www.jusletter.ch

David Rosenthal

Der Entwurf für ein neues Datenschutzgesetz

Was uns erwartet und was noch zu korrigieren ist

Am 15. September 2017 hat der Bundesrat die Botschaft für ein totalrevidiertes Datenschutzgesetz (DSG) publiziert. Nachdem in der Vernehmlassung sehr viel Kritik laut wurde, ging er deutlich über die Bücher. Das Ergebnis ist durchaus erfreulich, aber es besteht noch Anpassungsbedarf. Viel Zeit dazu gibt es nicht: Die Vorlage wird im Eilzugstempo beraten und soll schon 2018 in Kraft gesetzt werden, wenn es nach dem Bundesrat geht. Dieser Beitrag zeigt die heiklen Punkte und was der Entwurf, sollte er so umgesetzt werden, für die Unternehmen in der Schweiz bedeutet.

Beitragsarten: Beiträge
Rechtsgebiete: Datenschutz

Zitiervorschlag: David Rosenthal, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27. November 2017

Inhaltsübersicht

[Rz 1] Die Botschaft ist mit über 250 Seiten ein Wälzer, die Materie ist hochkomplex: Das Datenschutzrecht war schon bisher keine einfache Angelegenheit, und mit der Revision wird sie ein gutes Stück komplizierter und auch aufwändiger in der Umsetzung. Allerdings kann an dieser Stelle bereits Entwarnung gegeben werden: So schlimm wie in der Europäischen Union und deren Datenschutz-Grundverordnung (**DSGVO**)[1] wird es im Datenschutzgesetz (**DSG**; SR 235.1) nicht werden. Und so schlimm wie der im Dezember 2016 publizierte Vorentwurf auch nicht. Über 220 Eingaben – auch eine des Autors dieser Zeilen – kamen in der Vernehmlassung zusammen und sie wurden in einer Rekordzeit verarbeitet. Viele dieser Eingaben liessen kaum ein gutes Haar an der Vorlage.

[Rz 2] Die am 15. September 2017 veröffentlichte Botschaft «zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz» (die **Botschaft**) und der Entwurf für ein revidiertes DSG (**E-DSG**)[2] sind qualitativ deutlich besser, da etliche Kritikpunkte am Vorentwurf berücksichtigt und diesbezügliche Forderungen in der Vorlage berücksichtigt wurden. Das führte zu zahlreichen Änderungen gegenüber

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

2 BBl 2017 7193 (Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz; E-DSG), BBl 2017 6941 (Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz). Da zum Zeitpunkt der Redaktion dieses Beitrags die offizielle Fassung noch nicht erhältlich war, beziehen sich die Seitenangaben auf die am 15. September 2017 publizierte Version die hier abrufbar ist: http://swissblawg.ch/2017/09/entwurf-des-datenschutzgesetzes.html (Alle Websites zuletzt besucht am 14. November 2017).

dem Vorentwurf, selbst bezüglich des Aufbaus des Gesetzes. Kritik am Entwurf gibt es trotzdem, und zwar aus allen Lagern,[3] auch vom Autor des vorliegenden Beitrags.

[Rz 3] Im vorliegenden Beitrag soll erstens auf die Änderungen eingegangen werden[4], zweitens aufgezeigt werden, was die vorgeschlagenen Regeln in der Praxis bedeuten und drittens Verbesserungsbedarf aufgezeigt werden, der aus fachlicher Sicht besteht. Dabei wird der Fokus auf die Privatwirtschaft gelegt, auch wenn die Vorlage auch die Datenbearbeitung durch Behörden regelt. Dieser Beitrag geht mit wenigen Ausnahmen auch nicht auf die zahlreichen Anpassungen ein, die mit der Revision in anderen Erlassen vorgenommen werden sollen. Viele von diesen Änderungen in anderen Erlassen betreffen allerdings bloss Anpassungen, die sich aus der Anpassung der Terminologie des DSG ergeben, wie namentlich dem Wegfall des Begriffs des Persönlichkeitsprofils.

1. Verhältnis des revidierten DSG zur DSGVO: Angemessen oder nicht?

[Rz 4] Auch im Verhältnis zur DSGVO macht der Entwurf einen grundsätzlich positiven Eindruck: Das E-DSG ist wesentlich schlanker und auch materiell in einigen Punkten deutlich vernünftiger abgefasst als die (inoffizielle) Vorlage der EU. Trotzdem erfüllt das E-DSG jedenfalls auf den ersten und zweiten Blick die Vorgaben, welche die Schweiz gemäss der revidierten Konvention SEV 108 des Europarats (**K108**) umzusetzen hat. Der Autor vertritt zwar nach wie vor die Ansicht, dass aus Sicht des Datenschutzes keine Anpassung des geltenden Rechts erforderlich wäre, sondern dem Datenschutz wesentlich mehr gedient wäre, wenn dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**) massiv mehr Mittel zur Erfüllung seiner Aufgaben zur Verfügung stehen würden. Es ist aber auch klar, dass dies realpolitisch unrealistisch ist und schon aufgrund der völkerrechtlichen Vorgaben und der internationalen Erwartungen und Standards in Europa die Schweiz um eine Revision des DSG nach den Vorgaben der K108 nicht umhinkommt. Die Stimmen, die dereinst ein Nichteintreten auf die Vorlage verlangten, dürften dies inzwischen ebenfalls realisiert haben und nun versuchen, das aus ihrer Sicht Beste daraus zu machen.

[Rz 5] Dies bedeutet nicht, dass die DSGVO kopiert oder gar in allen Punkten nachgeahmt bzw. **autonom nachvollzogen** werden muss oder sollte. Im Gegenteil: Die Schweiz sollte nicht die Fehler begehen, die in der DSGVO begangen wurden und die schon jetzt – noch vor deren offiziellen Inkrafttreten am 25. Mai 2018 – klar erkennbar sind. Dieser Versuchung ist der Bundesrat mit dem E-DSG aber auch nicht erlegen, und das Parlament tut es hoffentlich auch nicht. Die Stossrichtung des revidierten DSG ist zwar dieselbe wie jene der DSGVO. Etliche Regelungskonzepte werden auch ins Schweizer Recht übernommen oder existieren schon. Aber dort, wo es sachlich sinnvoll ist, etwas weniger weit zu gehen, weil der Gesetzgeber der DSGVO sich gewisse Probleme seiner Regelung schlicht noch nicht bewusst war, sollte dies auch geschehen. Es macht zum Beispiel keinen Sinn, Bestimmungen einzuführen, bei denen schon heute klar ist, dass sie nicht eingehalten werden können oder zu unbilligen Ergebnissen führen, nur weil der Gesetzgeber

3 Vgl. etwa David Vasella, Zum Entwurf des DSG vom 15. September 2017, walderwyss rechtsanwälte (http://datenrecht.ch/wp-content/uploads/Kritikpunkte-beim-Entwurf-des-DSG.pdf) und Beat Rudin, Bruno Baeriswyl und Claudia Mund, Das revidierte Datenschutzgesetz ist keine souveräne Lösung, in Neue Zürcher Zeitung, 30. Oktober 2017 (https://www.nzz.ch/meinung/das-revidierte-datenschutzgesetz-ist-keine-souveraene-loesung-ld.1325078).

4 Ausführlicher Bericht zum Vorentwurf: David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017 (http://www.homburger.ch/fileadmin/publications/VORENTWURF.pdf).

der DSGVO sich politisch nicht auf eine vernünftige Lösung einigen konnte oder nicht darüber nachdenken wollte, was die Folgen gewisser Regelungen sind.

[Rz 6] Hingegen wären in der Schweiz Regelungen, die über die DSGVO hinausgehen, unsinnig und schädlich. Solche **Swiss Finishes** werden vermutlich auch politisch keine Chance haben. Es muss gerade für international tätige Unternehmen sichergestellt sein, dass die Befolgung der DSGVO grundsätzlich dazu führt, dass auch das DSG eingehalten ist. Der Botschaft ist zu entnehmen, dass auch der Bundesrat diesen Ansatz verfolgte. Allerdings finden sich auch im E-DSG – wohl irrtümlich – noch etliche solcher Swiss Finishes, die nun vom Parlament ausgemerzt werden müssen. In einer Beilage zu diesem Aufsatz (**hier abrufbar**) sind die dafür nötigen redaktionellen Korrekturen des Entwurfs des Bundesrates konkret beschrieben, zusammen mit den weiteren, in diesem Beitrag angeregten Anpassungen des Entwurfs.

[Rz 7] Nichtsdestotrotz werden in der politischen Diskussion die Erwartungen der EU gegenüber der Schweiz eine erhebliche Rolle spielen. Das Zauberwort lautet «**Adäquanz**» und wird überall als wesentliches Kriterium dafür zitiert, was die Schweiz mit der Revision im europarechtlichen Kontext sicherzustellen hat. Im Kern geht es dabei auf den ersten Blick um die Anerkennung des Datenschutzniveaus der Schweiz durch die Europäische Kommission. Ist es hinreichend, so werden auch in Zukunft Personendaten aus der EU (und dem EWR) ohne besondere Voraussetzungen in die Schweiz übermittelt werden können. Ist dies nicht mehr der Fall, werden Unternehmen im Ausland hierfür in einigen Jahren wie heute beim Datentransfer in andere «unsichere» Drittstaaten mit den Empfängern Verträge abschliessen müssen, um das erforderliche Datenschutzniveau auf diese Weise sicherzustellen.[5] Das Erfordernis eines angemessen Datenschutzniveaus bedeutet allerdings nicht, dass die Schweiz im Zuge ihrer jetzt laufenden Revision das EU-Recht vollständig übernimmt. Dies wird nur im Schengen-Bereich nötig sein, nicht jedoch bezüglich der privaten Datenbearbeitungen. Hier bleibt der Schweiz denn auch ein beträchtlicher Spielraum für ein eigenes, mithin vernünftigeres DSG.

[Rz 8] Die EU ist derzeit daran, den Status der Schweiz als Land mit angemessenem Datenschutzniveau neu zu beurteilen. Worauf es ihr dabei wirklich ankommt und was genau sie erwartet, ist nicht klar, zumal die Adäquanzentscheide in aller erster Linie politische Entscheide sind: Für jedes Land wird faktisch ein eigener Standard gelten. So werden an die USA aufgrund der wirtschaftlichen Bedeutung des Lands mit Sicherheit geringere Anforderungen gestellt werden wie etwa an Russland, das ungeachtet der Tatsache, dass es über ein Datenschutzrecht verfügt, welches dem der EU ähnelt, sehr viel geringere Chancen auf Adäquanz hat.

[Rz 9] Die Adäquanz ist damit ein primär psychologisch wichtiges Element, und sie wird vor allem für die Frage relevant sein, wie sehr die nationalen Aufsichtsbehörden in der EU ein Bedürfnis haben werden, auch gegen Unternehmen in der Schweiz vorzugehen – oder aber es dem EDÖB überlassen, für die Durchsetzung des Datenschutzes in der Schweiz zu sorgen. So wird das künftige Datenschutzniveau der Schweiz auch für die Frage des Kooperationsabkommens zur Koordination der Aufsicht im Bereich des Datenschutzes von Bedeutung sein, welches der Bun-

5 Wie problematisch das wäre, darüber gehen die Meinungen auseinander. Nach der hier vertretenen Ansicht ist die Frage der Adäquanz für internationale Transfers von untergeordneter Bedeutung, da diese ohnehin konzernintern und -extern auf vertraglicher Basis zu regeln ist und jeder Konzern schon heute viele Datentransfers in unsichere Drittstaaten hat und mit den diesbezüglichen Anforderungen des Datenschutzes, die unter der DSGVO und dem E-DSG im Wesentlichen gleichbleiben wie heute, gut zurecht kommt.

desrat im Auftrag des Parlaments mit der Europäischen Kommission auszuloten und anzustreben hat.[6] Die Arbeiten dazu dürften – mit einiger Verspätung – im Frühjahr beginnen.

[Rz 10] Der Regelungspunkt, welcher der EU mit Bezug auf die aktuelle Vorlage wohl am wichtigsten sein wird, dürften dabei die im E-DSG vorgesehenen **Sanktionen** sein. Sie wurden gegenüber dem Vorentwurf abgeschwächt und wirken auf den ersten Blick nicht sehr weitgehend, da die Strafsummen wesentlich geringer sind und sehr viel weniger Tatbestände umfassen. Hierbei ist allerdings zu beachten, dass die EU einen komplett anderen Ansatz verfolgt und in der Schweizer Rechtskultur Sanktionen einen wesentlich geringeren Stellenwert haben als etwa in der EU. Wird der Entwurf des Bundesrats bei Lichte betrachtet und diese Umstände angemessen berücksichtigt, wird die Europäische Kommission das Datenschutzniveau in der Schweiz als angemessen beurteilen. Alles andere wäre sehr erstaunlich und wohl durch andere, politische Motive begründet.

2. Grundkonzept der Vorlage: Weiter wie bisher, aber ohne Daten juristischer Personen

[Rz 11] Das E-DSG weicht wie schon der Vorentwurf vom heute bereits geltenden Regelungsprinzip im Datenschutz nicht ab: Es gibt Grundsätze, wie Personendaten zu bearbeiten sind, und wer diese verletzt, der verletzt die Persönlichkeit der betroffenen Person. Dies ist rechtswidrig, es sei denn, es kann ein Rechtfertigungsgrund nachgewiesen werden, einschliesslich eines überwiegenden eigenen Interesses. Grundsätzlich gilt das **Prinzip des «opt-out»,** d.h. das Bearbeiten von Personendaten ist grundsätzlich erlaubt, es sei denn, es ist im Einzelfall verboten, weil die Persönlichkeit widerrechtlich verletzt oder eine flankierende Bestimmung nicht eingehalten worden ist. Es ist weiterhin nicht erforderlich, für eine Datenbearbeitung eine Einwilligung der betroffenen Person einzuholen, im Übrigen selbst dann nicht, wenn es sich um besonders schützenswerte Personendaten oder um ein Profiling[7] handelt.[8] In der EU ist dies anders: Dort wird für jede Datenbearbeitung eine Rechtsgrundlage ähnlich der Rechtfertigungsgründe von Art. 27 E-DSG verlangt, was bedeutet, dass eine solche für jede Datenbearbeitung bzw. für jeden Bearbeitungszweck einzeln ermittelt und dokumentiert werden muss.[9] Diese Unterscheidung gibt es schon im heutigen Recht.

[Rz 12] Wesentlich ausgebaut wurden im Entwurf die flankierenden Massnahmen, wie zum Beispiel die formalisierte Informationspflicht in Art. 17 E-DSG (heute: Art. 14 DSG), die neu eingeführte Meldepflicht für Datenschutzverletzungen oder die Pflicht, ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Bis auf das Prinzip der **Datenportabilität**[10], auf das zu Recht verzichtet wurde, weil es an sich nichts mit Datenschutz zu tun hat, sondern reines Konsumenten-

6 Motion «Gegen Doppelspurigkeiten im Datenschutz» (16.3752).

7 Letzteres war im Vorentwurf noch angedacht.

8 Art. 5 Abs. 6 E-DSG ist daher nicht so zu verstehen, dass das Einholen einer Einwilligung ein Bearbeitungsgrundsatz ist. Abs. 6 besagt – wie heute – lediglich, wie eine Einwilligung zu erfolgen hat, falls auf eine solche abgestellt werden soll (etwa im Sinne von Art. 27 Abs. 1 E-DSG). Leider wurde es versäumt, Abs. 6 dahingehend klarer zu formulieren.

9 Art. 6 DSGVO.

10 Art. 20 DSGVO.

schutzrecht ist[11], finden sich alle wesentlichen Regelungen der DSGVO auf die eine oder andere Weise auch im E-DSG.

[Rz 13] Aufgegeben wurde im E-DSG der Schutz von **Daten juristischer Personen**, wie sie auch unter der DSGVO nicht geschützt sein werden. Hierbei sind allerdings drei Einschränkungen zu beachten:

- *Erstens* können sich juristische Personen auch in Zukunft weiterhin auf den Schutz ihrer Persönlichkeit durch Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB; SR 210) berufen, wie dies bisher schon anerkannt war. Da das DSG letztlich eben diese Bestimmung konkretisiert, wird es im Streitfall wohl möglich sein, sich als juristische Person auf eine analoge Anwendung der Bearbeitungsgrundsätze aus Art. 5 E-DSG zu berufen, wenn aufgezeigt werden muss, dass eine bestimmte Datenbearbeitung die Persönlichkeit der juristischen Person verletzt. Auch die Regelungen des E-DSG zu den Rechtfertigungsgründen werden in solchen Fällen analog herangezogen werden können.
- *Zweitens* können juristische Personen ihre «Daten» jedenfalls im Verhältnis mit ihren Geschäftspartnern durch vertragliche Regelungen schützen, zum Beispiel mittels Geheimhaltungsbestimmungen. Diese geniessen in der Schweiz sogar strafrechtlichen Schutz[12]. Ferner existieren noch etliche Verträge mit Datenschutzklauseln, welche die Einhaltung der Bestimmungen des Datenschutzes auch für juristische Personen ausdrücklich festschreiben. Je nach Formulierung werden diese Regelungen auch unter einem revidierten DSG weiterhin gelten.
- *Drittens* gibt es selbst in der EU gesetzliche Regelungen, welche auch Unternehmen bestimmte Rechte zusprechen, die jedenfalls mit dem Datenschutz verwandt sind. So wird in der EU derzeit eine Nachfolgeregelung für die ePrivacy-Richtlinie[13] ausgearbeitet, welche Themen wie kommerzielle Kommunikation (Spam), *Cookies* und öffentliche Verzeichnisse regelt und in diesem Zusammenhang einen gewissen Schutz auch von Daten juristischer Personen vorsieht.

[Rz 14] Von der Beschränkung auf natürliche Personen abgesehen, soll der **Begriff des Personendatums** jedoch gegenüber dem heutigen Recht unverändert bleiben. Dies ist auch sinnvoll so. Namentlich kommt weiterhin die «relative» Methode zum Tragen, d.h. ob Personendaten vorliegen, beurteilt sich aus der Perspektive desjenigen, der Zugang zu den fraglichen Daten hat. Für die Bestimmbarkeit einer Person genügt weiterhin nicht jede theoretische Möglichkeit der Identifizierung, d.h. es muss beurteilt werden, welche Mittel die Personen, die Zugriff auf die Daten haben, vernünftigerweise einsetzen würden, um eine Person zu identifizieren.[14] Derselbe Ansatz gilt auch in der EU.[15]

---

11 Es geht im Wesentlichen um das Recht, von einem Online-Dienst bei der Benutzung erzeugte Daten zu einem konkurrierenden Online-Dienst migrieren zu können, was den Wettbewerb unter diesen fördern soll. Die Bestimmung ist aber so breit und abstrakt formuliert, dass sie auch in ganz anderen Bereichen mit teils unkontrollierbaren Auswirkungen zur Geltung kommt, etwa wenn Stellenbewerber oder Angestellte eines Unternehmens verlangen, dass sie betreffende Daten an andere Unternehmen übertragen.

12 Art. 162 und 273 des Schweizerischen Strafgesetzbuches vom 21. Dezember 1937 (StGB; SR 311.0).

13 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 (Datenschutzrichtlinie für elektronische Kommunikation).

14 Vgl. Botschaft (Fn. 2), S. 81 und den Leitentscheid BGE 136 II 508 (E. 3) zum Thema.

15 Vgl. dazu David Rosenthal, Zauberwort Singularisierung: Personendaten ohne Identifizierbarkeit?, in: Digma 2017/4 (noch nicht erschienen).

