datenschutzrechtlich motivierte Bestimmung handeln[152].

[187] Wirkt eine Partei an einer Untersuchung des EDÖB vorsätzlich nicht, wie von ihm (zulässigerweise) verlangt, mit oder erteilt sie ihm vorsätzlich eine falsche Auskunft, so kann sie mit einer **Busse** von bis zu CHF 250'000 bestraft werden (Art. 60 Abs. 2 revDSG). Wird einer Anordnung nach Art. 50 revDSG (z.B. für den Zugang zu Räumlichkeiten) vorsätzlich nicht Folge geleistet, ist die Busse dieselbe (Art. 63 revDSG). Während nur Art. 63 revDSG die vorherige Androhung der Busse verlangt, muss dies analog auch für Art. 60 Abs. 2 revDSG gelten. Es ist nicht einzusehen, warum die Bussenhürde im Falle der Missachtung einer formlos verlangten Mitwirkung tiefer sein sollte als bei einer solchen, die per Verfügung angeordnet wird. Dieselbe Busse droht schliesslich auch bei Missachtung einer angeordneten Massnahme; dies bedeutet freilich, dass die Anordnung hinreichend präzis sein muss, so dass die kantonalen Strafverfolgungsbehörden feststellen können, ob sie eingehalten worden ist oder nicht. Die Busse richtet sich in Geschäftsbetrieben jeweils gegen die verantwortliche natürliche Person (N 191).

[188] Der Verfügungsadressat kann gegen die Verfügungen des EDÖB vor Bundesverwaltungsgericht **Beschwerde** führen und dessen Entscheid ans Bundesgericht weiterziehen; letzteres kann auch der EDÖB (Art. 52 Abs. 2 und 3 revDSG).

---

151 Nationalrat, AB 2019 N 1829 f.; Herbstsession 2019, 25. September 2019; vgl. gleichenorts: Mindermeinung von NR Minder, dass es dem EDÖB möglich sein müsse, vorsorgliche Massnahmen anzuordnen (AB 2019 N 1823); Es ist zu beachten, dass Art. 44 im Entwurf des Bundesrats zu Art. 50 im Revisionstext wurde.

152 Es muss sich um Normen handeln, welche die Bekanntgabe von *Personendaten* regeln, was zum Ausdruck bringt, dass es dem Gesetzgeber um Normen geht, welche eben solche und damit die Persönlichkeit der betroffenen Personen schützen sollen.

[189] Die betroffenen Personen, aber auch etwaige Dritte, haben keine Parteistellung. Erstere müssen etwaige Ansprüche auf dem Zivilweg geltend machen. Immerhin hat die betroffene Person – sofern sie Anzeige erstattet hat – ein Anspruch über die, gestützt auf die Anzeige, «unternommenen Schritte» und über das «Ergebnis» einer Untersuchung durch den EDÖB informiert zu werden (Art. 49 Abs. 4 revDSG). Ein Akteneinsichtsrecht ist das zwar nicht und andere betroffene Personen haben dieses Informationsrecht nicht. Der EDÖB hat es aber (unter Vorbehalt der Wahrung von Geschäftsgeheimnissen, dem Schutz der Persönlichkeit betroffener Personen und der Verhältnismässigkeit) weitgehend selbst in der Hand, wen er wie über seine Fälle informieren will. Kann er die Information nicht im Rahmen von Art. 49 Abs. 4 revDSG herausgeben, so kann er sich auf Art. 57 Abs. 2 revDSG berufen, der ihm die **Information der Öffentlichkeit** über seine «Feststellungen und Verfügungen» in Fällen von allgemeinem Interesse erlaubt. Diese Kompetenz hat er schon unter heutigem Recht grosszügig genutzt. Zu beachten ist weiter, dass der EDÖB nach abgeschlossenem Verfahren der Öffentlichkeit auch über das **Öffentlichkeitsgesetz** (BGÖ)[153] Zugang zu seinen Unterlagen gewähren kann und in der Regel auch umfassend gewähren wird. Es ist somit Vorsicht geboten, welche Unterlagen ihm im Rahmen einer Untersuchung offengelegt werden, soweit diesbezüglicher Spielraum besteht.