[Rz 15] Unverändert bleiben soll auch der Fokus des DSG auf den Schutz der Persönlichkeitsrechte jedenfalls im privaten Bereich. Zwar erwähnt das E-DSG nun nicht nur in Art. 1 E-DSG den Schutz der *Grundrechte* der betroffenen Personen, so etwa im Zusammenhang mit Datenschutz-Folgenabschätzungen[16]. Diese Erwähnung bedeutet jedoch nicht, dass über das DSG neu künftig generell eine **Drittwirkung** (von Grundrechten) vorgesehen ist; eine solche besteht in der Schweiz nur in besonderen Fällen.[17] Der Hinweis auf die Grundrechte bezieht sich jeweils auf die Bearbeitung von Personendaten durch Bundesorgane und nicht private Personen. Dies geht indirekt auch aus der Botschaft so hervor[18], und in systematischer Hinsicht daraus, dass im Rahmen der Informationspflicht, wie sie nur für private Datenbearbeiter gilt, nicht auch auf die Grundrechte verwiesen wird.[19] Die Frage ist insofern relevant, als in der EU eine solche Drittwirkung durchaus ein Thema ist und etwa bei der Frage des Begriffs des Personendatums von Relevanz sein kann.[20]

3. Geltungsbereich: Halb zurück zur bewährten Regelung

[Rz 16] Der Geltungsbereich des Datenschutzgesetzes ändert sich für private Datenbearbeiter nicht wesentlich. In der heutigen Aufzählung der ausgenommenen Bereiche in Art. 2 Abs. 2 DSG wurden im neuen Art. 2 E-DSG einige Anpassungen vorgenommen, die hier aber kaum relevant sind. War im Vorentwurf noch vorgesehen, staatliche Verfahren nicht mehr vom DSG auszunehmen, findet sich in Art. 2 Abs. 3 E-DSG nun wieder ein entsprechender Vorbehalt zugunsten der **Prozessgesetze**. Damit kann das Auskunftsrecht nach DSG innerhalb von laufenden Gerichtsverfahren zwar nicht zur Beweismittelbeschaffung eingesetzt werden; dessen Missbrauch ist damit aber in keiner Weise eingeschränkt, ganz im Gegenteil: Es ist mit der neuen Regelung ohne Weiteres denkbar, dass das Auskunftsrecht neu auch *neben* einem laufenden Gerichtsverfahren benutzt wird; Datenschutzgründe lassen sich bekanntlich immer vorschieben. Erste Fälle werden sicherlich nicht lange auf sich warten lassen.

[Rz 17] Am **räumlichen Geltungsbereich** des DSG wird mit der Revision nichts geändert. Hierzu ist wichtig zu wissen, dass das DSG schon unter heutigem Recht aufgrund von Art. 139 des Bundesgesetzes über das Internationale Privatrecht (IPRG; SR 291) jedenfalls im Bereich von auf dem Zivilweg geltend gemachten Ansprüchen ohne Weiteres auch auf Datenbearbeitungen und Datenbearbeiter ausserhalb der Schweiz zur Anwendung gelangen kann. Was die EU mit der DSGVO einführt[21], kennt die Schweiz schon lange.

4. Begriffsdefinitionen: Angleichung des DSG an die DSGVO

[Rz 18] Nebst der Einschränkung des Begriffs der Personendaten auf solche natürliche Personen wurden auch einige andere Begriffe an das Recht der EU angeglichen. Statt wie bisher vom «Inha-

16 Art. 20 E-DSG.

17 Art. 35 Abs. 3 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).

18 Botschaft (Fn. 2), S. 92.

19 Art. 17 Abs. 2 E-DSG.

20 Vgl. dazu David Rosenthal, Zauberwort Singularisierung: Personendaten ohne Identifizierbarkeit?, in: Digma 2017/4 (noch nicht erschienen).

21 Insbesondere Art. 3 Abs. 2 DSGVO.

ber einer Datensammlung» zu sprechen, ist neu vom «**Verantwortlichen**» und «**Auftragsbearbeiter**» die Rede[22], wobei die Schweiz in einem Punkt sich nach wie vor deutlich von der EU-Regelung unterscheidet: Ansprüche aus Persönlichkeitsverletzungen sind weiterhin gegen jeden möglich, der an einer solchen irgendwie «mitwirkt». Dies ergibt sich aus dem Verweis des DSG auf Art. 28 ZGB.[23] Als Mitwirkender kommt auch der Auftragsbearbeiter in Frage, und es sind sogar Konstellationen denkbar, in denen eine Person an einer Persönlichkeitsverletzung mitwirkt, ohne je mit Personendaten in Berührung zu kommen, etwa indem sie Mittel für die Datenbearbeitung zur Verfügung stellt. Sie ist dann weder Verantwortlicher noch Auftragsbearbeiter. In der EU ist sie damit nicht haftbar und kann auch von der Aufsichtsbehörde nicht ins Recht gefasst werden; zudem sind die Auftragsbearbeiter vor Haftung grundsätzlich geschützt, sofern sie ihren spezifischen Pflichten in der DSGVO und den Anweisungen des Verantwortlichen nachgekommen sind.[24] In der Schweiz sind auch in diesen Fällen sowohl zivilrechtliche Ansprüche als auch ein Vorgehen des EDÖB möglich. Letzterer kann gegen jede «private Person» vorgehen.[25]

[Rz 19] Der Katalog der **besonders schützenswerten Personendaten** wurde um genetische und biometrische Daten erweitert.[26] Hierbei sind allerdings zwei Dinge zu beachten: *Erstens* bedeutet die Aufzählung in Art. 4 nicht, dass es sich bei genetischen und biometrischen Daten per se um Personendaten handelt. Genetische Daten sind nur dann besonders schützenswerte Personendaten, wenn es überhaupt Personendaten sind, d.h. sie sich unter Anwendung der üblichen Regelungen auf eine bestimmte oder bestimmbare Person beziehen. Das ist selbst bei genetischen Daten nicht zwangsläufig der Fall.[27] *Zweitens* sind jedenfalls biometrische Daten nur dann besonders schützenswert, wenn sie eine Person «eindeutig identifizieren». Damit sollen zum Beispiel «normale» Bild- und Tonaufnahmen von Menschen ausgenommen werden und nur Fotos, Fingerabdrücke oder Sprachaufnahmen erfasst werden, die mit Verfahren zur sicheren Identifizierung bzw. Authentifizierung von Personen aufgenommen wurden.[28] Die Formulierung ist allerdings unglücklich. Klarer wäre, es wäre von biometrischen Daten die Rede, die dem *Zweck* einer eindeutigen Identifikation dienen, auch wenn genau dies gemeint ist. Dieselbe Einschränkung wird im Übrigen auch bei genetischen Daten verlangt.

[Rz 20] Im Zuge der Revision sollte im Zusammenhang mit der Definition von besonders schützenswerten Personendaten gleich noch mit zwei Swiss Finishes aufgeräumt werden: Daten über Massnahmen der sozialen Hilfe sollten nicht mehr als solche gelten.[29] In der EU tun sie es auch nicht.[30]Auch die Definition von genetischen Daten sollte analog des DSGVO konkretisiert werden.

---

22 Art. 4 Bst. i und j des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).

23 Vgl. Art. 28 Abs. 2 DSG.

24 Art. 82 Abs. 2 DSGVO.

25 Art. 43 Abs. 1 E-DSG.

26 Art. 4 Bst. c Ziff. 3 und 4 E-DSG.

27 Vgl. dazu David Rosenthal, Zauberwort Singularisierung: Personendaten ohne Identifizierbarkeit?, in: Digma 2017/4 (noch nicht erschienen).

28 Botschaft (Fn. 2), S. 82 f.

29 Art. 3 Bst. c Ziff. 6 E-DSG.

30 Art. 10 Abs. 1 DSGVO.

[Rz 21] Der Begriff des Bearbeitens wurde um den Begriff des «**Löschens**» erweitert.[31] Er ergänzt den Begriff des «Vernichtens». Die beiden Begriffe werden in Datenschutzkreisen derzeit diskutiert. Die Ergänzung ist insofern sinnvoll, als das «Vernichten» von Daten heute mitunter dahingehend verstanden wird, dass es die Zerstörung auch des Datenträgers erfordern kann, falls ansonsten mit forensischen Werkzeugen die Daten wiederhergestellt werden könnten. Das ist insofern ein wichtiger Punkt, als in vielen heutigen Systemen zur Speicherung von Dokumenten, E-Mails und anderen Daten ein eigentliches Vernichten von Daten gar nicht mehr möglich ist. Sie können bestenfalls überschrieben, in manchen Fällen aber auch nur als «gelöscht» markiert werden, sind dann aber auf dem physischen Datenträger noch vorhanden, auch wenn die Lesesoftware möglicherweise nicht mehr darauf zugreifen kann.

5. Profiling als neuer Begriff: Nicht die Erstellung eines Persönlichkeitsprofils

[Rz 22] Der Begriff des «Profilings» wird neu eingeführt und ersetzt das Persönlichkeitsprofil.[32] Der Begriff weist ungeachtet seiner Legaldefinition erhebliche Unschärfen auf und scheint – auch in der EU – nicht vollständig durchdacht. Anders als noch im Vorentwurf erfasst er im E-DSG nur noch **automatisierte Vorgänge**. Im Wesentlichen geht es im E-DSG um die Bewertung einer Person hinsichtlich spezifischer Merkmale. Ein blosses Sammeln von Daten stellt noch kein Profiling dar; sie müssen automatisiert analysiert werden. Klar ist, dass sich die Automatisierung nach E-DSG auf die Bewertung der einzelnen Person, nicht die Beschaffung ihrer Daten bezieht. Nicht klar ist, ob bzw. inwieweit auch die Festlegung der Bewertungsregeln automatisiert erfolgen muss, d.h. ob es genügt, wenn die Subsumption der Daten einer bestimmten Person unter eine Bewertungsregel ohne menschliches Zutun erfolgt, auch wenn die (Bewertungs-)Regel von Hand festgelegt worden ist.

[Rz 23] Demnach würde bereits ein Profiling vorliegen, wenn der HR-Verantwortliche sein Online-Bewerbungs-System so programmiert, dass es allen Bewerbern mit einem Notenschnitt unter einer Fünf automatisch eine Absage sendet: Der Computer errechnet den Notenschnitt jedes Bewerbers und stellt diesen den ihm einprogrammierten Anforderungen des Unternehmens (Notenschnitt mindestens eine Fünf, sonst ungeeignet) gegenüber, d.h. bewertet im Ergebnis die Eignung des Bewerbers anhand seines Notenschnitts.

[Rz 24] Wenn nun die Botschaft festhält, dass ein Profiling nur vorliegt, wenn der «Bewertungsprozess vollständig automatisiert» stattfindet[33], muss gefolgert werden, dass im genannten Beispiel der erste Schritt des Bewertungsprozesses – die Festlegung der Note, die noch als genügend erachtet ist – manuell erfolgte und somit im genannten Beispiel kein Profiling vorliegt. Eine solches läge demnach nur vor, wenn der Computer selbst ermitteln würde, welcher Notenschnitt hinreichend ist. Ob der Bundesrat derart restriktiv sein wollte, ist unklar. Aus dem Wortlaut der Norm geht dieses Erfordernis der vollständigen Automatisierung des Bewertungsprozesses nicht

31 Art. 4 Bst. d E-DSG.

32 Art. 4 Bst. f E-DSG.

33 Botschaft (Fn. 2), S. 84.

hervor, und der Botschaft darf hier wohl kein grosses Gewicht beigemessen werden.[34] Zwar betont sie, dass der Begriff im DSG an die europäische Terminologie angepasst worden sei[35], doch hilft dies nicht weiter: So entspricht die **Profiling-Definition der EU** nicht der Empfehlung des Europarats, und jene der EU nicht dem Begriffsverständnis der Schweiz. Jeder versteht unter dem Begriff somit etwas Anderes. Jedenfalls nach dem Verständnis der Artikel-29-Datenschutzgruppe der EU ist für ein Profiling gemäss Art. 4 Ziff. 4 DSGVO nicht entscheidend, ob der Bewertungsprozess vollständig automatisiert erfolgt, sondern ob aus dem Datenbild einer Person eine Schlussfolgerung mit Bezug auf persönliche Aspekte einer Person gezogen wird.[36] Ein Profiling liegt mit anderen Worten dann vor, wenn eine Person aufgrund diverser Daten bezüglich einer persönlichen Frage auf ein bestimmtes «Kästchen» reduziert wird. Nach diesem Verständnis betreibt der HR-Verantwortliche im genannten Beispiel ein Profiling, auch wenn er selbst den relevanten Notenschnitt manuell bestimmt; es genügt, wenn Teile der Datenbearbeitung automatisiert erfolgen, und er reduziert die Bewerber aufgrund ihres Notenschnitts als taugliche und untaugliche Bewerber. Ein Profiling betreibt demnach auch derjenige, der aufgrund einer automatisierten Auswertung von Betreibungsregisterdaten, Zahlungserfahrungen und anderen Angaben einen Bonitätsscore eines Kunden nach (manuell) vorgegebenen Regeln berechnet wie die Bank, die von einem Computer beurteilen lässt, ob der Auftrag zur Überweisung des gesamten Sparkontos einer Person nach China zum üblichen Verhalten dieser Person passt oder womöglich einen Betrugsversuch eines Dritten darstellt. Kein Profiling nimmt hingegen der Routenplaner im Handy einer Person vor, welcher berechnet, wann diese an ihrem Zielort ankommen wird, auch wenn dies eine Vorhersage der Person mit Bezug auf ihren künftigen Aufenthaltsort bzw. ihre Mobilität darstellt.

[Rz 25] Der Begriff bleibt unscharf und keine der Legaldefinitionen kann ihn wirklich erfassen. Dies wird nur die Praxis tun können. Sinnvoll wäre es daher, wenn die Schweiz für «Profiling» dieselbe Definition wie jene der DSGVO übernehmen würde statt mit einer eigenen Regel für Verunsicherung und abweichende Ergebnisse zu sorgen. So kann die Schweiz auch von der Rechtsfortentwicklung in der EU profitieren, die wohl ohnehin zu Rate gezogen würde.

[Rz 26] Der Hinweis in der Botschaft, dass Daten, die aufgrund eines Profiling entstehen, grundsätzlich Personendaten sind[37], stimmt so allerdings nicht. Ein Profiling kann ohne Weiteres auch zur **Erzeugung von anonymen Daten** benutzt werden, auch wenn der «Input» personenbezogen sein mag. Man nehme als Beispiel die Analyse einer Websitenutzung, in deren Rahmen nicht nur ermittelt wird, wofür sich ein bestimmter Nutzer interessiert und was er als nächstes anschauen wird, sondern ihn zugleich anonymisiert. Klar ist allerdings auch, dass in solchen Fällen zwar ein Profiling gemäss Legaldefinition des E-DSG oder auch der DSGVO vorliegen mag, das Datenschutzrecht auf das Ergebnis aber keine Anwendung mehr findet, weil es sich nicht mehr um Personendaten handelt. Mit anderen Worten: Alle Bestimmungen zum Profiling gelten nur insoweit, als dass es um Personendaten geht. Die automatisierte Bewertung bestimmter Merkmale einer Person ist nicht *per se* datenschutzrelevant, solange die Person nicht identifizierbar ist.

---

34 So auch: David Vasella, Zum Entwurf des DSG vom 15. September 2017, walderwyss rechtsanwälte (http://datenrecht.ch/wp-content/uploads/Kritikpunkte-beim-Entwurf-des-DSG.pdf), S. 2.

35 Botschaft (Fn. 2), S. 84.

36 Entwurf einer Leitlinie der Artikel-29-Datenschutzgruppe zu automatisierten Einzelentscheiden und Profiling vom 3. Oktober 2017 (WP251) (http://ec.europa.eu/newsroom/document.cfm?doc_id=50083), S. 6.

37 Botschaft (Fn. 2), S. 84.

[Rz 27] Eine schweizerische Besonderheit ist, dass der Begriff des Profilings im Schweizer Datenschutzrecht einen altbekannten, wenn auch ebenfalls nicht besonders scharfen Begriff ablöst: Das **Persönlichkeitsprofil**. Allerdings sind die Begriffe strikte zu trennen. Ein Profiling führt nicht unbedingt zu einem Persönlichkeitsprofil, und ein Persönlichkeitsprofil setzt nicht unbedingt ein Profiling voraus. Die Begriffe sind sich nur gefühlt sehr nahe. Wenn der Weinhändler in seiner Adresskartei für eine Werbeaktion jene Kunden selektiert, die bei ihm in der Vergangenheit spanische Weine gekauft haben, weil er davon ausgeht, dass sie an einem bestimmten Produkt besonders interessiert sind, betreibt er nach gängigem Verständnis ein Profiling. Ein Persönlichkeitsprofil wird damit jedoch keines erzeugt; es ist unter dem heutigen Recht unumstritten, dass die resultierende Adressliste der Käufer spanischer Weine kein Persönlichkeitsprofil ist oder solche Profile enthalten. Das Beispiel verdeutlicht auch, dass Profiling zwar «bedrohlich» klingt, aber auch völlig harmlose Vorgänge umfassen kann. Von daher ist es auch unverständlich, dass an das Profiling zum Beispiel bei der Einwilligung[38] höhere Anforderungen gestellt werden als an andere Datenbearbeitungen und dies damit begründet wird, dass diese früher ja auch für Persönlichkeitsprofile gegolten haben. Es sind dies eben zwei verschiedene Paar Schuhe. Ebenso ist es schlicht falsch, dass ein Profiling *per se* ein hohes Risiko für die Persönlichkeit einer Person darstellt, wie dies der Bundesrat in Art. 20 Abs. 2 Bst. b E-DSG sogar ins Gesetz schreiben will.

6. Bearbeitungsgrundsätze und Rechtfertigungsgründe: (Fast) alles bleibt beim Alten

[Rz 28] Bezüglich der Bearbeitungsgrundsätze soll grundsätzlich alles beim Alten bleiben. Zwar gibt es redaktionelle Anpassungen, auch wird der **Grundsatz der Datenrichtigkeit** von Art. 5 Abs. 1 DSG mit den anderen Bearbeitungsgrundsätzen aus Art. 4 DSG im neuem Art. 5 E-DSG zusammengeführt. Auch die Einführung des **Grundsatzes der Datensparsamkeit** in Art. 5 Abs. 4 E-DSG ist an sich nur Kosmetik: Er ergibt sich unmittelbar aus dem Grundsatz der Verhältnismässigkeit von Art. 5 Abs. 2 E-DSG. Der Bundesrat wird mit seinen Anpassungen allerdings eher weniger denn mehr Klarheit schaffen. Der neue Art. 5 E-DSG weist zwei grundsätzliche Mängel auf:

- *Erstens* findet sich der **Grundsatz einer transparenten Datenbearbeitung** nur noch teilweise wieder. Zwar betont die Botschaft, dass der Grundsatz der Erkennbarkeit (bisher: Art. 4 Abs. 4 DSG) neu mit dem Grundsatz der Zweckbindung vereint ist.[39] Zwar hält die Botschaft fest, dass sowohl der Zweck als auch die Beschaffung selbst auch mit der neuen Formulierung erkennbar sein müssen.[40] Der bisherige Grundsatz der Erkennbarkeit ging jedoch weiter und verlangte, dass alle wesentlichen Parameter einer Datenbearbeitung transparent sein mussten, also etwa die Weitergabe an Dritte. Dies fällt nun weg. Stattdessen wurde die Informationspflicht in Art. 17 E-DSG ausgebaut und entsprechend offen gestaltet. Wie weiter hinten noch erläutert wird, ist dies ein gesetzestechnischer Fehler. Richtigerweise gehört der Grundsatz der Transparenz unabhängig von der Informationspflicht in die Bearbeitungsgrundsätze, wie dies auch in der DSGVO der Fall ist. Zwar lässt er sich zur Not auch aus dem Grundsatz

38 Art. 5 Abs. 6 E-DSG.

39 In Art. 5 Abs. 3 E-DSG; Botschaft (Fn. 2), S. 87.

40 Botschaft (Fn. 2), S. 87.

der Bearbeitung nach Treu und Glauben ableiten. Da es sich aber um den wichtigsten Bearbeitungsgrundsatz überhaupt handelt, sollte er auch ausdrücklich erwähnt werden.[41] Dies würde es im Übrigen auch erlauben, den Grundsatz der Zweckbindung etwas einfacher zu formulieren.

- *Zweitens* wurde der **Grundsatz der Datensparsamkeit** missverständlich formuliert. Selbstverständlich ist es nicht erforderlich, Datenträger zu vernichten, wenn die darauf gespeicherten Daten nicht mehr benötigt werden. Ein einfaches Löschen genügt. Es muss sichergestellt sein, dass die nicht mehr benötigten Daten auch nicht mehr benutzt werden können. Ob dies durch eine physische Vernichtung geschieht oder durch eine bloss «logische» Löschung, indem nicht mehr darauf zugegriffen werden kann, kann letztlich keine Rolle spielen.[42] Wäre dem nicht so, müssten beispielsweise auch Sicherungskopien, auf denen sich (auch) nicht mehr benutzte Daten befinden, vernichtet werden, was nicht der Fall ist.