[190] Das revidierte DSG enthält neu auch **Amtshilfebestimmungen**, und zwar auch für das Ausland (Art. 55 revDSG). Der EDÖB kann seine Erkenntnisse somit neu auch mit ausländischen Datenschutzbehörden, etwa solchen im EWR, austauschen oder von diesen entsprechende Informationen entgegennehmen und für eigene Untersuchungen verwenden. Eine gegenseitige Vollstreckung von Zwangsmassnahmen ist jedoch nicht vorgesehen: Bussen oder sonstige Anordnungen von EU-Datenschutzbehörden können in der Schweiz somit weiterhin nicht vollstreckt werden. Der EDÖB müsste Bussen oder sonstige Anordnungen aus eigenem Recht erlassen, was im ersten Fall nicht geht. Was er immerhin tun kann, ist es den ausländischen Datenschutzbehörden zu erlauben, ihre Verfügungen selbst direkt in die Schweiz zu senden, ohne damit Art. 271 StGB zu verletzen (Art. 58 Abs. 3 revDSG).

B. Strafbestimmung

[191] Die Strafbestimmungen wurden im revidierten DSG deutlich ausgebaut: Einerseits sind nun wesentlich mehr Tatbestände strafbewehrt, andererseits wurde der Bussenrahmen von CHF 10'000 auf CHF 250'000 erhöht. Im Vorentwurf lag er noch bei CHF 500'000. Das mag im Vergleich zur DSGVO, welche einen Bussenrahmen von EUR 20 Millionen oder vier Prozent des weltweiten Umsatzes vorsieht, verschwindend klein erscheinen. Die Bussen gemäss der DSGVO richten sich jedoch gegen das jeweilige Unternehmen, die Schweizer Bussen hingegen **gegen die verantwortliche natürliche Person**[154]. Sie sind nach verbreiteter Auffassung weder versicherbar noch darf das Unternehmen sie für die natürliche Person bezahlen[155]. Das macht sie vom Prinzip

153 SR 152.3.

154 Begründet wurde dies damit, dass das Schweizer Verwaltungsverfahrensrecht noch nicht über die nötigen strafprozessualen Garantien verfügt, die bei mit der DSGVO vergleichbaren Verwaltungsbussen erforderlich wären (BBl 2017 7098 f.).

155 Vera Delnon/Bernhard Rüdy, in: Basler Kommentar, Strafgesetzbuch II, 4. Auflage, Art. 305 StGB, N 20, m.w.H.; gegen die Tatbestandsmässigkeit einer Vollstreckungsbegünstigung: Graf, Art. 305, N 9, in: Damian K. Graf (Hrsg.), Annotierter Kommentar StGB, 1. Auflage, Bern, 2020.

schärfer als die Bussen der DSGVO, denn kaum ein Arbeitnehmer wird bereit sein, für seinen Arbeitgeber ein solches Bussenrisiko einzugehen.

[192] In zweierlei Hinsicht steht die Schweiz allerdings deutlich hinter der DSGVO zurück: In der Schweiz wird nur die vorsätzliche Verletzung des DSG bestraft, der Katalog der Tatbestände ist ungleich kleiner als jener der DSGVO. Während fast jede Verletzung der DSGVO bussenbewehrt ist, gilt dies im revidierten DSG nur für einige wenige Bestimmungen. Die Verletzung der Bearbeitungsgrundsätze ist für sich ebenso wenig strafbar, wie die Verletzung der meisten flankierenden Massnahmen.

[193] Für die Durchsetzung der Strafbestimmungen sind zudem die **kantonalen Strafverfolgungsbehörden** zuständig (Art. 65 Abs. 1 revDSG), die bei datenschutzrechtlichen Fragen allerdings in der Regel keine Erfahrung haben. Der EDÖB kann zwar Anzeige erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen[156] (Art. 65 Abs. 2 revDSG), ein Strafantragsrecht hat er aber nicht – obwohl die meisten der Tatbestände Antragsdelikte sind. Es ist daher bereits heute davon auszugehen, dass die auf Strafbestimmungen von Art. 60 f. revDSG gestützten Bussen in der Schweiz die Ausnahme sein werden. Es ist jedoch ebenso davon auszugehen, dass die Bussen in Unternehmen – insbesondere im Management – für entsprechenden psychologischen Druck sorgen werden den Datenschutz einzuhalten.

[194] Unter Strafe gestellt sind gemäss Art. 60 revDSG – wie bisher – die vorsätzliche Verletzung der **Informationspflichten** nach Art. 19 und 21 revDSG und gewisse vorsätzliche Verstösse gegen das **Auskunftsrecht** in Art. 25 ff. revDSG durch private Personen. Zu den Einzelheiten vgl. N 92 und N 116. Die Busse beträgt neu auch hier bis zu CHF 250'000. Es ist davon auszugehen, dass die meisten Straffälle unter dem DSG das Auskunftsrecht betreffen werden, weil hier das Konfliktpotential zwischen Verantwortlichen und betroffenen Personen am grössten ist. Zweitplatziert dürften die Informationspflichten (von Konsumenten, die auf diese Weise gegen grössere Unternehmen vorzugehen versuchen) und Auslandstransfers (in strittigen Verhältnissen) sein. Strafantrag stellen können die konkret betroffenen Personen. Hierbei ist zwar zu beachten, dass ihr **Antragsrecht** drei Monate, nachdem ihnen der Täter bekannt wird, erlischt[157]. Da es sich beim Täter um eine natürliche Person handelt, die für die betreffende Information oder Auskunft verantwortlich war, und diese natürliche Person der betroffenen Person regelmässig nicht bekannt sein wird, wird die Antragsfrist in der Regel keine Rolle spielen.

[195] Die **verantwortliche Person** kann eine Leitungsperson sein (aufgrund ihrer gesetzlichen Verpflichtung, die Einhaltung des DSG im Unternehmen sicherzustellen[158]), muss es aber nicht. Auch wer kein Organ ist, aber trotzdem den relevanten Vorgang leitet, kann belangt werden[159], so etwa der betriebliche Datenschutzbeauftragte oder der externe Rechtsberater, der über die Datenschutzerklärung oder die zu erteilende Auskunft entscheidet. Will er sein Strafbarkeitsrisiko reduzieren, muss er heikle Entscheide seinen Vorgesetzten bzw. seinen Klienten überlassen, denn **Eventualvorsatz** genügt zur Strafbarkeit. Beim Eventualvorsatz hält der Täter den Deliktserfolg für möglich, nimmt diesen aber in Kauf; kein Eventualvorsatz sondern «bewusste Fahrlässigkeit» liegt hingegen vor, wenn er den Deliktserfolg zwar ebenfalls für möglich hält, aber darauf

156 Er kann also Einstellungsverfügungen anfechten und Rechtsmittel gegen kantonale Urteile ergreifen. Gegen Strafbefehle und das Strafmass soll er hingegen kein Rechtsmittel ergreifen können (BBl 2017 7104).

157 Art. 31 StGB.

158 BGE 142 IV 315, E. 2 ff.; Art. 29 StGB; Art. 6 Bundesgesetz über das Verwaltungsstrafrecht (VStrR; SR 313.0).

159 Art. 29 Bst. d StGB; Art. 6 Abs. 1 VStrR.

vertraut, dass er ausbleibt[160]. Entgegen den Beschwichtigungen in der Botschaft[161] dürfte die Strafbarkeit daher primär die ausführenden Stellen und nicht die Unternehmensleitung treffen. Sie wird sich erfahrungsgemäss mit den die Strafbarkeit begründenden Details der Informationspflicht oder einer Auskunftserteilung kaum je befassen.