[Rz 29] Werden die in Art. 5 Abs. 1–5 E-DSG aufgeführten Bearbeitungsgrundsätze verletzt, so stellt dies – wie auch heute – *per se* eine **Persönlichkeitsverletzung** dar[43], die nur dann erlaubt ist, wenn es hierfür einen Rechtfertigungsgrund gibt.[44] Dasselbe gilt auch für die Verletzung der Datensicherheit nach Art. 7 E-DSG (aber nicht mehr für die Verletzung von Art. 6 Abs. 1 E-DSG[45]), und ebenso – wie im heutigen Recht – die Weitergabe von besonders schützenswerten Personendaten an Dritte.[46]

[Rz 30] Hingegen führt ein **Profiling ohne Einwilligung** nicht mehr wie im Vorentwurf angedacht zwangsläufig zur Persönlichkeitsverletzung, d.h. es ist grundsätzlich ohne eine Einwilligung oder einen anderen Rechtfertigungsgrund zulässig. Das erscheint auch sinnvoll so, bedeutet doch der Umstand, dass eine Maschine bestimmte Aspekte eines Menschen oder seines Verhaltens automatisch beurteilt, grundsätzlich noch nicht, dass dieser in seiner Persönlichkeit tangiert ist (siehe vorne Rz. 22 ff.). Dies gesagt, ist darauf hingewiesen, dass die Aufzählung der Fälle in Art. 26 Abs. 2 E-DSG, in denen in jedem Fall eine Persönlichkeitsverletzung vorliegt, nicht abschliessend ist. Ein besonders heikles Profiling kann somit ohne Weiteres trotzdem eine Persönlichkeitsverletzung darstellen. Daher ist es wie erwähnt auch nicht nachvollziehbar, dass jedes Profiling automatisch eine Datenschutz-Folgeabschätzung nach sich ziehen soll, wie das Art. 20 Abs. 2 Bst. b E-DSG vorsieht. Eine Rolle spielt Profiling ferner im Zusammenhang mit der Informationspflicht zu automatisierten Einzelentscheiden in Art. 19 E-DSG (siehe unten Rz. 100 ff.).

[Rz 31] Zu einer Persönlichkeitsverletzung führt schliesslich der **Widerspruch der betroffenen Person**.[47] Es ist hierfür eine ausdrückliche Willenserklärung der betroffenen Person erforderlich, d.h. ein Widerspruch kann nicht einfach angenommen werden bzw. durch Stillschweigen entstehen. Das Widerspruchsrecht ist das Gegenstück zum Grundsatz der Transparenz, weshalb dieser auch so wichtig ist: Nur wenn eine Datenbearbeitung in allen wesentlichen Aspekten für die be-

41 Art. 5 Abs. 2 E-DSG.

42 Dieses «Problem» ist somit nicht erst auf der Ebene der Rechtfertigung zu lösen, sondern bereits durch ein entsprechendes Verständnis von Art. 5 Abs. 4 E-DSG. Nichts anderes ergab und ergibt sich auch aus dem Grundsatz der Verhältnismässigkeit, der mit dieser Bestimmung lediglich zum Ausdruck gebracht wird (Botschaft (Fn. 2), S. 88).

43 Art. 26 Abs. 2 Bst. a E-DSG.

44 Art. 27 Abs. 1 E-DSG.

45 Womit das E-DSG weniger weit geht als das heutige Recht, welches in Art. 7 Abs. 1 DSG den Inhalt von Art. 6 Abs. 1 E-DSG und Art. 7 Abs. 1 E-DSG in einer Norm vereint.

46 Art. 26 Abs. 2 Bst. c E-DSG.

47 Art. 26 Abs. 2 Bst. b E-DSG.

troffene Person transparent erfolgt, kann die Person auch entscheiden, ob sie ihr widersprechen will. Solange sie dies nicht tut und die weiteren Bearbeitungsgrundsätze eingehalten sind, ist die Datenbearbeitung zulässig (Prinzip des «opt-out»).

[Rz 32] In der Vernehmlassung wurde teilweise kritisiert, dass die Vorlage kein «**Recht auf Vergessen**» vorsehe. Dies ist jedoch falsch: Art. 26 Abs. 2 Bst. b E-DSG umfasst auch das «Recht auf Vergessen», wie es das heutige DSG schon tut. Richtigerweise gilt es aber nicht absolut, sondern der Widerspruch einer betroffenen Person kann durch einen entsprechenden Rechtfertigungsgrund aufgewogen werden. Das entspricht der ständigen Rechtsprechung. Es besteht somit keine Regelungslücke.

[Rz 33] An den **Rechtfertigungsgründen** soll sich nach Massgabe des Bundesrats ebenfalls nicht viel ändern. Das Grundkonzept, wonach eine Persönlichkeitsverletzung analog zu Art. 28 ZGB durch ein überwiegendes privates oder öffentliches Interesse, das Vorhandensein einer gesetzlichen Pflicht oder eine Einwilligung der betroffenen Person gerechtfertigt werden kann, bleibt erhalten. Im Vorentwurf war noch erwogen worden, die beispielhafte Aufzählung von Fällen, in welchen normalerweise von einem überwiegenden privaten Interesse auszugehen ist, restriktiver als heute zu handhaben. Aufgrund entsprechender Kritik in der Vernehmlassung wurde das nicht getan. Somit entspricht Art. 27 E-DSG weitgehend der heutigen Regelung, mit zwei Anpassungen:

- Der Rechtfertigungsgrund der **Bearbeitung von Personendaten zu nicht personenbezogenen Zwecken** (Art. 27 Abs. 2 Bst. e E-DSG) wird etwas eingeschränkt. Besonders schützenswerte Personendaten dürfen neu nicht mehr Dritten gegenüber offengelegt werden, ohne dass diese vorher anonymisiert worden sind.[48] Gemeint sind damit andere Verantwortliche, mit denen nicht nur die unpersönlichen Ergebnisse der Bearbeitung geteilt werden sollen, sondern gewissermassen auch die Rohdaten, die noch Personendaten enthalten. Zu denken ist zum Beispiel an Daten, die ein Unternehmen von seinen Kunden bezüglich deren Benutzung seiner Produkte sammelt, um diese danach für die Forschung und Entwicklung im Konzern zu benutzen, oder die nicht anonymisierten Daten aus einer medizinischen Studie. Es wäre zum Beispiel nicht mehr zulässig, solche Daten an andere Konzerngesellschaften weiterzugeben, wenn diese sie für ihre eigenen Zwecke (und nicht bloss zur Ausführung von Auftragsarbeiten) einsetzen wollen. Das Problem lässt sich in der Praxis etwa dadurch lösen, dass mehrere Verantwortliche die Daten gemeinsam beschaffen, da sie in diesen Fällen untereinander ebenfalls keine Dritte mehr sind, oder aber es wird bei den betroffenen Personen, wo dies möglich ist, die Einwilligung zur Weitergabe an Dritte eingeholt. Zudem sind Situationen denkbar, in denen ungeachtet der Einschränkung von Bst. e eine Weitergabe möglich ist, da sie aufgrund anderer Umstände als gerechtfertigt erscheint; Art. 27 Abs. 2 stellt ja nur eine beispielhafte, nicht abschliessende Aufzählung dar.
- Der Rechtfertigungsgrund der **Bonitätsprüfung** (Art. 27 Abs. 2 Bst. c E-DSG) ist ebenfalls verschärft worden, allerdings schiesst die Vorlage mehrfach übers Ziel hinaus und ist in dieser Form untauglich: Sie erlaubt es Wirtschaftsauskunfteien nicht mehr, Auskünfte über die Kreditwürdigkeit einer Person zu geben, obwohl gerade das der Sinn und Zweck des Rechtfertigungsgrunds ist. Grund für die redaktionelle Panne ist vermutlich die Gleichsetzung von Persönlichkeitsprofil und Profiling. Weil es Wirtschaftsauskunfteien im heutigen Recht nicht

48 Art. 27 Abs. 2 Bst. e Ziff. 2 E-DSG.

erlaubt ist, Persönlichkeitsprofile zu bearbeiten, wird ihnen im Entwurf nun kurzerhand auch das Profiling untersagt, obwohl diese Begriffe unterschiedliche Dinge abdecken. Der Bonitätscore einer Person, den Online-Shops, Leasinggesellschaften und Kreditfirmen benötigen, um zu beurteilen, ob sie einem Kunden einen Kauf auf Rechnung anbieten bzw. Kredit gewähren, gilt noch nicht als Persönlichkeitsprofil, doch stellt dessen Berechnung ein Profiling dar. Wirtschaftsauskunfteien dürfen somit das, wozu sie eigentlich da sind, nicht mehr tun. Beabsichtigt war das wohl kaum; es ging dem Bundesrat wohl eher darum zu verhindern, dass die Auskunfteien keine Profile von *anderen* übernehmen oder sich auf Profilings von Dritten stützen, wenn sie die Bonität einer Person beurteilen. Natürlich könnte dies auf dem Weg einer teleologischen Reduktion korrigiert werden und auch praktische Umgehungslösungen sind denkbar, aber solche gesetzgeberischen Fehler sollten von vorneherein beseitigt werden; der Ausschluss von Profiling ist ersatzlos zu streichen oder auf das Ausgangsmaterial einer Bonitätsberechnung zu beschränken. Auch Konsumenten profitieren letztlich davon, wenn Unternehmen ihre Leistungen auf Rechnung bzw. auf Kredit anbieten. Der Grundsatz der Verhältnismässigkeit ist hinreichend klar, um Auswüchse zu verhindern. Das gilt im Übrigen auch mit Bezug auf besonders schützenswerte Personendaten, die ebenfalls nicht bearbeitet werden dürfen (schon unter heutigem Recht). Die Information, dass es sich bei einer Person um einen mehrfach verurteilten Kreditbetrüger handelt, darf eine Wirtschaftsauskunftei daher zur Beurteilung der Kreditwürdigkeit nicht berücksichtigen.

Mit seiner Beschränkung auf Daten, die maximal fünf Jahre alt sind, schiesst der Bundesrat ebenfalls am Ziel vorbei. So bearbeiten Kreditauskunfteien nicht nur Daten über Betreibungen und Zahlungserfahrungen, sondern auch diverse weitere Daten, die bei den meisten Personen älter als fünf Jahre sein werden, wie z.B. Name, Adresse, oder Geburtstag, sowie frühere Adressen, die oft zur sicheren Identifikation der Person erforderlich sind. Auch weitere Angaben etwa über Bevormundungen oder Verlustscheine werden nicht bereits nach fünf Jahren irrelevant für die Kreditwürdigkeit. Dieses Zeitlimit ist daher durch 20 Jahre zu ersetzen oder noch besser ganz zu streichen und stattdessen auf den Grundsatz der Verhältnismässigkeit zu verweisen, der eine differenziertere Lösung ermöglicht.

Dass verlangt wird, dass nur Daten volljähriger Personen bearbeitet werden, leuchtet auf den ersten Blick als Kriterium ebenfalls ein, ist auf den zweiten Blick aber nicht sinnvoll, da Wirtschaftsauskunfteien heute auch dazu genutzt werden, festzustellen, ob eine Person überhaupt volljährig ist und mit ihr entsprechende Verträge gefahrlos abgeschlossen werden können. Hierzu müssen die Auskunfteien die Person verzeichnen, auch wenn sie noch minderjährig ist. Ob es verhältnismässig ist, über sie auch Angaben zur Zahlungserfahrung zu bearbeiten, ist eine andere Erfahrung. Einige Auskunfteien tun das denn auch nicht. Die Verhältnismässigkeit genügt auch hier als Kriterium. Wird die Volljährigkeit als Kriterium inskünftig verlangt, muss damit gerechnet werden, dass Kunden von Kreditauskunfteien davon ausgehen, dass jede Person, über die keine Angaben bei einer Kreditauskunftei vorliegen, nicht kreditwürdig oder nicht volljährig ist.

[Rz 34] Eine weitere, in der Vernehmlassung angeregte Anpassung der Rechtfertigungsgründe von Art. 27 Abs. 2 E-DSG, fand leider keinen Eingang in den Entwurf: Der **Rechtfertigungsgrund des Vertragsschlusses** (Bst. a) sollte nicht nur dann angerufen werden können, wenn es um Daten des Vertragspartners geht, sondern auch Daten der Personen, in deren Interesse der

Vertrag abgeschlossen wurde. Art. 14 Abs. 1 Bst. b E-DSG sieht dies bei Datenexporten bereits vor und es ist nicht ersichtlich, warum der Rechtfertigungsgrund des Vertragsabschlusses und der Vertragserfüllung in Art. 27 Abs. 2 Bst. a E-DSG nicht gleich formuliert sein sollte. Es wäre auch sachlich falsch, wenn nur die Bearbeitung des Vertragspartners gerechtfertigt ist: Wird ein Vertrag für einen Dritten abgeschlossen (z.B. Empfänger der Leistung), muss derjenige, der den Vertrag erfüllt, auch dessen Daten bearbeiten können (z.B. die Lieferadresse). Art. 27 Abs. 2 Bst. a E-DSG ist daher analog zu ergänzen.

7. Begriff der Einwilligung: Keine Verschärfung, aber eine verwirrende Botschaft

[Rz 35] Die Einwilligung als Rechtfertigungsgrund geniesst in der Praxis einen hohen Stellenwert. Sie wird nach der hier vertretenen Ansicht allerdings überbewertet, da sie in vielen Fällen gar nicht nötig oder aber ein zu wenig zuverlässiges Instrument ist, da sie von vielen Voraussetzungen abhängt und grundsätzlich widerrufen werden kann. Die Voraussetzungen einer für den Datenschutz gültigen Einwilligung sind in Art. 5 Abs. 6 E-DSG geregelt. Sie finden sich also wie heute und im Vorentwurf im Artikel zu den Bearbeitungsgrundsätzen, auch wenn dies systematisch keinen Sinn macht; warum die Definition der Einwilligung nicht wie alle anderen Definitionen in Art. 4 E-DSG verschoben wurde, bleibt schleierhaft.

[Rz 36] Nach wie vor bedeutet dies aber nicht, dass das Einholen einer Einwilligung ein Bearbeitungsgrundsatz bzw. dass für das Bearbeiten von Personendaten eine solche Einwilligung erforderlich ist. Gemäss Botschaft soll die **Legaldefinition einer gültigen Einwilligung** lediglich terminologisch an die Konvention angepasst werden, sich «grundsätzlich» aber nicht ändern.[49] Sie ist nur gültig, wenn sie nach angemessener Information freiwillig (bisheriger Text) und «eindeutig» (neu, zusätzlich) erteilt wird. Auf die zusätzlichen Anforderungen an eine Einwilligung wie im EU-Recht wurde wie im Vorentwurf verzichtet; namentlich besteht in der Schweiz nach wie vor **kein Koppelungsverbot**,[50] jedenfalls nicht explizit, und es wird auch nicht wie in der EU behauptet, das vorangekreuzte Kästchen auf Online-Formularen nicht mehr zulässig seien, was ohnehin systemwidrig wäre. Es gelten somit weiterhin die Grundsätze des Obligationenrechts, was sachgerecht ist, da sie bereits relativ streng sind und es keinen Sinn macht, eine Spezialregelung für den Datenschutz zu treffen. Allerdings sei auf die Ausführungen zum Grundsatz *Privacy by Default* weiter unten verwiesen (Rz. 42 ff.), der einem Koppelungsverbot nahe kommt.

[Rz 37] Das nunmehr ausdrücklich erwähnte Erfordernis der Eindeutigkeit ist an sich unproblematisch, wenn damit lediglich gesagt werden soll, dass eine Einwilligung hinreichend **eindeutig** sein muss, um gültig zu sein. Das gilt heute schon, und zwar im gesamten Schweizer Recht: Je einschneidender die Folgen einer Einwilligung, desto klarer muss sie sein. Je ungewöhnlicher die beabsichtigte Datenbearbeitung, desto deutlicher muss darauf hingewiesen werden. Die Botschaft stiftet nun aber durch ihre Erläuterungen einige Verwirrung, indem sie sagt, das Erfordernis der Eindeutigkeit bedeute, dass aus der Erklärung der Wille der betroffenen Person «zweifelsfrei» hervorgehen muss.[51] Dies suggeriert, dass im Datenschutz plötzlich nur noch das Willensprinzip

49 Botschaft (Fn. 2), S. 89.

50 Art. 7 Abs. 4 DSGVO.

51 Botschaft (Fn. 2), S. 89.

gelten soll – wie etwa bei Testamenten – und Einwilligungserklärungen nicht mehr danach ausgelegt werden dürften, wie eine vernünftige Person sie nach Treu und Glauben verstehen durfte, der normative Wille also nicht mehr zählt. Das würde jede serienmässige oder in einen zweiseitigen Vertrag eingebettete Einwilligung faktisch verunmöglichen. Da sich die Botschaft zu diesen Fragen keine Gedanken macht, muss davon ausgegangen werden, dass die genannten Ausführungen schlicht ein Versehen sind. Das gilt umso mehr, als dass die Botschaft festhält, dass eine eindeutige Willenserklärung auch stillschweigend erfolgen kann, was regelmässig ein klassischer Anwendungsfall des Vertrauensprinzips darstellt, und die Aussage, dass es von den «Umständen des Einzelfalls» abhängen soll, wie «zweifelsfrei» sich der Wille ergibt, schlicht ein Widerspruch in sich ist. Es bleibt somit alles beim Alten und die Botschaft hätte besser geschwiegen. Noch besser wäre es aber, den Zusatz «eindeutig» zu streichen. Er bringt nichts, öffnet aber Tür und Tor für eine rein ergebnisorientierte Rechtsanwendung, wie sie im Datenschutz leider an der Tagesordnung und ein Hauptgrund für die grosse Rechtsunsicherheit ist.

[Rz 38] Neu hält der Entwurf in Satz 1 von Art. 5 Abs. 6 E-DSG fest, dass eine Einwilligung **für eine oder mehrere Bearbeitungen** erteilt werden kann. Diese Wendung geht auf Kritik zu missverständlichen Erläuterungen des Vorentwurfs zurück und bedeutet nichts Neues; auch sie ist an sich unnötig, schadet aber nicht. Selbstverständlich gilt eine Einwilligung nur für jene Bearbeitungen, für welche sie eingeholt wird, dies bräuchte nicht extra betont zu werden.

[Rz 39] Nicht neu ist auch das **Erfordernis der Ausdrücklichkeit** in Satz 2 von Art. 5 Abs. 6 E-DSG, soweit eine Einwilligung die Bearbeitung von besonders schützenswerten Personendaten oder das Profiling betrifft. Die Botschaft beschränkt sich hierzu leider auf Allgemeinplätze, die im Kern an der Sache vorbeigehen. Die einzige klare Aussage ist, dass eine ausdrückliche Einwilligung nicht stillschweigend erfolgen kann. Da aber ausdrücklich keine Änderung der Rechtslage beabsichtigt ist, gilt weiterhin, was bisher galt. Demnach ist eine Einwilligung dann ausdrücklich im Sinne von Art. 5 Abs. 6 Satz 2 DSG, wenn ein (i) aktives Verhalten oder ein solches vorliegt, das als armativ vereinbart wurde, und (ii) die Bedeutung dieses armativen Verhaltens sich direkt auf die betreende Datenbearbeitung bezieht. Nicht ausdrücklich und somit konkludent ist eine Einwilligung in eine Datenbearbeitung dann, wenn das armative Verhalten sich lediglich auf eine Handlung bezieht, welche die fragliche Datenbearbeitung zur Folge hat und nicht auf die Datenbearbeitung selbst.[52] Wer also beispielsweise in den Erhalt personalisierter Werbung einwilligt, hat nicht ausdrücklich in die Vornahme des dafür erforderlichen Profilings eingewilligt, und zwar egal, ob die Einwilligung in den Erhalt der Werbung ausdrücklich erfolgte. Das Beispiel zeigt umgekehrt allerdings auch, dass es über das Ziel hinausschiesst, für jegliches Profiling eine ausdrückliche Einwilligung zu verlangen, so banal es auch ist: Wenn im oben zitierten Beispiel der Weinhändler seine Kunden nach Interessen sortieren und anschreiben will (Rz. 27), muss eine entsprechende Einwilligung ausdrücklich erfolgen. Das Profiling kann somit in Art. 5 Abs. 6 Satz 2 DSG ohne negative Folgen gestrichen werden. Ohnehin muss eine Einwilligung je klarer erfolgen je heikler die Datenbearbeitung ist. Mit der Frage, ob diese als Profiling qualifiziert oder nicht, hat dies nichts zu tun.

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

8. Neues Prinzip des «Privacy by Default»: Das Schweizer Koppelungsverbot?

[Rz 40] Die bisherige Regelung war einfach: Art. 7 DSG verlangt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Der Bundesrat konnte nähere Ausführungen zur Datensicherheit erlassen. Neu wird diese Regelung auf zwei volle Artikel aufgeblasen und aufgetrennt: Art. 7 E-DSG regelt die **Datensicherheit**, wobei dieser Begriff neu enger als bisher verstanden wird. Er meint nur den Schutz von Daten vor dem ungewollten Verlust, der ungewollten Löschung, Vernichtung, Veränderung oder Offenlegung oder anderem Zugänglichmachen gegenüber Unbefugten[53], nicht aber beispielsweise eine **zweckwidrige, unrichtige, intransparente oder unverhältnismässige Datenbearbeitung**. Diese war bisher ebenfalls von Art. 7 DSG erfasst. Die gegen die letztgenannten Datenschutzverletzungen zu treffenden technischen und organisatorischen Vorkehrungen sind neu nach Art. 6 Abs. 1 und 2 E-DSG zu treffen. Dass dies «ab der Planung» der Datenbearbeitung zu geschehen hat, liegt in der Natur der Sache. Die Erwähnung dient somit einzig dazu, zu verdeutlichen, dass auch die Schweiz ein ***Privacy by Design*** vorsieht; der Grundsatz gilt schon im heutigen Recht, denn wer den Datenschutz im laufenden Betrieb ab dessen Beginn einhalten will, muss die dafür nötigen Voraussetzungen logischerweise schon vorher schaffen. Die Bestimmung hält also das Offenkundige fest.