[196] Auch die in Art. 64 revDSG vorgesehene Regelung, dass bei Bussen bis CHF 50'000, statt der natürlichen Person, der **Geschäftsbetrieb selbst gebüsst** werden kann, dürfte in manchen Fällen nicht greifen auch wenn die Bussen die Grenze von CHF 50'000 normalerweise nicht überschreiten werden: Die Regelung setzt voraus, dass sich die verantwortlichen Personen nur mit unverhältnismässigem Aufwand ermitteln lassen. Das wird bei den hier relevanten Delikten aber selten der Fall sein.

[197] Weiter definiert Art. 61 revDSG drei **«Sorgfaltspflichten»**, deren vorsätzliche Verletzung durch private Personen ebenfalls mit bis zu CHF 250'000 bestraft wird. Auch hier wird nur verfolgt, wenn betroffene Personen dies mit einem Strafantrag verlangen. Die drei Tatbestände sind: die Verletzung der Bestimmungen über die Bekanntgabe von Personendaten ins Ausland (Art. 16 f. revDSG), die Verletzung gewisser Vorgaben an den Verantwortlichen im Bereich der Auftragsbearbeitung (Art. 9 Abs. 1 und 2 revDSG) sowie die Missachtung der vom Bundesrat in der Verordnung noch festzuhaltenden Mindestvorgaben an die Datensicherheit (Art. 8 Abs. 3 revDSG). Weitere Ausführungen dazu finden sich in N 79, N 61 und N 53.

C. Zivilrechtlicher Klageweg

[198] Materiell keine nennenswerten Änderungen bringt die Revision des DSG im Bereich der **zivilrechtlichen Durchsetzung** von Ansprüchen durch die betroffenen Personen. Sie richten sich nach Art. 32 Abs. 2 revDSG, welcher wie bisher auf Art. 28 ff. ZGB verweist. Es können, wie bisher, Schadenersatz, Genugtuung und die Gewinnherausgabe verlangt werden; aber auch konkrete Massnahmen betreffend die Datenbearbeitung (wie deren vollständiges oder teilweises Verbot, das Verbot der Bekanntgabe von Personendaten an Dritte oder die Löschung oder Berichtigung von Personendaten).

[199] Wie bei arbeitsrechtlichen Streitigkeiten bis CHF 30'000, sollen künftig auch bei zivilrechtlichen Streitigkeiten nach DSG für das Schlichtungs- und Entscheidverfahren **keine Gerichtsgebühren** mehr erhoben werden (Art. 113 Abs. 2 Bst. g der revidierten Zivilprozessordnung [revZPO][162], Art. 114 Bst. g revZPO). Auch die Sicherstellung der Parteientschädigung ist nicht mehr erforderlich (Art. 99 Abs. 3 Bst. d revZPO).

160 Ist die Wahrscheinlichkeit des Delikterfolgs allerdings hinreichend gross und handelte der Täter trotzdem, gehen die Gerichte davon aus, dass der Täter gar nicht anders konnte als sich mit dem Erfolg abzufinden. Je grösser die Wahrscheinlichkeit der Tatbestandsverwirklichung ist und je schwerer die Sorgfaltspflichtverletzung wiegt, desto näher liegt die tatsächliche Schlussfolgerung, der Täter habe die Tatbestandsverwirklichung in Kauf genommen (BGE 130 IV 58).

161 BBl 2017 7099.

162 Vgl. dazu den Schlussabstimmungstext des revidierten DSG (N 4).

VI. Weitere Bestimmungen

A. Übergangsbestimmungen

[200] Relevante Übergangsbestimmungen hinsichtlich der neuen DSG-Pflichten für private Personen gibt es keine mehr. Das Parlament hat sie in den Beratungen weitgehend gestrichen. Übrig geblieben ist lediglich die Regelung, wonach Art. 7 revDSG (Privacy by Design, Privacy by Default) und Art. 22 und 23 revDSG (DSFA) nicht für Datenbearbeitungen gelten, mit denen schon vor Inkrafttreten des revidierten DSG begonnen wurde, soweit der Bearbeitungszweck unverändert bleibt und keine neuen Daten beschafft werden. Mit diesen Einschränkungen ist auch diese Übergangsbestimmung praktisch irrelevant.

[201] Das Fehlen einer Übergangsfrist dürfte mit einem Inkrafttreten erst im Jahre 2022 allerdings weitgehend ausgeglichen werden, denn fundamentale Anpassungen an den Datenbearbeitungen erfordert das revidierte DSG in den meisten Fällen nicht. Ausgebaut werden muss vor allem die Governance. Immerhin werden sich Unternehmen frühzeitig überlegen, ob und wie sie ihre AGB und Datenschutzerklärungen anpassen möchten, so im Hinblick auf das neue Berufsgeheimnis für jedermann (dazu sogleich), die angepassten Informationspflichten, den Datentransfer ins Ausland (auch vor dem Hintergrund von «Schrems II», N 74) und die Nennung bestimmter heikler Datenbearbeitungen. Im Bereich der Auftragsbearbeitungen werden viele Unternehmen davon profitieren, dass bereits im Rahmen der Einführung der DSGVO die dazu erforderlichen Verträge angepasst worden sind. Hier sind oft nur Retuschen erforderlich, aber immerhin erfordert auch dies eine Sichtung der Verträge.

B. Berufsgeheimnis für jedermann

[202] Eine der bemerkenswertesten Neuerungen im revidierten DSG ist der Ausbau der bisherigen Schweigepflicht zu einer allgemeinen **Schweigepflicht für alle Berufstätigen** (Art. 62 revDSG). Das bisherige DSG kannte zwar eine berufliche Schweigepflicht, doch war ihr Anwendungsbereich eng auf beruflich notwendige besonders schützenswerte Personendaten und Persönlichkeitsprofile begrenzt[163]. Neu wird auf Antrag derjenige mit bis zu CHF 250'000 statt wie bisher CHF 10'000 bestraft, der vorsätzlich geheime Personendaten von denen er bei der Ausübung seines Berufes, die solche Personendaten erfordert, offenbart. Auch Hilfspersonen und Auszubildende sind erfasst. Die Ausweitung der Schweigepflicht auf alle Arten von Personendaten begründete der Bundesrat unter anderem mit «der massenhaften Verbreitung von Smartphones»[164].

[203] Das «kleine Berufsgeheimnis» im DSG wurde auch terminologisch an das «grosse» Berufsgeheimnis von Art. 321 StGB und Bankgeheimnis (Art. 47 BankG) angenähert, indem neu (wie dort) von **«Offenbaren» als Tathandlung** die Rede ist. Gemeint ist damit die Preisgabe der betreffenden Daten an dazu unberufene Personen. Auch der Geheimnisbegriff ist derselbe wie in Art. 321 StGB[165]: Es muss sich um eine nicht allgemein bekannte Information handeln, an wel-