[Rz 41] Ebenso unnötig ist die Auftrennung von Art. 7 Abs. 1 DSG auf die beiden neuen Artikel. Sie verkompliziert das DSG nicht nur, sondern schafft im konkreten Fall auch neue Lücken im «Vorfeld»-Schutz, um den es bei diesen beiden Bestimmungen geht. So wird die Verletzung von Art. 6 E-DSG in keiner Weise sanktioniert: Weder stellt ihre Verletzung – einschliesslich die Nichtbefolgung von *Privacy by Design* oder *Privacy by Default* – eine Persönlichkeitsverletzung dar[54], noch knüpft daran eine Strafbarkeit.[55] Bei Art. 7 E-DSG ist hingegen beides gegeben. Mit anderen Worten: Der Entwurf tut so, als würde er den Datenschutz verstärken, macht in Tat und Wahrheit mit Art. 6 Abs. 1 und 2 E-DSG aber einen Schritt zurück. Auch die Ausführungen in Art. 6 Abs. 2 E-DSG galten schon bisher, auch wenn lediglich im Rahmen der Verordnung zum DSG und waren dort besser formuliert; insbesondere wurde dort auch auf die Notwendigkeit einer periodischen Überprüfung hingewiesen, was neu nicht mehr ausdrücklich festgehalten wird.[56]

[Rz 42] Wirklich neu ist an sich nur Art. 6 Abs. 3 E-DSG, welche Bestimmung den Grundsatz des ***Privacy by Default*** normiert, das Prinzip, dass «Grundeinstellungen» datenschutzfreundlich sein müssen. Die Regelung wurde gegenüber dem Vorentwurf umformuliert und ist jetzt verständlicher, auch wenn sie noch einige Fragen aufwirft. Sie setzt begriffslogisch zunächst voraus, dass es um eine Datenbearbeitung geht, die der betroffenen Person «Einstellungen» zum Umfang oder zur Art der Datenbearbeitung ermöglicht, denn nur wo es Einstellungsmöglichkeiten gibt, kann es auch *Vor*einstellungen geben. Dies wiederum setzt eine Schnittstelle zwischen Datenbearbeitung und betroffener Person voraus, wie es beispielsweise bei einem Online-Dienst der Fall ist, aber auch bei der Installation einer App oder Software, die Daten bearbeitet und z.B.

53 Botschaft (Fn. 2), S. 93, mit Verweis auf die Legaldefinition der «Verletzung der Datensicherheit» in Art. 4 E-DSG.

54 In Art. 26 Abs. 2 Bst. a E-DSG wird nicht auch auf Art. 6 E-DSG verwiesen. Die Persönlichkeitsverletzung liesse sich allenfalls auf dem Umweg über Art. 5 Abs. 1 E-DSG konstruieren. Allerdings dürfte dies nicht die Absicht des Gesetzgebers sein.

55 Art. 26 Abs. 2 Bst. a E-DSG.

56 Art. 8 der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG; SR 235.11).

über eine Internet-Verbindung mit einem Dienstleister abgleicht. Es muss also vorgesehen sein, dass die Person die Möglichkeit hat, die Einstellungen der Datenbearbeitung zu ändern. Wer bei sich intern eine Datenbearbeitung betreibt und dafür zwar vielleicht Einwilligungen, auch unterschiedlich weitgehende einholt, aber keine Steuerung von aussen durch die betroffene Person vorsieht, fällt somit mangels «Einstellungen» nicht unter diese Regelung.

[Rz 43] Wird nun eine Datenbearbeitung betrieben, die der betroffenen Person Einstellungen ermöglicht, so müssen diese gemäss Art. 6 Abs. 3 E-DSG dann, wenn die betroffene Person *keine* Einstellungen vornimmt bzw. sich zu den Einstellungen nicht äussert, so eingestellt sein, dass sie auf das vorgesehene Mindestmass beschränkt ist. Was das Mindestmass ist, bestimmt aber der Verantwortliche selbst, was sich daraus ergibt, dass er es ja ist, der den Verwendungszweck bestimmt, auf den die Regelung verweist. Wird also eine Software, die Daten des Benutzers via Internet mit dem Hersteller austauscht, installiert und beschränkt sich die Interaktion mit der betroffenen Person darauf, dass sie gar nichts tut (jemand anders installiert die Software) oder sie lediglich den Befehl zur Installation erteilt, und kann die Software so benutzt werden, dass sie dem Hersteller keinen Zugriff auf die Daten des Benutzers erlaubt, so muss eben dies die Grundeinstellung sein, mit welcher die Software installiert wird. Der Benutzer muss dann dem Hersteller den Zugang öffnen, wenn er die Software benutzt.

[Rz 44] Dies ist allerdings nur ein Anwendungsfall der Regelung. Der häufigere Anwendungsfall dürfte ein anderer sein: Die genannten Voreinstellungen sind gemäss Art. 6 Abs. 3 E-DSG nur dann erforderlich, «soweit die betroffene Person nicht etwas anderes bestimmt». Wird mit der betroffenen Person *vorgängig* eine **andere Abrede getroffen** oder von ihr eine andere Instruktion erteilt, gilt Art. 6 Abs. 3 E-DSG nicht mehr. Das ist zum Beispiel möglich, indem die gewünschten Einstellungen während der Installation abgefragt werden. Hierbei ist es ohne Weiteres möglich, dass dem Benutzer eine Seite präsentiert werden kann, auf welcher er die diversen Einstellungen vornehmen kann und mehr als die minimalen Bearbeitungen bereits vorangekreuzt sind. Art. 6 Abs. 3 E-DSG verpflichtet nicht dazu, dass in einer Einwilligungserklärung irgendwelche Kästchen nicht bereits vorausgewählt sein dürfen. Solange die betroffene Person die Möglichkeit hat, die Kästchen abzuwählen, was naturgemäss immer der Fall sein wird, wenn der Verantwortliche die Datenbearbeitung optional anbieten will (sonst bräuchte es gar kein Kästchen), ist Art. 6 Abs. 3 E-DSG genüge getan. Die Bestimmung regelt nur *Vor*einstellungen, nicht Einwilligungserklärungen. Voreinstellungen sind Einstellungen, die gerade ohne eine darauf ausgerichtete Willenserklärung der betroffenen Person vorgenommen werden.

[Rz 45] Damit ist auch die sich stellende Frage beantwortet, ob aufgrund von Art. 6 Abs. 3 E-DSG indirekt ein **Koppelungsverbot** im Bereich von Einwilligungserklärungen resultiert, wenn sie so verstanden wird, dass einer betroffenen Person die Möglichkeit gegeben werden muss, zu jeder Option der Datenbearbeitung separat Stellung nehmen zu können. Dem ist nach dem Gesagten nicht so, denn es obliegt im Regelungskonzept von Art. 6 Abs. 3 E-DSG dem Verantwortlichen zu bestimmen, wie er seine Datenbearbeitung strukturieren und welche Optionen er anbieten will.

[Rz 46] Die Botschaft erwähnt als ein Anwendungsbeispiel den Online-Shop, in welchem mit oder ohne Erstellung eines Benutzerprofils eingekauft werden kann. Das Beispiel ist allerdings eher verwirrend als klärend, denn erstens verlangt die Bestimmung nicht, dass ein Online-Shop diese Alternative anbietet, und zweitens wird der Online-Shop, der dies doch tut, nicht mit einer Voreinstellung operieren, sondern im Bestellvorgang ganz einfach fragen, ob der Benutzer sich anmelden, ein Konto anlegen oder lediglich als Gast bestellen will. Der Benutzer muss sich für eine der drei Optionen entscheiden; eine darf auch ohne Weiteres voreingestellt sein, denn es ist

dies keine Voreinstellung einer Datenbearbeitung, sondern die Voreinstellung der Willenserklärung, wie er bestellen will, und diese ist von Art. 6 Abs. 3 E-DSG nicht erfasst, indem diese darauf ausdrücklich Bezug nimmt («soweit er nicht etwas anderes bestimmt»).

[Rz 47] Wie schon bei Art. 6 Abs. 1 und 2 E-DSG gilt im Übrigen auch hier: Die Verletzung von Art. 6 Abs. 3 E-DSG ist nicht direkt sanktioniert, weder über Art. 26 Abs. 2 Bst. a E-DSG noch über das Strafrecht. Wird die Bestimmung nicht befolgt, wird die Durchsetzung primär in der Hand des EDÖB liegen.

9. Datenschutz-Folgenabschätzungen: Profiling führt nicht immer zu einem hohen Risiko

[Rz 48] Datenschutz-Folgenabschätzungen (**DSFA**) – auch bekannt als *Privacy Impact Assessments* (**PIA**) – sind in der Sache selbst nichts Neues. Neu ist, dass es in Art. 20 E-DSG eine formale Pflicht gibt, sie durchzuführen. Auch hierbei lehnt sich der Entwurf an die Regelung der EU an.[57] Gegenüber dem Vorentwurf wurde sie deutlich eingeschränkt. Im Grund geht es darum, dass bei heikleren Vorhaben eine etwas formalere Beurteilung der Einhaltung des Datenschutzes durchgeführt und dies entsprechend dokumentiert wird. Eine DSFA durchzuführen ist weder besonders kompliziert noch besonders aufwändig. Im Grund besteht sie darin, dass die geplante Datenbearbeitung beschrieben wird, geprüft wird, ob die Bestimmungen des DSG eingehalten werden, die möglichen Risiken der Datenbearbeitung für die betroffene Person identifiziert und dokumentiert werden, ebenso entsprechende Massnahmen zum Schutz der betroffenen Personen.[58] Häufig wird den Risiken für die betroffene Person der Nutzen der Datenbearbeitung, quasi die Interessen an der Bearbeitung, gegenübergestellt und abgewogen, ob die Datenbearbeitung unter diesem Aspekt vertretbar ist, aber zwingend ist diese Interessenabwägung nicht; das DSG schreibt sie auch in der Sache nicht vor. Das alles wird in einem Dokument vom Verantwortlichen festgehalten.

[Rz 49] Die neue Bestimmung schreibt nun vor, dass eine solche DSFA immer dann vorzunehmen ist, wenn eine (geplante) Bearbeitung oder eine Gruppe von vergleichbaren Bearbeitungen ein «**hohes» Risiko** der Persönlichkeit der betroffenen Person mit sich bringen kann[59] (wobei richtigerweise nicht wie in der DSGVO von einer Wahrscheinlichkeit des Risikos die Rede ist, auch wenn dasselbe gemeint ist[60]). Dieses Kriterium des hohen Risikos ist letztlich der springende Punkt bei dieser Bestimmung. Auch die DSGVO orientiert sich am «hohen» Risiko, doch werden dort hohe Risiken etwas anders definiert. Der Bundesrat will ein hohes Risiko nach Art. 20 Abs. 2 E-DSG bereits dann vorliegen wissen, wenn es zu einer umfangreichen Bearbeitung besonders schützenswerter Personendaten kommt, zu einem **Profiling** oder zu einer systematischen Überwachung öffentlicher Bereiche. In der EU besteht heute das Verständnis, dass Dinge wie ein Profiling oder die Bearbeitung besonders schützenswerter Personendaten zwar Hinweise auf ein hohes Risiko sind, sie jedoch nicht *per se* ein solches darstellen, sondern als Faustregel gilt,

57 Art. 35 DSGVO.

58 Art. 20 Abs. 3 E-DSG.

59 Art. 20 Abs. 1 E-DSG.

60 Der Begriff des Risikos umfasst den Faktor der Eintrittswahrscheinlichkeit bereits. Auch wenn der Entwurf nicht wie die DSGVO davon spricht, dass eine Datenbearbeitung «voraussichtlich» zu einem hohen Risiko führt, ist dasselbe gemeint (Botschaft (Fn. 2), S. 123). Dies ist somit kein Swiss Finish.

dass mindestens zwei kritische Aspekte vorliegen müssen.[61] Das macht auch Sinn: Der Begriff des «Profiling» ist zwar ein im Allgemeinen negativ konnotierter Begriff, kommt aber in vielen unterschiedlichen, auch ganz harmlosen Ausprägungen daher – erwähnt sei das oben zitierte Beispiel des Weinhändlers, der Käufer spanischer Weine anschreibt. Wenn der Bundesrat nun festhält, dass ein Profiling immer ein hohes Risiko für die Persönlichkeit einer Person darstellt, so ist dies ein nicht sachgerechter und auch völlig unnötiger Swiss Finish. Der Weinhändler (Rz. 27) müsste eine DSFA durchführen, was Unsinn ist. Genauso wenig taugen die beiden anderen Beispiele in Art. 20 Abs. 2 E-DSG. Es ist nicht erforderlich, im DSG abstrakt und pauschal zu definieren, wann ein hohes Risiko vorliegt. Dies hängt, wie der erste Satz von Art. 20 Abs. 2 E-DSG selbst festhält, von diversen Umständen ab. So könnte beispielsweise das Führen von Personaldossiers und die Administration von Krankentagen in grösseren Unternehmen als «umfangreiche Bearbeitung von besonders schützenswerten Personendaten» gelten, was bedeutet, dass dies als «hohes» Risiko für die betroffenen Personen gelten würde und eine DSFA durchgeführt werden müsste (im Gegensatz zu kleinen Unternehmen, die zwar dasselbe tun, aber mit viel weniger Mitarbeitern). Das ist nicht sachgerecht. Zwar hält der Entwurf fest, dass keine solche für jene Datenbearbeitungen durchgeführt werden muss, die der Erfüllung einer gesetzlichen Pflicht des Verantwortlichen dienen.[62] Da diese Ausnahme gemäss Botschaft jedoch nicht gelten soll, wo Daten nicht ausschliesslich zur Erfüllung einer gesetzlichen Pflicht erfolgen,[63] würde sie hier nicht greifen: Unternehmen führen die genannten Daten zwar auch zur Erfüllung gesetzlicher Pflichten, aber eben nicht nur. Sinnvoller wäre es, wenn der Bundesrat gewisse konkrete Datenbearbeitungen auf Verordnungsstufe ausnimmt, für die eine DSFA keinen Sinn macht.

[Rz 50] Keinen Sinn macht im Übrigen auch die Ausnahme für Bearbeitungen, für die eine **Datenschutzzertifizierung** vorliegt:[64] Wer eine solche Zertifizierung will, muss bereits für die Zertifizierung im Ergebnis eine DSFA durchführen. Die Ausnahme bringt also nichts.

[Rz 51] Wurde eine DSFA durchgeführt und stellt sich heraus, dass ungeachtet der getroffenen Massnahmen die Bearbeitung zu einem hohen Risiko für die Person führt, so muss nach Art. 21 E-DSG die geplante Bearbeitung **dem EDÖB zur Beurteilung vorgelegt** werden. Die Formulierung im Entwurf ist leider nicht geglückt; sie erweckt den Eindruck, dass der EDÖB selbst dann konsultiert werden muss, wenn dank der getroffenen Massnahmen kein hohes Risiko mehr resultiert, was aber mit Blick auf die Regel der DSGVO nicht zutrifft.[65] Seitens EDÖB ist die Rede von einer Stellungnahme und dem Recht, Massnahmen vorzuschlagen, und nicht einer Genehmigung des EDÖB, die einzuholen ist; freilich steht es dem EDÖB frei, von sich aus ein Verfahren zu eröffnen und in diesem Zusammenhang auch Anordnungen zu treffen. Für seine Stellungnahme hat der EDÖB zwei Monate Zeit, und er kann die Frist bei komplexen Verhältnissen verlängern. Das wird es für Unternehmen besonders interessant machen, die alternative Vorgehensweise zu wählen: Die Bestellung eines Datenschutzberaters nach Art. 9 E-DSG. Besteht ein solcher, kann dieser anstelle des EDÖB konsultiert werden.[66]

---

61 Vgl. die Leitlinie der Artikel-29-Datenschutzgruppe zu Datenschutz-Folgenabschätzungen vom 4. Oktober 2017 (WP248, Rev. 01) (http://ec.europa.eu/newsroom/document.cfm?doc_id=47711).

62 Art. 20 Abs. 4 E-DSG.

63 Botschaft (Fn. 2), S. 125.

64 Art. 20 Abs. 5 E-DSG.

65 Leitlinie der Artikel-29-Datenschutzgruppe zu Datenschutz-Folgenabschätzungen vom 4. Oktober 2017 (WP248, Rev. 01) (http://ec.europa.eu/newsroom/document.cfm?doc_id=47711), S. 18.

66 Art. 21 Abs. 4 E-DSG.

10. Weitere flankierende Massnahmen: Auftragsbearbeitung, Datenschutzberater, Verhaltenskodizes und Inventar

[Rz 52] Die Art. 8 bis 12 E-DSG enthalten diverse flankierende Massnahmen, die die Durchsetzung des Datenschutzes im Betrieb unterstützen sollen.

[Rz 53] Keine grosse Änderung erfährt die **Auftragsbearbeitung**, die neu in Art. 8 E-DSG geregelt ist. Neu ist hier im Wesentlichen nur die Regelung, dass eine Unterbeauftragung (d.h. der Beizug von *Sub-Processors*) nur mit Genehmigung des Verantwortlichen erfolgen kann. Die Regelung entspricht der Vorgabe der DSGVO, die allerdings auch eine stillschweigende Zustimmung gelten lassen will: Will der Auftragsbearbeiter einen Unterbeauftragten beiziehen, so genügt es, wenn er im Vertrag mit dem Verantwortlichen diesem diesbezüglich ein zeitlich befristetes Vetorecht einräumt, was in der Praxis zum Beispiel bei den grossen Cloud-Providern der Regelfall sein wird.[67] Dies gilt auch in der Schweiz.[68] Daraus ergibt sich auch, dass der Auftraggeber (wie schon bisher) lediglich eine indirekte Kontrolle über die Unterauftragnehmer haben muss, d.h. mit diesen keine direkte Vertragsbeziehung nötig ist.

[Rz 54] Besondere Formvorschriften für Verträge mit Auftragsbearbeitern gibt es keine, und die Idee des Vorentwurfs, dass der Bundesrat Vorgaben für solche Verträge auf dem Verordnungsweg erlassen muss, wurde offenbar fallengelassen.[69] Die Vorgaben der DSGVO[70] dürften allerdings auch in der Schweiz zum Standard werden. Zu begrüssen ist in der Botschaft die Absage an die in der Lehre teilweise vertretene, aber praxisfremde und unzutreffende Ansicht, das Berufsgeheimnis etwa nach Art. 321 des Schweizerischen Strafgesetzbuches (StGB; SR 311.0) stehe einem Outsourcing der Datenbearbeitung ohne Einwilligung der betroffenen Personen grundsätzlich entgegen.[71]

[Rz 55] Verständlich, aber trotzdem falsch ist hingegen die Behauptung der Botschaft, die Datenbearbeitung innerhalb derselben juristischen Person stelle grundsätzlich keine Auftragsbearbeitung dar;[72] selbstverständlich ist die Übertragung einer Datenbearbeitung an Personen, die keine Organe der juristischen Person sind, immer eine Auftragsbearbeitung, ganz gleich, wo diese Personen sich befinden, organisatorisch eingegliedert sind oder in welchem Rechtsverhältnis (Arbeitsvertrag, Mandat, Werkvertrag etc.) sie zur juristischen Person als dem Verantwortlichen stehen: Es sind andere Personen, und ihr Verhalten wird – anders als im Falle der Organe – nicht automatisch der juristischen Person zugerechnet. Die Frage braucht hier aber nicht weiter erörtert zu werden, weil sie in der Praxis im Allgemeinen auch von Seiten der Behörden nicht beachtet wird und daher von geringer Relevanz ist (vgl. aber Rz. 73).

[Rz 56] Auf vielfachen Wunsch führt der Entwurf in Art. 9 E-DSG neu die Funktion des **Datenschutzberaters** ein; im Vorentwurf war nichts vorgesehen, was heftig kritisiert wurde. Die Bezeichnung verdeutlicht gegenüber der heutigen Terminologie des Datenschutzverantwortlichen, dass die neue Funktion lediglich beratend wirkt, d.h. er hat keine Befugnisse, gegen unzulässige Datenbearbeitungen vorzugehen, ist für solche (in seiner Rolle) aber auch nicht verantwortlich.