163 Art. 35 DSG.

164 BBl 2017 7102.

165 BBl 2017 7102.

cher der Geheimnisherr ein erkennbares, schutzwürdiges Geheimhaltungsinteresse hat[166]. Wer im Falle von Art. 62 revDSG als Geheimnisherr in Frage kommt, erschliesst sich nicht unmittelbar und wird auch in der Botschaft nicht thematisiert. Aus dem Sinn und Zweck der Norm sowie ihrer vom Gesetzgeber gesuchten Nähe zu Art. 321 StGB muss es sich, gleich wie in Art. 321 StGB, um die Person handeln, welche das Geheimnis dem Berufstätigen zur Durchführung seines Berufs anvertraut hat. Mit anderen Worten: Wie im Falle von Art. 321 StGB das Vertrauen geschützt wird, welches der Mandant etwa seinem Anwalt entgegenbringt, wenn er ihm geheime Informationen anvertraut, so soll gemäss Art. 62 revDSG der Kunde in seinem Vertrauen gegenüber seinem Dienstleister geschützt werden, dem er geheime Personendaten bekanntgibt. Art. 62 revDSG ist daher im Kern keine datenschutzrechtliche Norm, auch wenn sie nur für *Personen*daten gilt und sie sich im DSG befindet. Dieser Schluss ist zwar nicht selbstverständlich, aber entscheidend: Wenn darüber bestimmt wird, wessen Einwilligung der Berufstätige einholen muss, damit er die geheimen Personendaten einem Dritten offenlegen darf, so ist dies nur der Kunde, d.h. die Person, die ihm die Personendaten als Geheimnis anvertraut hat. Auch in diesem Punkt verweist die Botschaft auf Art. 321 StGB[167].

[204] Würde Art. 62 revDSG hingegen als datenschutzrechtliche Norm qualifiziert, hätte dies mitunter zur Folge, dass jede betroffene(n) Person(en) in die Offenlegung ihrer Daten einwilligen müsste oder sich die Zulässigkeit einer Bekanntgabe aus den Grundsätzen des DSG ergeben müsste: Bestünde ein überwiegendes Interesse an der Offenlegung, könnten selbst geheime Informationen preisgegeben werden. Die Einwilligung des Kunden würde umgekehrt nicht genügen, wenn die Informationen auch andere Personen betreffen würden. Die Verletzung der Bearbeitungsgrundsätze würde in diesen Fällen durch die Hintertür strafrechtlich sanktioniert, obwohl zwischen diesen Dritten und der berufstätigen Person kein Vertrauensverhältnis besteht und er sie oft nicht einmal fragen kann (und darf). Ein Rechtsberater könnte somit wegen Verletzung der beruflichen Schweigepflicht bestraft werden, wenn er zwar im Auftrag seines Klienten, aber gegen den Willen seiner Gegenpartei, deren Personendaten bekanntgibt[168]. Es ist nicht anzunehmen, dass dies der Absicht des Gesetzgebers entspricht. Die umgekehrte Aussage, dass nach Art. 62 revDSG nicht verfolgt werden kann, wer eine datenschutzrechtlich *zulässige* Bekanntgabe vornimmt, stimmt daher in dieser Form nicht uneingeschränkt, auch wenn in der Praxis kaum Fälle denkbar sind, wo sie im Ergebnis nicht zutreffend wäre, weil auch das DSG im Ergebnis das Vertrauen des Geheimnisherrn jedenfalls bezüglich seiner Daten schützt[169].

[205] Art. 62 revDSG ist, anders als Art. 321 StGB, kein Sonderdelikt mehr: Der beruflichen Schweigepflicht unterliegt ***jede* berufstätige Person**, welche Personendaten erfährt, die sie für ihren Beruf braucht. Das ist extrem breit und eine – auch im internationalen Vergleich – ungewöhnlich scharfe Regelung. Zwar waren Arbeitnehmer nach Art. 321a Abs. 4 OR schon bisher zur

166 Niklaus Oberholzer, in: Basler Kommentar, Strafgesetzbuch II, 4. Auflage, Art. 321 StGB, N 14.

167 BBl 2017 7102, wonach die allgemeinen Regeln und die im Rahmen von Art. 321 Ziff. 2 StGB von der Rechtsprechung und Dogmatik entwickelten Grundsätze sinngemäss gelten sollen. Dies würde bedeuten, dass neben der Einwilligung des Berechtigten auch eine Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde die Preisgabe erlauben würde. Welche Behörde das sein soll, lässt dies Botschaft jedoch offen.