67 Art. 28 Abs. 2 DSGVO.

68 Botschaft (Fn. 2), S. 95.

69 Botschaft (Fn. 2), S. 94 f.

70 Art. 28 DSGVO.

71 Botschaft (Fn. 2), S. 94, m.w.H.

72 Botschaft (Fn. 2), S. 95.

Ihn trifft insbesondere kein Strafbarkeitsrisiko, ausser, er ist nicht mehr beratend, sondern entscheidend und ausführend tätig (z.B. bei der Beantwortung von Auskunftsbegehren). Er muss zwar intern unabhängig sein und über das nötige Fachwissen verfügen, muss aber weder spezifische interne Kompetenzen haben (z.B. Zugangsrechte), noch spezifische Aufgaben (z.B. Prüfung von Datenbearbeitungen auf ihre Konformität). Damit fällt der Entwurf deutlich hinter die heutige Regelung in Art. 12b Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11) zurück, was nicht wirklich nachvollziehbar ist. Anders als in der EU gibt es für kein Unternehmen eine Pflicht, einen Datenschutzberater zu ernennen. Es gibt nur einen einzigen Anreiz für die Ernennung: Datenschutz-Folgenabschätzungen müssen nicht mehr dem EDÖB gezeigt werden, sofern diesbezüglich der eigene Datenschutzberater konsultiert wurde. Hier wären weitere Anreize sinnvoll gewesen. Sinnvoll – weil auch den EDÖB entlastend – wäre zum Beispiel eine Ergänzung von Art. 22 E-DSG (*Data Breach Notifications*), wonach die Meldung an den Beauftragten unterbleiben kann, wenn der Datenschutzberater bereits beurteilt hat, ob das Unternehmen angemessen auf die Verletzung der Datensicherheit reagiert hat. Weil die K108 eine Meldepflicht an die Behörde erfordert, kann diese Ausnahme zugunsten von Firmen mit Datenschutzberatern in vernünftiger Weise gedeckelt werden (siehe unten Rz. 63 ff.). Ein weiterer Anreiz wäre es, für Unternehmen mit Datenschutzberater auch die Meldung nach Art. 13 Abs. 2 Bst. b E-DSG auszunehmen.

[Rz 57] In praktisch nichts zerfallen ist auch die im Vorentwurf angedachte Idee der «Empfehlungen der guten Praxis», die private Stellen hätten ausarbeiten und sich genehmigen lassen können, und deren Einhaltung dann verbindlich als DSG-konform gegolten hätte. So spannend und innovativ die Idee war, so war sie trotz allem unausgegoren und es stand zu wenig Zeit zur Verfügung, die vielen sich stellenden Fragen vernünftig zu lösen. Dies hat der Bundesrat erkannt und die Regelung in Art. 10 E-DSG zu einer banalen Regelung zu **Verhaltenskodizes** eingedampft. Demnach können Berufs- und Wirtschaftsverbände solche dem EDÖB zur Beurteilung vorlegen. Eine besondere Rechtswirkung hat das nicht, und es bleibt abzuwarten, welche faktische Wirkung sie haben. Die Beschränkung auf die Verbände soll vermutlich sicherstellen, dass nicht einzelne Unternehmen sich mittels auf sie zugeschnittene Kodizes einen Wettbewerbsvorteil verschaffen und damit anderen Unternehmen, die ihre Daten zwar ebenfalls datenschutzkonform bearbeiten, aber eben anders, schaden. Der Autor dieser Zeilen bezweifelt, dass diese Bestimmung von grösserer Bedeutung sein wird, wenn es auf die Initiative der Wirtschaft ankommt und die Verhaltenskodizes keine Rechtswirkung haben. Immerhin erlaubt sie der Schweiz zu behaupten, sie fördere die Selbstregulierung auch im Datenschutz.

[Rz 58] Mehr Wirkung hätte die Bestimmung, wenn ein Weg gefunden würde, wie die Wirtschaft mit Verhaltenskodizes allfälligem Soft Law seitens des EDÖB «zuvorkommen» könnte. Heute entsteht solches so, dass der EDÖB sich eine Branche vornimmt, einen Anbieter herauspickt, dessen Praktiken untersucht und mit ihm schliesslich Anpassungen an den Datenbearbeitungen aushandelt, wo diese erforderlich erscheinen. Die dort bilateral gefundenen Lösungen betrachtet der EDÖB dann regelmässig als Musterlösungen für die gesamte Branche. Das ist insofern problematisch, als die Verhältnisse bei anderen Unternehmen der Branche anders sein können. Auch erfolgt die Bildung dieses Soft Laws quasi im stillen Kämmerchen. Hier könnten die Kodizes eine sinnvolle Alternative darstellen. Allerdings müsste Art. 10 E-DSG dahingehend ergänzt werden, dass der EDÖB bei aus seiner Sicht bestehendem Handlungsbedarf eine Branche einladen kann, einen Kodex zu erarbeiten, um bestimmte, sich abzeichnende Probleme zu lösen, bevor der EDÖB

selbst aktiv wird. Ohne eine solche Kompetenz wird der EDÖB nicht entsprechend handeln können.

[Rz 59] Bleibt die Norm so, wie sie ist, dürfte die Entwicklung jedoch ähnlich sein wie im Bereich der Datenschutz-Zertifizierungen, die im freiwilligen Bereich ebenfalls ein Schattendasein führten, seit sie bei der letzten Revision vor bald zehn Jahren eingeführt wurden. Daran wird auch die neue Regelung in Art. 12 E-DSG nichts ändern. Immerhin können neu auch Dienstleistungen nach DSG zertifiziert werden, was den Anwendungsspielraum etwas vergrössert. Ob sich der Aufwand lohnt angesichts des Werbenutzens, der mit einer Zertifizierung erreicht werden kann, erscheint zweifelhaft. Wichtiger wäre wohl eine Zertifizierung nach DSGVO. Die Formulierung von Art. 12 E-DSG ist übrigens missverständlich. Nach dem Wortlaut des Gesetzes können nur Systeme, Produkte und Dienstleistungen zertifiziert werden, nicht aber Organisationen und Verfahren. Erst aus der Botschaft wird klar, dass der Begriff der Systeme im revidierten DSG nicht mehr die bisherige Bedeutung haben soll, sondern Organisationen und Verfahren meint (die Botschaft spricht von «Datenbearbeitungssystemen», was an sich falsch ist; wenn schon sollte von Datenschutzmanagementsystemen die Rede sein), während Systeme im wahren Wortsinne als Produkte gelten.

[Rz 60] Die flankierende Bestimmung, die den grössten Aufwand für die Unternehmen mit sich bringen wird, ist jedoch die **Inventarpflicht** nach Art. 11 E-DSG. Demnach ist vom Verantwortlichen wie auch vom Auftragsbearbeiter (je aus ihrer Warte und unabhängig voneinander) ein Verzeichnis der Bearbeitungstätigen zu führen. Art. 11 E-DSG wurde nach dem Vorbild der DSGVO gestaltet. Auch hier sind die Staaten anzugeben, in welche exportiert wird,[73] was ebenfalls der Vorgabe der DSGVO entspricht.[74]

[Rz 61] Für einen Auftragsbearbeiter wird die einfachste Methode zur Inventarpflicht eine Dokumentation der Verträge mit den Verantwortlichen sein; sie enthalten in der Regel alle nötigen Angaben – ausser der erwähnten Liste der Staaten, die häufig gar nicht offengelegt werden.

[Rz 62] Im Gegensatz zur DSGVO sieht der Entwurf des Bundesrates eine Ausnahmeregelung vor, die auch tatsächlich greifen kann: Unternehmen mit weniger als 50 Mitarbeiter (EU: 250) und Datenbearbeitungen mit geringem Risiko können vom Bundesrat ausgenommen werden. Noch vernünftiger wäre es, wenn er Datenbearbeitung mit geringem Risiko bei allen Unternehmen ausnimmt. Für viele Betriebe ist es eine grössere Herausforderung, ein Verzeichnis aller Datenbearbeitungen zu erstellen. Allerdings kann einem Unternehmen wenig geschehen, wenn es das Inventar nicht erstellt: Weder ist die Verletzung von Art. 11 E-DSG strafrechtlich sanktioniert, noch stellt sie eine Persönlichkeitsverletzung dar. Einzig der EDÖB kann aktiv werden, wenn er davon erfahren sollte.

11. Data Breach Notifications: Bundesrat übt Zurückhaltung gegenüber DSGVO

[Rz 63] Eine weitere konzeptionelle Neuerung im Schweizer Datenschutz wird die Einführung einer Pflicht zur Vornahme von *Data Breach Notifications* sein. Verantwortliche sollen verpflichtet sein, gewisse Verletzungen des Datenschutzes von sich aus dem EDÖB und ggf. den betroffenen

73 Art. 11 Abs. 2 Bst. g E-DSG.

74 Art. 30 Abs. 1 Bst. d DSGVO.

Personen zu melden. Das heutige Recht kennt keine Meldepflicht gegenüber dem EDÖB, auch wenn dieser natürlich das Recht hat, Datenschutzverletzungen aufzuklären und Verantwortliche ihm umgekehrt auf freiwilliger Basis Meldung erstatten können, was auch immer wieder geschieht. Neu wird dies formalisiert: Liegt eine «Verletzung der Datensicherheit» vor, so ist dies nach Art. 22 Abs. 1 E-DSG **dem EDÖB zu melden**, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeitsrechte der betroffenen Person führt.[75] In der Meldung ist dem EDÖB mitzuteilen, was geschehen ist, was die Folgen sind und welche Massnahmen ergriffen wurden oder werden. Dies soll ihm die Möglichkeit geben, bei Bedarf zum Schutz der betroffenen Personen zu intervenieren, insbesondere falls das Unternehmen seiner Meinung nach nicht angemessen reagieren sollte.

[Rz 64] Der Begriff der **Verletzung der Datensicherheit** ist in Art. 4 Bst. g E-DSG extrem breit definiert. Es soll dies gemäss Botschaft jeden Vorgang erfassen, bei welchem Personendaten verloren gehen, gelöscht, vernichtet, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden.[76] Das geht weit. Eine versehentliche Löschung einer Datei auf dem eigenen PC fällt ebenso darunter wie die an einen falschen Empfänger versandte E-Mail. Klar ist aufgrund der Legaldefinition, dass es nicht darauf ankommt, ob die Verletzung absichtlich oder widerrechtlich erfolgte, mithin eine Datenschutzverletzung darstellt. Da beabsichtigt ist, dass sie inhaltlich der Parallelregelung in der DSGVO[77] entspricht, ist der Begriff wohl etwas einschränkender zu verstehen als die Botschaft suggeriert: Es kommt nicht bloss darauf an, ob es zu den besagten Vorgängen kommt. Erforderlich ist vielmehr, dass die Vorgänge nicht gewollt sind und daher Massnahmen getroffen wurden, um sie zu verhindern, die jedoch im konkreten Fall versagt haben oder ungenügend waren. Dies können technische Massnahmen sein, die einen unbefugten Datenzugriff verhindern sollen, aber auch organisatorische Massnahmen wie etwa Weisungen, also Massnahmen, wie sie Art. 7 E-DSG verlangt. Werden also keine Schutzvorkehrungen getroffen und Personendaten für alle frei abrufbar gespeichert, stellt der Zugriff durch Unbefugte darauf keine Verletzung der Datensicherheit dar. Es gab in diesem Fall keine (Massnahmen zur) Datensicherheit, die verletzt werden konnte(n). Eine solche Verletzung liegt somit dann vor, wenn der Gewahrsam des Verantwortlichen über die von ihm kontrollierten Personendaten von ihm ungewollt gebrochen wird, ob durch Löschung, Offenlegung oder Veränderung.

[Rz 65] Die Schweizer Meldepflicht geht in verschiedener Hinsicht weniger weit als jene der DSGVO. Dies ist zu begrüssen. So sind zunächst nur jene Verletzungen zu melden, die voraussichtlich zu einem **hohen Risiko** führen, während in der DSGVO faktisch alle Fälle, die ein Risiko mit sich bringen, zu melden sind.[78] Die DSGVO sieht in Fällen von hohem Risiko zusätzlich die Benachrichtigung der betroffenen Person vor.[79] Wann ein solcher Fall vorliegt, erläutert auch die Botschaft nicht; der Begriff ist nicht identisch mit dem «hohen» Risiko, der eine Datenschutz-Folgeneinschätzung nach Art. 20 E-DSG auslöst. Die Botschaft spricht von «schwerwiegenden» Risiken[80].

---

75 Die Bestimmung spricht auch von einem hohen Risiko für die Grundrechte der betroffenen Person. Dies betrifft nicht die Bearbeitung durch private Datenbearbeiter.

76 Botschaft (Fn. 2), S. 84.

77 Botschaft (Fn. 2), S. 84.

78 Art. 33 Abs. 1 DSGVO.

79 Art. 34 Abs. 1 DSGVO.

80 Botschaft (Fn. 2), S. 128.

[Rz 66] Eine falsch versandte E-Mail an einen vertrauenswürdigen Empfänger, der die Mail voraussichtlich nicht missbrauchen wird, dürfte beispielsweise nicht meldepflichtig sein. Der Verlust eines Notebooks, auf dem alle Daten verschlüsselt gespeichert sind, ebenfalls nicht, jedenfalls wenn die Daten noch anderweitig verfügbar sind. Zwar läge auch in diesem Fall eine Verletzung der Datensicherheit vor: Sie erfasst nicht nur die Bekanntgabe von Personendaten an Unbefugte (wozu es dank der Verschlüsselung nicht kommen wird), sondern auch den Verlust der Daten. Konsequenzen wird er jedoch keine haben, weshalb auch keine Meldung erforderlich ist. Dasselbe wäre der Fall, wenn in einem Unternehmen kurzzeitig alle Mitarbeiter auf die sonst vertraulichen Personaldaten zugreifen könnten, aber unwahrscheinlich ist, dass keine Zugriffe erfolgten. Der Hack einer Datingbörse, bei welcher – wie tatsächlich geschehen – die Identitäten eines Grossteils der Benutzer veröffentlicht werden, wäre hingegen ein meldepflichtiger Fall. Werden wiederum aus einem Online-Shop die Kreditkartendaten gestohlen, ist dies nicht unbedingt meldepflichtig: Werden die Karten rasch gesperrt und beobachtet die Kartengesellschaft die betroffenen Kundenkonten auf Missbräuche hin, dürfte sich das Risiko der Kunden in Grenzen halten, erst Recht, was deren Persönlichkeitsrechte betrifft. Die negativen Folgen werden sich in den mit dem Wechsel einer Kartennummer verbundenen Umtrieben erschöpfen. Dasselbe gilt, wenn eine Bank einem Kunden versehentlich die Unterlagen eines anderen Kunden sendet, aber in der Folge die Unterlagen zurückerhält oder anderweitig davon auszugehen ist, dass die Unterlagen nicht missbraucht oder weiter offengelegt werden.

[Rz 67] Auf den ersten Blick unbestimmt ist, ob das «hohe Risiko» gemäss Art. 22 E-DSG sich nicht nur auf die Qualität der Verletzung bezieht, sondern auch auf deren Quantität. Werden vertrauliche Daten einer Person gestohlen, so kann dies für diese erhebliche Konsequenzen haben. Ist aber nur eine einzige Person betroffen, rechtfertigt es sich nicht, dass der EDÖB involviert wird. Dies macht im Hinblick auf seine beschränkten Ressourcen erst Sinn, wenn eine Vielzahl von Personen betroffen ist. Erfahrungen aus dem Ausland, wo Behörden aufgrund **fehlender De-Minimis-Regelungen** mit Meldungen geflutet wurden, zeigen dies. Dies gilt auch mit Bezug auf die Pflicht, Verletzungen den betroffenen Personen mitzuteilen. Hier hat sich in Ländern mit solchen Pflichten eine regelrechte «*Data Breach Fatigue*» entwickelt, wie inzwischen durch eine Studie belegt ist:[81] Die Meldungen werden nur noch von einer Minderheit beachtet. Dieser Gedanke scheint auch der schweizerische Gesetzgeber zu verfolgen, wie die milde Ausgestaltung der Meldepflicht an die betroffenen Personen verdeutlicht (siehe nachfolgend Rz. 70). Von einem hohen Risiko im Sinne von Art. 22 E-DSG sollte daher nur dann ausgegangen werden, wenn die Verletzung nicht nur qualitativ, sondern auch quantitativ schwerwiegende Folgen haben kann, eine Meldung an den EDÖB also beispielsweise erst erfolgen muss, wenn mutmasslich 10'000 oder mehr Personen betroffen sind. Dies sind die Fälle, auf die der EDÖB seine Energie setzen soll; selbstverständlich kann er aufgrund seiner Kompetenzen stets auch Fälle mit geringerer Tragweite untersuchen, wenn er davon erfährt. Die Zahl von 10'000 mag auf den ersten Blick hoch erscheinen, ist heute jedoch in Zeiten der automatisierten Datenbearbeitung rasch erreicht; schon eine E-Mail-Newsletter-Datenbank kann rasch diese Grösse erreichen. Eine solche Schranke bedeutet auch nicht, dass das Unternehmen bis zu dieser nichts zu tun hat, sondern lediglich, dass hier nicht zwingend der EDÖB involviert werden muss. So bestätigte kürzlich auch eine inter-

81 Dazu Andrew Bolson, If Not All Data Breaches Are Created Equal, Why Are All Data Breach Notifications Treated the Same? (https://iapp.org/news/a/if-not-all-data-breaches-are-created-equal-why-are-all-data-breach-notifications-treated-the-same/; Studie: http://www.experian.com/data-breach/2014-aftermath-study-consumer-sentiment.html).

nationale Data-Breach-Studie aus den USA, wo seit Jahren Meldepflichten bestehen und daher auch statistische Zahlen vorliegen, dass Fälle mit weniger als 10'000 Datensätzen vernachlässigbar waren.[82] Im Hinblick auf die formale Natur dieser Bestimmung wäre es jedoch für die Rechtssicherheit wichtig, wenn die Kriterien, ab wann eine Verletzung gemeldet werden muss, auf Verordnungsstufe weiter konkretisiert werden. Ein entsprechender Regelungsauftrag sollte in Art. 22 E-DSG vorgesehen werden. Er sollte überdies auch das Verfahren der Meldung regeln, das möglichst einfach sein sollte, z.B. über ein Online-Formular, das seitens der Unternehmer keinen grossen Aufwand erfordert.

[Rz 68] Weniger weit als die DSGVO geht der Entwurf auch mit Bezug auf die **Meldefristen**: Zu melden ist so rasch wie möglich, was aber bedeutet, dass erst dann gemeldet werden muss, wenn alle relevanten Informationen beisammen sind, so dass sich der EDÖB ein vernünftiges Bild der Lage machen kann. Die DSGVO verlangt hingegen eine Meldung innert 72 Stunden und Teilinformationen, was wenig sinnvoll ist. Häufig ist nach Entdeckung eines Zwischenfalls noch nicht klar, welches Ausmass dieser hat und welche Massnahmen schlussendlich sinnvoll sind. Wichtiger ist in solchen Fällen, dass der Verantwortliche sich der Verletzung und Minderung von Schäden widmet, nicht der Information des EDÖB.

[Rz 69] Weniger weit als die DSGVO geht der Bundesrat schliesslich bezüglich der **Protokollierung** der Verletzungen der Datensicherheit. Die DSGVO sieht eine entsprechende Pflicht vor,[83] der Entwurf anders noch als der Vorentwurf nicht mehr. Dies erscheint auch sinnvoll.

[Rz 70] Die **betroffene Person** muss informiert werden, «wenn es zu ihrem Schutz erforderlich ist» (oder der EDÖB es verlangt, was hoffentlich dasselbe bedeutet).[84] Auch diese Regelung grenzt sich im Hinblick auf die bereits erwähnte *Data Breach Fatigue* sinnvollerweise von der Regelung der DSGVO ab[85], welche eine starre Pflicht zur Notifikation vorsieht. Die Pflicht zur Information der betroffenen Person ist unabhängig von jener zur Notifikation des EDÖB. Sie kann auch früher einsetzen, oder in Fällen, in denen der EDÖB gar nicht informiert werden muss, weil der Schutz der betroffenen Person auch dann sichergestellt werden muss, wenn das damit verbundene Risiko nicht hoch ist. Dies kann sich somit durchaus als *Swiss Finish* auswirken und insofern vor allem für Konzerne problematisch sein, die europaweite Data-Breach-Prozesse aufbauen wollen und somit für die Schweiz bezüglich der Meldung an betroffene Personen eine eigene Regelung vorsehen müssen, auch wenn sie sinnvoll erscheint (und sich eine solche Pflicht abgesehen davon auch aus anderen, schon heute geltenden Grundsätzen des Schweizer Rechts ergeben kann). Immerhin sieht die Regelung **Ausnahmen** vor, so namentlich dann, wenn die Information der betroffenen Person unmöglich wäre oder einen unverhältnismässigen Aufwand verursachen würde.[86] Alternativ kann ein Unternehmen die Information auch durch öffentliche Bekanntmachung (z.B. auf der eigenen Website) vornehmen,[87] allerdings müsste die Wirkung vergleichbar sein, was nur selten der Fall sein wird. Zu beachten ist, dass der Grundsatz der Bearbeitung nach Treu und Glauben, Art. 6 Abs. 1 E-DSG und vertragliche Nebenpflichten einen Verantwortlichen dazu

82 Benjamin Edwards, Steven Hofmeyr, Stephanie Forrest, Hype and heavy tails: A closer look at data breaches, in: Journal of Cybersecurity, Volume 2, Issue 1, 1. Dezember 2016, S. 3–14 (https://doi.org/10.1093/cybsec/tyw003).