168 Für das Beispiel wurde ein Nicht-Anwalt gewählt, der nicht unter Art. 321 StGB fällt, womit sich die Frage der Konkurrenz der beiden Normen nicht stellt. Da Art. 321 StGB aber ohnehin nur den Klienten bzw. das Vertrauen in den Anwalt schützt und nicht die Gegenpartei, könnte das Beispiel auch mit einem Rechtsanwalt vertreten werden.

169 Hypothetisch wäre dies ein Fall, wo der Klient des Schweigepflichtigen eine Bekanntgabe untersagt, sie aber aufgrund überwiegender Interessen trotzdem datenschutzrechtlich als gerechtfertigt erscheint. Dieses Interesse müsste wohl so gross sein, dass es auch im Rahmen von Art. 321 StGB als übergesetzlicher Rechtfertigungsgrund gelten könnte.

Geheimhaltung verpflichtet, doch schützte dies die Geschäfts- und Fabrikationsgeheimnisse des *Arbeitgebers* und nicht die Geheimisse dessen Kunden – oder höchstens mittelbar. Neu sind sie auch gegenüber den Kunden des Arbeitgebers zur Wahrung beruflicher Geheimnisse verpflichtet.

[206] Die Tragweite dieser Regelung ist noch nicht genau absehbar. Branchen, die zwar regelmässig mit vertraulichen Informationen umgehen, aber bisher keinem Berufsgeheimnis unterlagen, werden hierzu möglicherweise ihre Allgemeinen Geschäftsbedingungen anpassen wollen, um ein Risiko der Strafbarkeit zu vermeiden, wenn Kundendaten zwar nicht breit gestreut, aber trotz allem mit Dritten ausgetauscht werden. Das kann einen Privatversicherer ebenso treffen wie der Betreiber eines Onlineshops; beide unterlagen bisher grundsätzlich keiner strafrechtlich sanktionierten Schweigepflicht. Allerdings ist hierbei auch zu beachten, dass nicht jede Information, die ein Unternehmen von seinem Kunden erhält, tatsächlich auch als geheim zu qualifizieren ist. Hinzu kommt, dass selbst im Falle von an sich geheimen Informationen zu differenzieren ist, wer zum Kreis derjenigen gehört, denen die Information trotz allem mitgeteilt werden darf: Während ein Versicherer die Akten zu einem Schadenfall eines Kunden zweifellos nicht auf seiner Website publizieren darf, wird deren Offenlegung gegenüber etwaigen Mitversicherern selbst dann keine strafbare Offenbarung darstellen, wenn die Versicherungsbedingungen hierzu keinen ausdrücklichen *Waiver* vorsehen. In solchen Fällen steht der Bekanntgabe erstens in aller Regel kein schutzwürdiges Interesse entgegen und zweitens wird der Einbezug von Mitversicherern normalerweise mindestens implizit mitvereinbart sein – und damit auch die Erlaubnis, diesen die nötigen Informationen mitzuteilen. Wie im Falle von Art. 321 StGB, kann auch hier die Schweigepflicht nur soweit gehen, wie es sich aus dem Verhältnis zwischen dem Geheimnisherrn und Geheimnisträger ergibt. Zur Risikoreduktion wird auch beitragen, auf Datenbekanntgaben in Datenschutzerklärungen hinzuweisen; das mag zwar technisch nicht unbedingt einen Waiver begründen, doch kann der Umstand, dass ein Kunde dem Dienstleister Daten im Wissen um deren geplante Verwendung anvertraute das erkennbare Geheimhaltungsinteresse bezüglich einer solchen Verwendung tangieren. Ohnehin gilt, dass jeder Austausch, der für die Vertragsabwicklung nötig oder sonst vertraglich vorgesehen ist, auch ohne Freizeichnung nach Art. 62 revDSG erlaubt sein muss. Erfüllt eine Datenbekanntgabe diese Kriterien zwar nicht, aber muss dem Kunden klar sein, dass sie stattfindet und vertraut er seine Daten seinem Dienstleister trotzdem an, liegt kein Vertrauensbruch bzw. diesbezüglich kein Geheimhaltungsinteresse und somit abermals keine Verletzung von Art. 62 revDSG vor. Wer sich absichern möchte, kann in seinen AGB den Verweis auf die Datenschutzerklärung um den Hinweis ergänzen, dass er sich die dort vorgesehenen Datenbekanntgaben vorbehält[170]. Die Ungewöhnlichkeitsregel und Unklarheitenregel sind trotzdem zu beachten. Ein solcher Vorbehalt ist also kein Freipass. Je sensibler die Daten sind, desto mehr muss vorgekehrt werden.