83 Art. 33 Abs. 5 DSGVO.

84 Art. 22 Abs. 4 E-DSG.

85 Art. 34 Abs. 1 DSGVO.

86 Art. 22 Abs. 5 Bst. b E-DSG.

87 Art. 22 Abs. 5 Bst. c E-DSG.

verpflichten können, nebst der Informationspflicht auch weitere Massnahmen zur Schadensminderung vorzunehmen.

[Rz 71] Der **Auftragsbearbeiter** wird ebenfalls zur Meldung verpflichtet, allerdings an den Verantwortlichen. Während die DSGVO eine «unverzügliche» Meldung erfordert[88], hat in der Schweiz eine Meldung an den Verantwortlichen so rasch als möglich zu erfolgen, was aus den bei der EDÖB-Meldung genannten Gründen zu Recht weniger streng sein kann – je nach Interpretation der Begriffe.[89] Wichtig ist hierbei, dass keine Einschränkung mit Bezug auf die sich daraus ergebenden Risiken vorgesehen ist. Daher ist an sich jede auch noch so kleine Verletzung der Datensicherheit zu melden. Die Logik dieser Regel ist, dass der Verantwortliche darüber befinden soll, was er wem weitermeldet und was nicht. In der Praxis wird sie freilich nicht vernünftig zu erfüllen sein. Es macht schlicht keinen Sinn, wenn der Auftragsbearbeiter jede verlorene Datei, deren Verlust keine Konsequenzen hat, protokolliert und seinem Kunden meldet. Sinnvoller wäre auch hier eine Regelung, dass nicht gemeldet werden muss, wo selbst für den Auftragsbearbeiter absehbar ist, dass die Verletzung keine relevanten Folgen haben wird.

[Rz 72] Zu prüfen ist, wie vorne erwähnt, ferner, ob auf eine Pflicht zur Meldung an den EDÖB nicht ganz oder jedenfalls für einen Grossteil der Fälle verzichtet werden kann, wenn sich stattdessen ein Datenschutzberater im Sinne von Art. 9 E-DSG um die Sache kümmert. Es wäre dies ein analoges System wie in Art. 21 Abs. 4 E-DSG für Datenschutz-Folgenabschätzungen.

[Rz 73] Mit einer Besonderheit wartet die Schweizer Regel ferner noch auf: Nach Art. 22 Abs. 6 E-DSG kann eine Meldung der Verletzung der Datensicherheit in einem **Strafverfahren** gegen den Meldepflichtigen nur mit dessen Einverständnis verwendet werden. Damit soll der Grundsatz, dass niemand gezwungen werden kann, sich selbst zu belasten, umgesetzt werden. Die Bestimmung ist in verschiedener Hinsicht speziell:

- *Erstens* betrifft sie zwar die Meldung an den EDÖB (durch den Verantwortlichen) und an den Verantwortlichen (durch den Auftragsbearbeiter), wohl aber nicht an die betroffene Person, da sie nicht den Charakter einer Meldung hat und hier auch nicht vorgeschrieben ist, was genau der betroffenen Person mitzuteilen ist. Der Verantwortliche muss somit vorsichtiger sein, wenn er die betroffene Person informiert als wenn er den EDÖB informiert.
- *Zweitens* schützt die Regel von Art. 22 Abs. 6 E-DSG nur im Strafverfahren, nicht vor zivilrechtlichen Ansprüchen; ein Zivilkläger wird somit über das Öffentlichkeitsgesetz beim EDÖB die entsprechende Meldung der Verletzung herausverlangen und für seinen Zivilprozess verwenden können.
- *Drittens* ist der Meldepflichtige typischerweise nicht derjenige, der strafrechtlich verfolgt wird und geschützt werden sollte (z.B. wenn die Verletzung der Datensicherheit gleichzeitig eine strafbare Verletzung eines Berufsgeheimnisses darstellt). Ersteres wird ein Unternehmen sein, letzteres einzelne Angestellte. Damit erweist sich die Regel in diesen Fällen als nutzlos, denn zu einem Strafverfahren gegen den Meldepflichtigen (d.h. den Auftragsbearbeiter oder den Verantwortlichen) wird es kaum je kommen. Folgt man der Ansicht des Bundesrates, sind die einzelnen Mitarbeiter selbst nicht als meldepflichtig zu qualifizieren, da sie gemäss Botschaft nicht als Auftragsbearbeiter gelten (Rz. 55).[90] Damit wäre die Bestimmung

88 Art. 33 Abs. 2 DSGVO.

89 Art. 22 Abs. 3 E-DSG.

90 Botschaft (Fn. 2), S. 95.

ein Schlag ins Wasser. Werden Mitarbeiter hingegen richtigerweise als Auftragsbearbeiter betrachtet, macht nicht nur diese Bestimmung Sinn, sie würde auch dazu führen, dass Mitarbeiter verpflichtet wären, Verletzungen der Datensicherheit, die ihnen unterlaufen, von sich aus zu melden. Sie wären dann strafrechtlich insofern vor Verfolgung geschützt, wenn die Meldung gesetzeskonform («aufgrund dieses Artikels») erfolgte, nämlich so rasch wie möglich, und die Verletzung ihnen nicht anders nachgewiesen werden kann. Art. 22 Abs. 6 E-DSG schützt nicht pauschal vor Verfolgung, sondern nur vor der Verwendung der Meldung gegen die Person.

[Rz 74] Die Verletzung der Meldepflicht ist notabene anders als noch im Vorentwurf strafrechtlich nicht sanktioniert. Wenn ein Verantwortlicher oder Auftragsbearbeiter nicht meldet, wird dies für ihn in aller Regelung keine Konsequenzen haben. Schlimmstenfalls kann der EDÖB ihn zur Einführung und Befolgung eines entsprechenden Prozesses zwingen.

[Rz 75] In diesem Zusammenhang wird auch der **extraterritoriale Geltungsbereich der DSGVO** eine besondere Rolle spielen: Unterliegt ein Unternehmen in der Schweiz der DSGVO, besteht eine Meldepflicht im Falle von Verletzungen der Datensicherheit auch gegenüber den zuständigen nationalen Datenschutzbehörden. Diese wird aufgrund der strengeren Regelung der DSGVO in mehr Fällen und unter Umständen früher erforderlich sein als unter dem neuen DSG. Über die Fragen, wann ein Unternehmen in der Schweiz der DSGVO unterliegt, wird derzeit besonders aktiv diskutiert, da inzwischen mit guten Gründen auch einschränkende Auslegungen vertreten werden – sowohl für die Fälle, in denen ein Schweizer Unternehmen seine Datenbearbeitung in der EU durchführen lässt[91] als auch mit Bezug auf die Frage, wie deutlich ein Unternehmen sich auf den EU-Markt ausrichten muss, um in den Anwendungsbereich von Art. 3 Abs. 2 Bst. a DSGVO zu fallen (Marktortprinzip). Mindestens in den Fällen, in denen nicht beabsichtigt ist, Daten von Personen mit Wohnsitz in der EU zu bearbeiten, löst sich das Problem der Meldepflicht und der ausländischen Datenschutzaufsicht aber auf andere Weise: Die nationalen Datenschutzbehörden in der EU sind gar nicht zuständig. Dies sind sie nach Art. 50 Abs. 1 DSGVO nur auf dem Hoheitsgebiet ihres eigenen Mitgliedsstaats. Diese Zuständigkeit erstreckt sich zwar durchaus auf extraterritoriale Sachverhalte, die eine gewisse Auswirkung auf das Territorium des Mitgliedsstaats haben. Erwägungsgrund 122 stellt aber auch klar, dass bei einem Unternehmen mit Niederlassung ausserhalb der EU daran angeknüpft wird, ob dessen Verarbeitungstätigkeit auf Personen mit *Wohnsitz* im betreffenden Mitgliedsstaat *ausgerichtet* ist. Ist das nicht der Fall, muss gegenüber der Aufsichtsbehörde auch keine Data Breach Notification vorgenommen werden.

12. Bekanntgabe ins Ausland: Im Ergebnis alles wie gehabt

[Rz 76] Mit Bezug auf die Bekanntgabe von Personendaten ins Ausland ändert sich im Ergebnis nicht viel gegenüber heute. Was heute an Personendaten grenzüberschreitend zugänglich gemacht wurde, darf es auch unter dem revidierten DSG. Für die Wirtschaft ändert sich also nicht viel. Allerdings soll das DSG in technischer Sicht einen Systemwechsel erfahren, wie er bereits im Vorentwurf vorgeschlagen worden ist: Neu liegt es nicht mehr am Datenexporteur zu beurteilen, ob die grenzüberschreitende Bekanntgabe die Persönlichkeit einer Person schwerwiegend

91 Vgl. David Vasella, Zum Anwendungsbereich der DSGVO, in: Digma 2017/4 (noch nicht erschienen).

gefährden würde, namentlich, weil eine Gesetzgebung fehlt, die einen **angemessenen Schutz** gewährleistet. Es ist gemäss Art. 13 Abs. 1 E-DSG neu der Bundesrat, der entscheidet, in welche Länder (und an welche internationale Organisationen) Personendaten ohne weitere Vorkehrungen bekanntgegeben werden dürfen, und in welche nicht.[92]

[Rz 77] Diese Regel ist gegenüber dem Vorentwurf aufgrund von Kritik in der Vernehmlassung nun klarer formuliert worden. Die bisher vom EDÖB geführte Staatenliste wird damit neu vom Bundesrat in Form einer Verordnung mit einer Positiv-Liste erlassen und ist rechtsverbindlich. Das ändert freilich nichts daran, dass die (anderen) Bearbeitungsgrundsätze weiterhin gelten und auch bei einer Bekanntgabe ins Ausland zu berücksichtigen sind. So ist es weiterhin möglich, dass eine Bekanntgabe ins Ausland – selbst in ein Land mit gemäss Bundesrat angemessenem Datenschutz – eine Persönlichkeitsverletzung darstellt, weil sie als unverhältnismässig im Sinne von Art. 5 Abs. 2 E-DSG eingestuft werden muss.

[Rz 78] Besteht kein angemessener Schutz, gibt es zwei Möglichkeiten, wie weiter verfahren werden kann: Entweder wird auf andere Weise ein angemessener Schutz geschaffen («andere Garantien» gemäss Art. 13 Abs. 2 E-DSG), oder aber es greift eine der Ausnahmen (Art. 14 E-DSG). Der Katalog an anderen Garantien und Ausnahmen war bisher in Art. 6 Abs. 2 DSG vereint. Er wurde inhaltlich in verschiedener Hinsicht erweitert.

[Rz 79] Bei den anderen Garantien, die einen «geeigneten» Datenschutz gewährleisten müssen, kann wie in der DSGVO zunächst weiterhin auf die heute gängigen **Standardvertragsklauseln** abgestellt werden; sind diese vom EDÖB anerkannt oder ausgestellt, entfällt sogar die Notifikationspflicht, die heute in Art. 6 Abs. 3 DSG enthalten ist und immer wieder zu Diskussionen mit dem EDÖB führte, weil er sie breiter auslegte als sie es war.

[Rz 80] Beibehalten wurde wie auch in der DSGVO die Möglichkeit von verbindlichen **unternehmensinternen Datenschutzvorschriften**, besser bekannt als *Binding Corporate Rules* (**BCR**), die regelmässig als konzerninterner Vertrag ausgestaltet sind. Neu müssen BCR vom EDÖB nicht nur gesichtet und kommentiert werden, sondern es wird eine formale Genehmigung vorgesehen, wie dies in der EU schon bisher der Fall war und auch unter der DSGVO ist. Eingeschränkt wird nun gegenüber heute die Möglichkeit, mit anderen Garantien zu arbeiten, ob in Form von Verträgen oder anders. Art. 6 Abs. 2 DSG sah keine Einschränkung vor, wie der erforderliche Datenschutz im Rahmen einer Bekanntgabe ins Ausland sichergestellt wird. Neu wird in Art. 13 Abs. 2 E-DSG abschliessend definiert, was benutzt werden kann; immerhin kann der Bundesrat die Liste erweitern.[93]

[Rz 81] Kann weder mit vom EDÖB anerkannten oder ausgestellten Standardvertragsklauseln gearbeitet werden, noch mit BCR, bestehen in Art. 13 Abs. 2 E-DSG noch drei Möglichkeiten:

- Der Verantwortliche entwickelt **eigene Standardvertragsklauseln** und lässt sich diese vom EDÖB genehmigen;[94]

---

92 Soweit hingegen ein Land nur unter bestimmten Voraussetzungen einen angemessenen Datenschutz bietet, wie etwa im Falle einer Selbstzertifizierung eines Unternehmens gemäss dem Swiss-US Privacy Shield, soll dies gemäss Botschaft (Fn. 2), S. 105, neu über Art. 13 Abs. 3 E-DSG abgewickelt werden, was in systematischer Hinsicht sauberer ist, im Ergebnis aber wohl keinen Unterschied macht.

93 Art. 13 Abs. 3 E-DSG.

94 Art. 13 Abs. 2 Bst. d E-DSG.

- Der Verantwortliche kann sich auf eine spezifische Garantie stützen, die ein Bundesorgan zuvor ausgearbeitet (und dem EDÖB mitgeteilt) hat, z.B. im Rahmen einer Vereinbarung im Bereich der internationalen Amtshilfe;[95]
- Der Verantwortliche oder Auftragsbearbeiter schliesst mit seinem Vertragspartner eine **nicht standardisierte Vertragsklausel** ab. In diesen Fällen ist weiterhin keine Genehmigung seitens des EDÖB nötig. Eine Notifikation wie heute unter Art. 6 Abs. 3 DSG genügt aber.[96] Die Stellungnahme des EDÖB muss wie heute rechtlich gesehen nicht abgewartet werden.

[Rz 82] Wie lange sich der EDÖB für eine Genehmigung, die in Form einer Verfügung erfolgt, Zeit lassen darf, ist im E-DSG anders als noch im Vorentwurf nicht geregelt. Es kommt stattdessen die Verordnung über die Ordnungsfristen (OrFV)[97] zur Anwendung, die eine Frist von bis zu drei Monaten vorsieht. Eine solche Frist scheint jedenfalls für BCR als angemessen. Für «normale» Verträge im operativen Bereich wird die Frist jedoch zu lang sein; hier wird daher weiterhin mit den üblichen Standardvertragsklauseln etwa der Europäischen Kommission gearbeitet werden, was problemlos möglich ist.

[Rz 83] In Art. 14 E-DSG sind abschliessend jene **Ausnahme-Situationen** aufgezählt, in denen Personendaten ins Ausland trotz dort mangelndem (gesetzlichen oder vertraglichen) Datenschutz bekanntgegeben werden dürfen. Hier bringt die Revision zusätzliche Möglichkeiten: Die wichtigste Anpassung ist zweifellos, dass Personendaten neu auch ausländischen Behörden übermittelt werden dürfen, wenn dies zur **Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen** erforderlich ist (Abs. 1 Bst. c Ziff. 2). Bisher war dies nur im Rahmen ausländischer Gerichtsverfahren möglich (z.B. im Rahmen einer *pre-trial discovery*). Die zahlreichen Fälle, in denen die Gerichte in den letzten Jahren die Bekanntgabe von Namen von Mitarbeitern und Dritten an das US-Justizministerium zur Beilegung des Steuerstreits mit den USA verboten haben, werden damit quasi Geschichte. Dies entspricht allerdings auch der Rechtslage unter der DSGVO und ist auch in der Sache richtig. Es bedeutet im Übrigen nicht, dass Daten künftig beliebig an ausländische Behörden weitergegeben werden dürfen. Die Bearbeitungsgrundsätze nach Art. 5 E-DSG sind nach wie vor einzuhalten und falls dies nicht der Fall wäre, wird weiterhin eine Interessenabwägung nötig sein (neu nunmehr im Rahmen von Art. 27 E-DSG), wobei nunmehr alle schutzwürdigen Interessen zugunsten einer solchen Bekanntgabe berücksichtigt werden dürfen, und nicht mehr nur die öffentlichen. Gegenüber dem Vorentwurf wurde die Norm insofern präzisiert, als das nicht mehr nur von Verwaltungsbehörden die Rede ist, sondern von «zuständigen» Behörden.

[Rz 84] Gegenüber dem Vorentwurf (und dem heutigen Recht) wurde – analog der Regelung in der DSGVO – in Art. 14 Abs. 1 Bst. b E-DSG weiter festgehalten, dass der Rechtfertigungsgrund des **Abschlusses oder der Abwicklung eines Vertrags** nicht nur Daten des Vertragspartners, sondern auch jener Personen erfasst, in deren Interesse ein Vertrag ist oder sein soll. Auch diese Klarstellung ist nur folgerichtig.

[Rz 85] Der damit verwandte Fall der Bekanntgabe gestützt auf eine Einwilligung wurde im Entwurf gegenüber dem Vorentwurf und heutigen DSG ebenfalls leicht geändert: Neu wird nicht

95 Art. 13 Abs. 2 Bst. c E-DSG.

96 Art. 13 Abs. 2 Bst. b E-DSG.

97 Verordnung über Grundsätze und Ordnungsfristen für Bewilligungsverfahren vom 25. Mai 2011 (Ordnungsfristenverordnung, OrFV; SR 172.010.14).

eine Einwilligung im Einzelfall verlangt, sondern eine **ausdrückliche Einwilligung**. Das ist insofern zu begrüssen, als dass die Formulierung «im Einzelfall» bisher eher unglücklich war. Die Ausdrücklichkeit verlangt neu, dass die betroffene Person darin einwilligen muss, dass ihre Daten in ein Land exportiert werden, ohne dass diese Daten in einer Weise geschützt werden, die aus Sicht des schweizerischen Datenschutzes angemessen wäre. Der klassische Fall ist die Einwilligung in die Publikation von Daten oder die Bekanntgabe an eine Firma oder Behörde im unsicheren Ausland, ohne von dieser eine Zusage zu erhalten, wie sie mit diesen Daten umgehen wird oder die Zusage den hiesigen Anforderungen an den Datenschutz nicht genügt. Die Aussage in der Botschaft, dass die betroffene Person den Namen des Ziellandes kennen muss, ist schlicht falsch, weil sie keinen Sinn macht.[98] Was die Person wissen muss ist, dass ihre Daten nicht oder nicht mehr wie unter schweizerischem Recht erwartet geschützt sind. Vielleicht ist das Land für die Person im konkreten Fall relevant, *ob* sie überhaupt bereit ist, einzuwilligen. Aber die Einwilligung ist gerade deshalb nötig, weil nach der Bekanntgabe eben unter Umständen nicht mehr kontrolliert werden kann, wohin die Daten fliessen, mithin auch in welches weitere Land. Von daher macht es keinen Sinn zu verlangen, dass das Land des ersten Empfängers genannt wird. Eine Einwilligung wird also auch in Zukunft ohne Weiteres pauschal «ins Ausland» oder an einen Empfänger «irgendwo auf der Welt» erfolgen können müssen. Eine Einwilligung in eine Publikation von Daten, die zweifellos zulässig ist (so auch Art. 14 Abs. 1 Bst. e E-DSG, wo notabene keine Ausdrücklichkeit verlangt wird), besagt übrigens nichts anderes. Es stellt sich daher die Frage, was das Kriterium der Ausdrücklichkeit überhaupt noch soll. Nach der hier vertretenen Ansicht kann es bedenkenlos gestrichen werden.

[Rz 86] In diesem Zusammenhang hat der Bundesrat die bisher in der Verordnung zum DSG enthaltene Bestimmung, wonach die **Online-Publikation** von Daten keine Bekanntgabe ins Ausland darstellt, mit einem neuen Art. 15 E-DSG ins Gesetz verschoben. Er hat es allerdings verpasst, die Bestimmung korrekt zu formulieren, da sie weiterhin auf Online-Medien beschränkt ist, in Tat und Wahrheit aber für jede Publikation gelten muss. Wäre dem nicht so, dürften Zeitungs- und Buchverlage oder auch Buchhändler ihre Erzeugnisse nicht mehr ohne Weiteres in Länder ohne angemessenen Datenschutz exportieren, was niemand behaupten will. Die Regel spielte in der Praxis bisher allerdings eine nur untergeordnete Rolle; sie geht auf einen viele Jahre zurückliegenden Gerichtsfall in der EU betreffend eine Website zurück. Da sie nun ausdrücklich ins DSG Eingang finden soll, erscheint es als angezeigt, sie im Zuge der parlamentarischen Beratung entweder zu streichen (weil faktisch im Wesentlichen bereits von Art. 14 Abs. 1 Bst. e E-DSG erfasst) oder richtig zu formulieren, d.h. festzuhalten, dass keine Bekanntgabe von Personendaten ins Ausland vorliegt, wenn einer Person im Ausland bereits publizierte Personendaten zugänglich gemacht werden. Der Rechtsschutz gegen unerwünschte Publikationen ist über die allgemeinen Bearbeitungsgrundsätze (Art. 5 E-DSG) und das Widerspruchsrecht betroffener Personen (Art. 26 Abs. 2 Bst. b E-DSG) schon sichergestellt.

[Rz 87] Im Vorentwurf war noch vorgesehen, dass dem EDÖB Meldung erstattet werden muss, wenn für eine Bekanntgabe von Personendaten auf bestimmte Ausnahmen abgestellt wird, was völlig unpraktikabel gewesen wäre und entsprechend kritisiert wurde. Das wurde nun geändert: Es muss dem EDÖB nun nur noch auf Rückfrage Auskunft erteilt werden, z.B. inwieweit Personendaten für ausländische Gerichts- und Behördenverfahren gestützt auf die Ausnahmebestim-

98 Botschaft (Fn. 2), S. 105.

mung von Art. 14 E-DSG exportiert wurden. Dies ist eine Vorgabe der Konvention. Für die Praxis heisst dies allerdings auch, dass Betriebe **Protokoll** darüber führen müssen, inwieweit sie sich auf die betreffenden Ausnahmen abstützen. Wird das wirklich befolgt, was zu bezweifeln ist, wird das einen erheblichen Aufwand mit sich bringen, ohne, dass dies aus der Vorlage auf den ersten Blick ersichtlich ist und ohne wirklichen Mehrwert für den Datenschutz.

13. Regelung von Daten verstorbener Personen: Ein Fremdkörper

[Rz 88] Mit dem Tod endet die Persönlichkeit einer Person,[99] weshalb Regeln zu deren Daten im DSG, soweit sie nicht auch Dritte betreffen, an sich nichts zu suchen haben. Das heutige DSG kennt eine solche Regelung nur in der Verordnung. Da es hierfür keine Rechtsgrundlage gibt, wurde schon mit dem Vorentwurf eine entsprechende Bestimmung aus Gesetzesstufe vorgeschlagen, und in der Botschaft wird am Prinzip festgehalten, so unter anderem mit Verweis auf Gerichtspraxis und Bestimmungen der Verfassung, die gewisse Wirkungen der Persönlichkeit über den Tod hinaus vorsehen. Die Regel soll im DSG verbleiben und nicht, wie von diverser Seite vorgeschlagen, im Rahmen der laufenden Revision des Erbrechts eingeführt werden, wo ebenfalls ein neues Einsichtsrecht vorgesehen ist. Die Bestimmung bleibt ein Fremdkörper im DSG. Immerhin wurde sie gegenüber dem Vorentwurf inhaltlich etwas bereinigt und gestrafft.

[Rz 89] Vorgeschlagen ist in Art. 16 Abs. 1 E-DSG ein **Auskunftsrecht** an Daten verstorbener Personen, welches jede Person mit schutzwürdigem Interesse gegenüber dem Verantwortlichen geltend machen kann. Ein solches Interesse kann die Klärung eines familiären Konflikts, aber ebenso ein Forschungsinteresse sein. Weiter können es ohne Interessennachweis der Willensvollstrecker, in gerader Linie verwandte Personen, aktuelle Ehepartner und Personen, die mit der verstorbenen Person eine eingetragene oder mindestens eine faktische Lebensgemeinschaft führten, geltend machen. Es ist davon auszugehen, dass der Auskunftssuchende die Beweislast trägt, dass er die Anforderungen erfüllt. Liegt ein solches Auskunftsgesuch vor, muss der Verantwortliche prüfen, ob dies gegen Vorgaben des Verstorbenen verstösst, dieser sonst ein besonderes «Schutzbedürfnis» hat, welches der Auskunft entgegenstehen würde, oder es überwiegende Interessen des Verantwortlichen oder Dritter gegen die Auskunft gibt. Im Vorentwurf konnte sich ein Verantwortlicher noch nicht auf eigene überwiegende Interessen berufen.

[Rz 90] Solche überwiegenden eigenen Interessen und Drittinteressen wird ein Verantwortlicher auch dann anführen müssen, wenn er gar nicht zur Bekanntgabe berechtigt ist, weil die Daten einer Geheimhaltungspflicht unterliegen, die er gegenüber einer Drittperson schuldet. Das ist insofern unsauber, als dass in solchen Fällen die Auskunft in jedem Fall ausgeschlossen sein muss (wie im Falle des Auskunftsrechts gemäss Art. 24 Abs. 1 Bst. a E-DSG) und nicht bloss einer Interessenabwägung unterzogen werden darf. Im Vorentwurf hiess es freilich noch, dass ein Amts- oder Berufsgeheimnis gar nicht geltend gemacht werden kann. Hierzu wird neu nur geregelt, dass Auskunftersuchende die Entbindung von der Geheimhaltungsvorschrift verlangen können (Art. 16 Abs. 2 E-DSG). In Bereichen, in denen es wie beim Bankgeheimnis keine gesetzliche Entbindungsmöglichkeit gibt, wird somit nie eine Auskunft über die Daten verstorbener Personen erteilt werden können, soweit kein Verzicht bzw. keine Vollmachten und keine erbrechtlichen Instrumente bestehen. Auf diese Problematik geht die Botschaft nicht ein.

99 Art. 31 Abs. 1 des Schweizerischen Zivilgesetzbuches vom 10. Dezember 1907 (ZGB; SR 210).

[Rz 91] Wie im Vorentwurf ist weiterhin ein **Anspruch auf Löschung oder Vernichtung** von Daten Verstorbener vorgesehen, der allerdings nicht mehr von einzelnen Erben, sondern nur noch den Erben zusammen oder vom Willensvollstrecker geltend gemacht werden kann. Einstiger Anlass dieser Regelung war das Bedürfnis, einen Anspruch gegenüber den Betreibern sozialer Netzwerke zu schaffen, die Entfernung von Angaben über verstorbene Personen verlangen zu können. Ob die Regel ihr Ziel wirklich erfüllen wird, ist indes unklar, da beispielsweise eine entsprechende vertragliche Regelung zwischen betroffener Person und dem Verantwortlichen einer Löschung entgegenstehen würde. Gegenüber dem Vorentwurf wird dem Verantwortlichen neu auch die Berufung auf eigene Interessen oder sogar «Interessen des Verstorbenen» erlaubt, womit das Feld der Argumente sehr weit geöffnet ist. Letztlich werden die Gerichte entscheiden müssen, weil ein Verantwortlicher, der nicht Auskunft erteilen will, praktisch immer Gründe gegen eine Auskunft finden wird.

[Rz 92] Problematisch ist im Zusammenhang mit der Regel überdies, dass die Löschung *oder* Vernichtung verlangt werden kann. Da der Begriff der Vernichtung sehr weit geht, ja mithin die physische Zerstörung des Datenträgers erfordert, würde dies etwa bei einem Betrieb, welcher die Daten eines Kunden auf seinen IT-Systemen gespeichert hat, bedeuten, dass er diese Systeme und etwaige Backups zerstören müsste, um einem Anspruch auf Vernichtung nachzukommen. Einer solchen Vernichtung werden regelmässig überwiegende Interessen des Verantwortlichen entgegenstehen; es wird die Löschung genügen müssen.

14. Erweiterung der Informationspflicht: Schildbürgerstreich mit Swiss Finishes

[Rz 93] Eine der zentralen neuen Bestimmungen im neuen DSG für private Datenbearbeitung ist die Informationspflicht in Art. 17 f. E-DSG. Sie dehnt die heute bereits bestehende Informationspflicht bei der Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen[100] auf alle Datenbearbeitungen aus, wie dies bisher bereits für Bundesorgane galt. Sie bildet die Informationspflicht in der DSGVO nach[101], geht andererseits aber mit mehreren Swiss Finishes darüber hinaus.

[Rz 94] Die Informationspflicht ist so ausgestaltet, dass zum einen ein Katalog an **Mindestinformationen** aufgeführt ist, die der betroffenen Person mitzuteilen ist. Dies sind die Identität und Kontaktdaten des Verantwortlichen, der Bearbeitungszweck, die bearbeiteten Daten (falls diese nicht bei der Person direkt beschafft werden), etwaige Empfänger oder Kategorien von Empfängern (z.B. Behörden, Auftragsbearbeiter, Konzerngesellschaften), die Länder, in welche die Daten übermittelt werden und auf welcher Rechtsgrundlage (etwaige vertragliche Garantien oder in Anspruch genommene Ausnahmen) dies geschieht.[102] Zum anderen sind der Person auch alle weiteren Informationen zu liefern, die diese braucht, «damit sie ihre Rechte [nach DSG] geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist». Dies alles muss der Person auch dann mitgeteilt werden, wenn die Daten nicht bei ihr direkt, sondern aus einer anderen Quelle, zum Beispiel über eine andere Person (Ehepartner, Geschäftskollege etc.), der Datenbank

100 Art. 14 DSG.

101 Art. 13 f. DSGVO.

102 Art. 17 Abs. 2–4 E-DSG.

eines Dritten, von einer Behörde, einem Konzernunternehmen oder aus einer Publikation beschafft werden. In diesem Fall hat derjenige, der für die Beschaffung verantwortlich ist, maximal einen Monat Zeit, es sei denn, er gibt die Daten selbst schon früher weiter; dann muss auch früher informiert werden.[103]

[Rz 95] Keine ausdrückliche Aussage enthält Art. 17 E-DSG zur Frage, ob **nachinformiert** werden muss, wenn sich die kommunizierten Parameter einer Datenbearbeitung im Laufe der Zeit ändern, also beispielsweise ein neuer Zweck hinzukommt. Aufgrund der Logik der Bestimmung ist eine solche Nachinformation jedoch nicht erforderlich. Die Informationspflicht knüpft an die Beschaffung an; ist sie abgeschlossen, und ist informiert, findet sie keine Anwendung mehr. Werden laufend neue Daten beschafft, wird jedoch auch laufend informiert und die Information folglich angepasst werden müssen (z.B. durch eine nachgeführte Datenschutzerklärung auf einer Website). Nachträgliche Zweckänderungen und dergleichen sind im Rahmen der Bearbeitungsgrundsätze zu prüfen; sollen für einen Zweck A beschaffte Daten somit später für einen bei der Beschaffung noch nicht angegebenen Zweck B benutzt werden, muss nach Art. 5 Abs. 3 E-DSG geprüft werden, ob dies mit dem ursprünglichen Zweck A vereinbar ist. Falls nicht, ist aufgrund der sich daraus ergebenden Zweckentfremdung ein Rechtfertigungsgrund nach Art. 27 E-DSG erforderlich.

[Rz 96] Es gibt eine Reihe von Fällen, wo nach Art. 17 E-DSG keine Information erfolgen muss oder die Information sonst eingeschränkt werden kann. Diese Ausnahmen sind in Art. 18 E-DSG definiert. Es wird hierbei eine Unterscheidung zwischen **Ausnahmen** und **Einschränkungen** gemacht, wobei diese Unterscheidung von Relevanz ist: Die Person muss zwar anders als beim Auskunftsrecht (das ähnlich ausgestaltet ist) nicht darüber aufgeklärt werden, dass sie nicht oder nicht vollständig informiert wird. Handelt es sich jedoch bloss um eine «Einschränkung» der Informationspflicht und nicht eine Ausnahme und liegt kein hinreichender Grund vor, auf die Information ganz zu verzichten, muss sie dann, wenn der ursprüngliche Grund wegfällt, nachgeholt werden. In Frage kommen insbesondere Fälle, in denen Interessen von Dritten oder des Datenbearbeiters gegen eine Information eines Tages nicht mehr überwiegen, aber nach wie vor ein Informationsinteresse der betroffenen Person besteht. In diesem Falle kann die Information lediglich aufgeschoben werden. Das wiederum kann für den Verantwortlichen einen erheblichen Überwachungsaufwand mit sich bringen, da zur Sicherstellung der Nachinformation entsprechende Prozesse geschaffen werden müssen.

[Rz 97] Einige der Ausnahmen und Einschränkungen liegen auf der Hand. Hat die betroffene Person beispielsweise bereits die nötigen Informationen, braucht nicht nachgedoppelt zu werden (was im Übrigen auch dann gelten sollte, wenn kein besonderes Interesse an der Information besteht). Das wird in der Praxis wichtig sein, weil es erlaubt, dass ein «Erstbeschaffer» von Daten mit seiner Information gleich auch die Informationspflichten von nachfolgenden Empfängern der Daten erfüllen kann. Beschafft beispielsweise eine Versicherung Daten der Versicherungsnehmer, muss sie diese teilweise zur Rückversicherung ihrer Verträge an weitere Versicherungen weiterreichen, die mit dem Versicherungsnehmer keinen Kontakt haben. Hier macht es Sinn und genügt es, wenn die Erstversicherung über die gesamte Datenbearbeitung auch der Rückversicherer informiert. Dasselbe wird dort geschehen, wo ein Kunde eines Unternehmens dem Unternehmen auch Angaben über weitere Personen aus seinem Umfeld liefert (z.B. an wen eine

103 Art. 17 Abs. 5 E-DSG.

Vertragsleistung zu erbringen ist). In solchen Fällen wird das Unternehmen vernünftigerweise stillschweigend davon ausgehen können (und müssen), dass sein Kunde etwaige andere Personen darüber informiert hat (auch im Sinne von Art. 17 E-DSG), dass das Unternehmen auch seine Daten bearbeitet. Wäre dem nicht so, müsste dies in den AGB geregelt werden, da ansonsten das Unternehmen ständig einem Rechtsrisiko ausgesetzt wäre. Es ist darauf zu hoffen, dass auch die Aufsichtsbehörden damit pragmatisch umgehen werden. Auf die weiteren Ausnahmen sei hier nicht im Einzelnen eingegangen; die meisten betreffen spezielle Konstellationen (z.B. Medien, gesetzliche Geheimhaltungspflichten). Auf das überwiegende eigene Interesse kann ein privater Datenbearbeiter sich allerdings nur berufen, wenn er die Daten nicht an Dritte weitergibt, wozu freilich auch Aufsichtsbehörden oder Konzerngesellschaften zählen;[104] das macht schlicht keinen Sinn und wird in der Botschaft auch nicht begründet (vgl. dazu unten Rz. 99, «Swiss Finish Nr. 3»).

[Rz 98] So ist die Informationspflicht in der vorgeschlagenen Ausgestaltung in mehrerlei Hinsicht **problematisch**. Schon jetzt ist klar, dass sie so von niemandem vollständig eingehalten werden kann. Folgendes Beispiel illustriert dies: Zwei Personen unterhalten sich über ein Thema. Die eine Person bittet daraufhin die andere, ihr doch weiterführende Informationen zuzusenden, und erhält in der Folge eine E-Mail mit den gewünschten Angaben, darunter auch diverse Zeitungsartikel. Dies stellt wohl unbestrittenermassen eine Datenbeschaffung dar. Bei der E-Mail handelt es sich um Personendaten, da in ihr die E-Mail-Adresse des Absenders enthalten ist, womöglich eine Signatur und vielleicht noch weitere Angaben zum Absender oder zu weiteren Personen enthalten sind. Auch die mitgelieferten Zeitungsartikel sind Personendaten mindestens der Personen, die in der Autorenzeile genannt werden. Art. 17 E-DSG verlangt, dass der Empfänger der E-Mail dem Absender innert Monatsfrist, aber auch etwaigen weiteren darin genannten Personen, inklusive der Autoren der Zeitungsartikel, alle Angaben gemäss Art. 17 E-DSG liefert, einschliesslich der Liste der Staaten, in welchen die vom E-Mail-Empfänger möglicherweise benutzten IT-Provider die E-Mail bearbeitet haben. Der Empfänger der E-Mail muss den Absender und allen weiteren Personen in der Mail auch über den Grund informieren, warum er die Information haben möchte, selbst wenn es den Absender und die anderen Personen nicht interessiert; sagt er diesbezüglich nicht die Wahrheit, kann er mit bis zu CHF 250'000 gebüsst werden. Art. 18 E-DSG sieht zwar diverse Ausnahmen von der Informationspflicht vor, aber keine dieser Ausnahmen greift im vorliegenden Fall. Am besten lässt sich der Sachverhalt unter die Berufung auf überwiegende private Interessen subsumieren (Art. 18 Abs. 3 Bst. c E-DSG), aber auf diese kann sich ein Verantwortlicher nur stützen, wenn er die E-Mail nicht an Dritte weiterleitet. Ob die Weiterleitung problematisch oder völlig harmlos ist, soll jedoch gemäss Bundesrat keine Rolle spielen.

[Rz 99] Das Beispiel zeigt, dass sich der Bundesrat über die praktischen Folgen der Informationspflicht nicht wirklich nachgedacht oder aber sie ignoriert hat, was besonders bedenklich ist, weil ihre Verletzung strafbar ist. Das von ihm angedachte System der Ausnahmen ist zudem unnötig kompliziert und wird selbst Spezialisten herausfordern. Die vier wichtigsten Mängel von Art. 17 und 18 E-DSG sind:

- **Swiss Finish Nr. 1:** Die Pflicht in Art. 17 E-DSG, über alle Länder zu informieren, in die Daten bekanntgegeben werden, geht über die DSGVO hinaus, ebenso die Angaben zu den diver-

104 Art. 18 Abs. 3 Bst. c E-DSG.

sen Rechtfertigungsgründen. In der EU muss nur informiert werden, ob Daten ins EU/EWR-Ausland gehen, und über die dabei benutzten Garantien.[105] Die Regel ist daher anzupassen und maximal auf das zu beschränken, was auch die DSGVO verlangt. Es ist in der Praxis bei global immer stärker verteilten Datenbearbeitungen schlicht nicht möglich, die betroffenen Personen über aller Länder zu informieren, und es bringt auch keinen datenschutzrechtlichen Nutzen. Sollte das Land, in welchem Daten bearbeitet werden, ausnahmsweise von Bedeutung sein, wird dies im Rahmen des Grundsatzes der Verhältnismässigkeit und Treu und Glauben zu berücksichtigen sein, wie das heute schon der Fall ist. Sollte die Bestimmung unverändert bleiben, werden Unternehmen in ihre Informationen gemäss Art. 17 E-DSG kurzerhand eine Liste alle Länder aufnehmen, mit generischen Formulierungen arbeiten («in alle Länder, in denen wir über eine Tochtergesellschaft, Zweigniederlassung oder Büro verfügen») oder sagen, dass die Daten in jedes Land der Welt exportiert werden können, um auf Nummer sicher zu gehen. Der betroffenen Person wird das an zusätzlicher Transparenz gar nichts bringen. Die Vorstellung, dass Personendaten in der Wirtschaft nur in einzelne, bestimmte Länder exportiert werden, entspricht nicht mehr der Realität. Tätigt eine Bank beispielsweise für einen Kunden eine Geldüberweisung ins Ausland, so kann dies ohne Weiteres eine Bearbeitung seiner Daten in einem halben Dutzend Länder nach sich ziehen. Das interessiert weder den Kunden noch lässt es sich ohne einen grossen Bürokratieapparat ermitteln und dokumentieren noch kann er es ändern. Dasselbe Problem hat aber auch der Bäckermeister an der Ecke, der seine Office-Produkte künftig in der Cloud betreiben lässt und daher alle Kunden und Dritte, die in seinen E-Mails und Dokumenten genannt werden, laufend über die Länder informieren müsste, in denen die Microsofts, Googles und anderen Cloud-Anbieter dieser Welt seine Daten gerade speichern oder bearbeiten. Diese Information ist für den Datenschutz bei Lichte betrachtet weder relevant noch mit vertretbarem Aufwand zu beschaffen; entscheidend ist in solchen Fällen auch aus Sicht des Datenschutzes nur, dass die Daten sicher aufbewahrt sind – und dies ist regelmässig gewährleistet.