C. Identitätsdiebstahl

[207] In Erfüllung einer vom Parlament angenommenen Motion[171] wurde die Revision des DSG auch zur Einführung eines neuen Straftatbestands gegen Identitätsdiebstahl benutzt. Nach

[170] Beispiel: «Weitere Angaben zum Datenschutz, einschliesslich der Datenbekanntgaben, die wir uns vorbehalten, finden Sie in der Datenschutzerklärung unter [link].».

[171] SR Comte, Motion vom 21. März 2014, Nr. 14.3288.

Art. 179^{decies} des revidierten Strafgesetzbuches (revStGB)[172] wird neu auf Antrag mit Freiheitsstrafe bis zu einem Jahr Geldstrafe bestraft, wer die **Identität einer anderen Person ohne deren Einwilligung verwendet**, um dieser zu schaden oder um sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen. Die Tragweite der Norm ist sehr breit: Die «Identität» einer Person meint nicht nur deren Namen, sondern auch andere Merkmale wie deren Bild, deren Kontonummer, deren Benutzername oder *Nickname*, deren Internetadresse oder auch die Kombination von Merkmalen, die eine bestimmte Person identifizierbar machen[173]. Erfasst wird also etwa derjenige, der ein fremdes Online-Konto benutzt; ebenso wie derjenige, der ein solches unter fremdem Namen einrichtet oder unter fremdem Namen auftritt. Solche Fälle konnten bisher über das Strafrecht häufig nicht erfasst werden, oder zumindest nicht zum Schutz desjenigen, dessen Identität verwendet wurde (z.B. für einen Betrug).

[208] Die Verwendung einer fremden Identität aus reinem Übermut oder als Scherz fällt nicht unter die Bestimmung[174]. Der Täter muss in der **Absicht handeln, Schaden zu verursachen oder einen Vorteil zu erwirken** (wobei die Absicht, beim Betroffenen massiven Ärger auszulösen, genügen soll[175]). Auch die Verwendung erfundener Identitäten ist nicht erfasst. Nicht erfasst ist ferner der Fall, in welchem eine Person zwar identifizierende Merkmale einer anderen Person verwendet, jedoch nicht deren Identität behauptet (z.B. der Bühnenauftritt eines Kabarettisten unter Verwendung einer Maske mit dem Abbild eines Politikers). Dies bleibt, wenn überhaupt, «nur» eine Persönlichkeitsverletzung gemäss DSG.

David Rosenthal, lic. iur., Partner, VISCHER AG, Zürich, Lehrbeauftragter ETH Zürich und Universität Basel, Sekretär des Vereins Unternehmens-Datenschutz (VUD).

Der Autor dankt Seraina Gubler und Maria Winkler herzlich für die Mithilfe bei diesem Beitrag.

172 Vgl. dazu den Schlussabstimmungstext des revidierten DSG (N 4).

173 Vgl. BBl 2017 7127.

174 BBl 2017 7127.

175 BBl 2017 7128.