- **Swiss Finish Nr. 2:** Die Informationspflicht ist in Art. 17 E-DSG nicht abschliessend definiert,[106] im Gegensatz zur Regelung der EU.[107] Die Schweizer Regelung geht also über jene der EU hinaus und sollte entsprechend angepasst werden. Es ist beim vorgeschlagenen Wortlaut völlig unklar, welche weiteren Informationen geliefert werden müssen. Da die Bestimmung strafbewehrt ist, werden Unternehmen sie tendenziell übererfüllen. Mehr Transparenz scheint auf den ersten Blick nicht schlecht, wird sich aber als kontraproduktiv erweisen: Erstens fördert Art. 17 E-DSG ohnehin bereits eine Flut an «Kleingedrucktem» zum Datenschutz, das die Mehrheit der betroffenen Personen, wie die Erfahrung zeigt, schlicht nicht interessiert und eher als notwendiges Übel empfunden wird. Zweitens kostet es die Wirtschaft einigen Aufwand, der bezahlt werden muss. Drittens ist es ein konzeptioneller Fehler, Art. 17 E-DSG dafür zu nutzen, das Grundbedürfnis an Transparenz zu erfüllen; diese Aufgabe ist Sache des Bearbeitungsgrundsatzes der Transparenz und kann doch sachgerechter erfüllt werden (siehe dazu sogleich).

105 Art. 17 Abs. 4 E-DSG.

106 Art. 17 Abs. 2 E-DSG.

107 Art. 13 f. DSGVO; die revidierte Konvention des Europarats (K108) ist ebenfalls nicht abschliessend in Art. 7bis, erlaubt aber in der Umsetzung eine abschliessende Aufzählung der Pflichtangaben.

- **Swiss Finish Nr. 3:** Die Berufung auf überwiegende private Interessen darf gemäss Art. 18 Abs. 3 Bst. c E-DSG wie erläutert nicht davon abhängig sein, ob die Daten auch Dritten bekanntgegeben werden. Diese unsinnige Einschränkung ist eine Schweizer Eigenheit und lässt sich sachlich nicht begründen; sie verbietet dem Richter das Fällen von vernünftigen Entscheiden und gehört daher gestrichen. Es sei auf die Ausführungen zum selben Problem beim Auskunftsrecht verwiesen (siehe unten Rz. 111 ff.); im heutigen Recht war sie im Zusammenhang mit der Informationspflicht deshalb kaum ein Problem, weil sich erstens kaum jemand an die Informationspflicht hielt und sie zweitens einen nur sehr eingeschränkten Anwendungsbereich hatte. In der DSGVO ist vorgesehen, dass nationales Recht Interessenabwägungen vorsehen kann, und zwar ohne die vorgeschlagene Einschränkung.[108] Der Vorbehalt von Fällen der Datenweiterleitung an Dritte bedeutet, dass sich Unternehmen zum Beispiel – anders als in der EU – in manchen Fällen nicht mehr auf den Schutz der eigenen Geschäftsgeheimnisse mehr berufen können, selbst wenn deren Schutz objektiv wichtiger erscheint als das Informationsinteresse einer betroffenen Person. Ein weiteres Beispiel aus dem Alltag: Eine Firma sammelt Presseberichte über sich und verteilt diese an andere Firmen und Kunden. In den Presseberichten sind auch die Namen der verfassenden Journalisten und weitere Personen genannt. Nach Art. 17 E-DSG muss die Firma die Journalisten und alle in den Artikeln genannten Personen darüber informieren, dass sie Personendaten von ihnen gesammelt hat, nämlich die Zeitungsberichte, falls sie diese nicht mit geschwärzten Namen an die anderen Interessenten weiterleitet. Tut sie dies ohne Schwärzung, gibt sie Personendaten an Dritte weiter und kann wegen des Vorbehalts in Art. 18 Abs. 3 Bst. c E-DSG nicht mehr mit überwiegenden eigenen Interessen begründen, dass sie auf die Information der betroffenen Personen verzichtet. Das aber wäre die vernünftige Lösung. Die anderen Rechtfertigungsgründe für einen Verzicht auf die Information greifen nicht. Wird dem Entwurf des Bundesrates gefolgt, kann der zuständige Mitarbeiter somit wählen zwischen einem strafbaren Verhalten und einer völlig unsinnigen Information der betroffenen Personen – ein klassischer Schildbürgerstreich.
- **Konzeptioneller Mangel:** Es wird nicht festgehalten, dass die Informationspflicht dadurch erfüllt werden kann, dass ein Unternehmen seine Pflichtinformationen auf seiner Website oder auf andere, allgemein zugängliche Weise publiziert. Art. 17 E-DSG ist vom Wortlaut so ausgestaltet, dass mit betroffenen Person aktiv kommuniziert werden muss, was – wie das vorne genannte Beispiel (Rz. 98) illustriert – zu völlig unsinnigen Ergebnissen führt. Auch die Botschaft spricht sich leider für eine solche praxisfremde Auslegung aus. Zwar wird festgehalten, dass dort, wo Informationen bei einer Person direkt beschafft werden, es genügen kann, dass ihr die Informationen auf einer Website zur Verfügung gestellt werden. Doch für den Fall einer indirekten Beschaffung wird dies mit dem Argument verneint, die betroffene Person wisse diesfalls ja nicht, dass über sie Daten beschafft werde.[109] Das stimmt zwar auf den ersten Blick, verkennt aber auf den zweiten Blick, worum es bei dieser Regelung gehen sollte. Art. 17 E-DSG dient – entgegen der Botschaft[110] – nicht dazu sicherzustellen, *dass* Personen erfahren, ob Daten über sie bearbeitet werden, sondern soll ihnen lediglich zusätzliche Informationen liefern, falls sie daran interessiert sind. Hier liegt auch der konzeptionelle

108 Art. 23 Abs. 1 Bst. i E-DSG.

109 Botschaft (Fn. 2), S. 114.

110 Botschaft (Fn. 2), S. 114.

Mangel und Denkfehler des Entwurfs: Er vermengt die Informationspflicht mit dem Bearbeitungsgrundsatz der Transparenz und sorgt damit für unbefriedigende Ergebnisse. Beides dient zwar der Transparenz, befriedigt aber unterschiedliche Bedürfnisse. Der Transparenzgrundsatz ist es, der sicherstellen soll, dass betroffene Personen – wo erforderlich – erkennen können, *dass* Daten über sie bearbeitet werden und durch wen. Entsprechend variabel ist er ausgestaltet. Dem gegenüber sollte die Informationspflicht nach Art. 17 E-DSG wie die Pflicht zur Deklaration der Zusammensetzung von Lebensmitteln ausgestaltet sein: Was hinein gehört ist abschliessend definiert, und es genügt, sie kleingedruckt auf der Verpackung zu deklarieren. Wer sich dafür interessiert, muss sich darum bemühen. Es käme niemand auf die Idee, bei einer Einladung zum Essen allen Gästen nebst den Speisen auch noch eine Liste mit allen Zutaten und deren Inhaltsangaben zu liefern. Genau von diesem Konzept liess sich der Bundesrat leiten. Das erklärt auch, warum er auf den ausdrücklichen Bearbeitungsgrundsatz der Transparenz verzichtete und nur eine Minivariante – den Grundsatz der Erkennbarkeit des Zwecks – in den Bearbeitungsgrundsätzen in Art. 5 E-DSG vorsieht. In der DSGVO wurde dieser Fehler nicht gemacht.[111] Eine einfache Lösung des Problems bestünde in einem Zusatz in Art. 17 E-DSG, wonach die Informationspflicht durch eine allgemein zugängliche Deklaration erfüllt werden kann; der Grundsatz der Transparenz kann zur Not auch ohne textliche Änderung in Art. 5 E-DSG über den Grundsatz der Bearbeitung nach Treu und Glauben[112] hergeleitet werden. Dass selbst bei indirekten Datenbeschaffungen eine Information via Website und allfällige andere, öffentlich zugängliche Kanäle (z.B. Aushang in einem Ladenlokal) genügt, entspricht im Übrigen auch der heutigen Praxis des EDÖB.[113] Dies sollte im Gesetzgebungsprozess klargestellt werden.

15. Automatisierte Einzelentscheide: Zurückhaltende Schweizer Regelung

[Rz 100] Ebenfalls ins Kapitel der Informationspflichten fällt die Bestimmung über automatisierte Einzelentscheide in Art. 19 E-DSG. Sie hat jedoch eine eigenständige Bedeutung. Hintergrund der Regel ist ein Misstrauen gegenüber Entscheidungen, die ein Computer alleine trifft, dabei möglicherweise nicht alle relevanten Faktoren berücksichtigt und so zu ungerechten Ergebnissen kommt. Die Regel geht von der Vorstellung aus, durch Menschen getroffene Entscheide seien gerechter, weil auch Sonderfälle berücksichtigt werden könnten und es eine Möglichkeit geben muss, um auf falsche oder unvollständige Daten hinzuweisen. Das mag im Einzelfall zutreffen, doch in vielen Fällen ist dies eine Illusion; der Sachbearbeiter der Bank, der über die Genehmigung eines Kredits entscheidet, hat heute genauso wenig Spielraum von den vordefinierten Regeln abzuweichen wie ein Computer, der dasselbe tut, und spricht mit der Person möglicherweise auch gar nicht. Die revidierte Konvention des Europarats schreibt jedoch eine solche Regel vor, und so muss sie auch die Schweiz einführen. Erfreulicherweise hat der Bundesrat die in der

111 Vgl. Art. 5 Abs. 1 Bst. a DSGVO; die Informationspflicht in Art. 13 und 14 DSGVO ist abschliessend definiert.

112 Art. 5 Abs. 2 E-DSG.

113 Vgl. Empfehlung des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten betr. Itonex AG vom 6. November 2014 («Moneyhouse»), Rz. 80 ff. und S. 31, Pkt. i; dort wurde es als hinreichend erachtet, dass Moneyhouse auf ihrer Website darüber informiert, aus welchen Quellen sie welche Daten wozu beschafft, auch wenn die betroffenen Personen mit Moneyhouse – wie im Beispiel mit dem Online-Buchhändler in der Botschaft – keine Beziehung haben. In diesem Sinne auch schon die Empfehlung vom 15. November 2012 (https://www.edoeb.admin.ch/datenschutz/00626/00747/01022/index.html?lang=de).

DSGVO enthaltene Regelungsvariante[114] nicht einfach übernommen. Es ist weder ein Verbot vorgesehen, noch ein Anspruch der betroffenen Person, nicht einer automatisierten Einzelentscheidung zu unterliegen. Vielmehr sind sie voraussetzungslos erlaubt. Es wird lediglich bestimmt, dass eine betroffene Person grundsätzlich über eine solche automatisierte Einzelentscheidung informiert und ihr die Möglichkeit gegeben werden muss, sich mit einem Menschen über den Entscheid zu unterhalten. Dieser muss den vom Computer getroffenen Entscheid zwar umstossen können, denn sonst macht die Regel keinen Sinn. Tun muss er es jedoch nicht. Es ist dies mit anderen Worten ein **Anspruch auf «menschliches Gehör»,** so wie ein Rechtsunterworfener gegenüber einer Behörde Anspruch auf «rechtliches Gehör» hat, wenn über ihn entschieden werden soll.

[Rz 101] Während dieses menschliche Gehör unter der DSGVO fast immer gewährt werden muss, wenn es zu automatisierten Einzelentscheiden mit einer gewissen Wirkung kommt, differenziert der Bundesrat für die Schweiz: Hat die betroffene Person darin ausdrücklich eingewilligt, dass der Entscheid in einer Angelegenheit vom Computer definitiv beschlossen wird, dann kann auf das menschliche Gehör verzichtet werden.[115] Die Informationspflicht gemäss Art. 19 Abs. 1 E-DSG entfällt zwar regelungstechnisch gesehen, aber da dies nur der Fall ist, wenn eine ausdrückliche Einwilligung vorliegt, wird im Rahmen der Einwilligung trotzdem informiert werden müssen: Die betroffene Person muss ja wissen, worauf sie sich einlässt.[116] Tut sie dies, würde freilich auch eine nicht ausdrückliche Einwilligung genügen; dieses Erfordernis kann daher ohne Not gestrichen werden. Der zweite Fall ist derjenige, in welchem ein automatisierter Einzelentscheid im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht. In der EU muss in solchen Fällen immer informiert und immer menschliches Gehör angeboten werden. In der Schweiz ist dies hingegen nur der Fall, wenn dem Begehren der betroffenen Person nicht stattgegeben wird. Wer also auf der Website einer Kleinkreditgesellschaft einen Online-Kredit beantragt, der von einem Computer automatisch zu den beantragten Konditionen bewilligt wird, muss über diese Tatsache nur informiert und ihm die Möglichkeit geboten werden, mit einem Menschen zu sprechen, wenn ihm der Kredit verweigert oder aber er ihn nur zu schlechteren Konditionen erhält, als ursprünglich angegeben wurde[117] oder – soweit die Möglichkeit bestand – von ihm verlangt wurde. Ist das der Fall, wird ihm mit dem Entscheid mitgeteilt werden müssen, dass ein Computer diesen gefällt habe, er aber mit einer entscheidbefugten Person sprechen kann, die sich den Fall nochmals anhöre. Anders entscheiden muss diese Person nicht; es muss ihr lediglich möglich sein, anders zu entscheiden oder jemanden anders entscheiden zu lassen, sollten Anhaltspunkte dafür bestehen, dass der Computer den Fall «falsch» aufgrund der (beschränkten) Datenlage beurteilt hat – das ist der Kernzweck der Bestimmung.

[Rz 102] Bei der spannenden Frage, wann überhaupt ein **automatisierter Einzelentscheid** im Sinne von Art. 19 Abs. 1 DSG vorliegt, folgt die Schweiz im Wortlaut weitgehend der EU:

---

114 Art. 22 DSGVO.

115 Art. 19 Abs. 3 Bst. b E-DSG.

116 Art. 5 Abs. 6 E-DSG.

117 Die Konditionen, zu denen ein Unternehmen seine Leistungen auf einer Website anbietet, gelten in der Regel als Einladung zur Offerte, auf welche hin der Kunde eine Bestellung vornimmt. Diese gilt in der Regel als Offerte zum Vertragsschluss und stellte zugleich das «Begehren» im Sinne von Art. 19 E-DSG dar. Diese Begehren werden allerdings auf Online-Plattformen in der Regel vom Anbieter automatisiert vorformuliert sein, was für sich aber noch nicht unter Art. 19 E-DSG fällt.

- Erforderlich ist zunächst ein **Einzelentscheid** über eine betroffene Person. Wenn also beispielsweise eine Fluggesellschaft von einem Computer bestimmen lässt, wie hoch die Preise für bestimmte Sitzplätze an eine bestimmte Destination zu einem bestimmten Zeitpunkt am besten sind, so ist das kein Einzelentscheid. Es wird keine Entscheidung über eine einzelne Person gefällt. Wird hingegen der Computer so programmiert, dass er auf einen bestimmten Kunden individualisierte Preise berechnet, so liegt ein Einzelentscheid vor.
- Der Einzelentscheid muss aufgrund der **Bearbeitung von Personendaten** der betroffenen Person erfolgen. So kann der Spieler am Glücksspielautomat dann nicht verlangen, mit einem Menschen darüber zu diskutieren, warum er nicht gewonnen hat, wenn der Entscheid darüber einzig nach dem Zufallsprinzip und damit gerade nicht aufgrund einer Bearbeitung der Daten des Spielers getroffen wurde, selbst wenn dieser als solcher persönlich identifiziert worden wäre. Kein Einzelentscheid liegt auch dort vor, wo zwar Daten der betroffenen Person bearbeitet werden, diese für den Computer bzw. den Verantwortlichen nicht identifizierbar ist, d.h. keine Personendaten vorliegen. Dann findet auch das DSG keine Anwendung. Wer also den Computer Einzelentscheide über anonyme Besucher einer Website treffen lässt, fällt nicht unter Art. 19 E-DSG.
- Der Einzelentscheid muss vollständig **von einer Maschine getroffen** werden. Bereitet der Computer Entscheide vor, und segnet ein Mensch sie inhaltlich ab, bevor sie der betroffenen Person kommuniziert werden, liegt kein automatisierter Einzelentscheid vor. Heikel wird die Abgrenzung bei der Frage, wie weit der Mensch hinsichtlich der Entscheidkriterien noch mitwirken darf, damit ein Fall von Art. 19 E-DSG vorliegt. So kann argumentiert werden, ein (vollständig) automatisierter Einzelentscheid liege nur dann vor, wenn der Computer auch die Entscheidlogik selbst erarbeitet – im Sinne von künstlicher Intelligenz oder auf der Basis von Zufallselementen. Wenn hingegen ein Mensch vorgibt, dass allen Website-Benutzern, die aufgrund ihrer Online-Kenndaten als Nutzer von Apple-Produkten erkannt werden, ein höherer Preis angezeigt werden soll, weil sie statisch gesehen mehr zu zahlen bereit sind, so könnte argumentiert werden, der Mensch habe den Entscheid vorweggenommen. So ist es jedoch nicht: Die Entscheidregeln dürfen durchaus von Menschenhand sein, wesentlich ist, dass die Subsumption des konkreten Sachverhalts im Einzelfall – hier: die Beurteilung der Daten der betroffenen Person (ist sie Nutzer von Apple-Produkten?) – maschinell erfolgt und diese bis zur Fällung des definitiven Entscheids nicht mehr von einem Menschen überprüft wird. Bereitet umgekehrt ein Computer den Entscheid eines Menschen lediglich vor, so wird ebenfalls kein automatisierter Einzelentscheid vorliegen, soweit ihn vor seiner Wirksamkeit[118] ein Mensch inhaltlich überprüft und ihn direkt oder indirekt umstossen kann.[119] Eine Stichprobenprüfung wird aufgrund des Normzwecks nicht genügen; es geht nicht darum, ob der Computer im Allgemeinen richtig entscheidet, sondern dies gerade auch in Ausnahmefällen tut. Diese kann nach der Logik des Gesetzgebers nur der Mensch zuverlässig erkennen. Allerdings führt auch dies wieder zu Fragen, ob z.B. kein automatisierter Einzelentscheid vorliegt, wenn der Computer Sonderfälle selbständig erkennt und sie einem Menschen aussteuert, was im Hinblick auf den Normzweck genügen muss, damit insgesamt keine automatisierten Einzelentscheide vorliegen. Wo genau die Grenze durchläuft, bleibt offen. Der

118 Dies grenzt den automatisierten Einzelentscheid vom menschlichen Gehör ab: Zu letzterem kommt es nur, wenn die betroffene Behörde dies verlangt. Tut sie dies nicht, bleibt der Entscheid wirksam.

119 Vgl. Botschaft (Fn. 2), S. 120.

Bundesrat will hier ggf. mit der Verordnung Klarheit schaffen. In jedem Fall als automatisierter Entscheid gilt kraft ausdrücklicher Regelung jede Form von Profiling. Falls das Profiling nach Begriffsverständnis des Bundesrates (vgl. oben Rz. 22 ff.) anders als in der EU jedoch immer eine allein von einer Maschine vorgenommene Bewertung umfassen muss, ergeben sich hier keine weiteren Abgrenzungsschwierigkeiten.

- Die maschinelle Subsumption bzw. Entscheidung muss gemäss Bundesrat ferner **eine gewisse Komplexität** aufweisen, d.h. es muss um eine inhaltliche Beurteilung bzw. Bewertung und nicht eine reine «wenn-dann-Entscheidung» gehen.[120] Ist lediglich letzteres der Fall, so kann argumentiert werden, dass gar kein Entscheid im engeren Sinn vorliegt, weil in der Sache kein Spielraum besteht, zu welchem Ergebnis der Vorgang richtigerweise kommen kann. In diesem Sinne würde ein elektronisches Türschloss keinen Entscheid über den Zutritt zum Gebäude fällen: Wird der richtige Code eingegeben, hat es zu öffnen, sonst eben nicht. Der Bundesrat bringt als weiteres Beispiel den Entscheid des Geldautomaten, dem Kunden Geld auszuzahlen, nämlich nach der Prüfung, ob sich auf dem Konto genügend Geld befindet.[121] Sollte der Vorgang jedoch auch eine Kreditprüfung beinhalten, weil das Konto überzogen ist und daher der Bankomat entscheiden muss, ob der Person nicht doch Kredit gewährt wird, liegt nach herrschendem Verständnis wieder ein automatisierter Einzelentscheid vor.[122] Der Unterschied besteht nicht darin, dass der Computer im letzteren Fall Spielraum hat und im ersteren nicht, denn technisch gesehen hat er in beiden Fällen keinen, weil sein Entscheid in beiden Fällen durch eine Serie von «wenn-dann»-Regeln vorgegeben ist, er also in starrer Weise programmiert ist. Der Unterschied besteht darin, dass im ersten Fall die *Bank* keinen Spielraum hat bzw. haben will (Genug Geld auf dem Konto?), im zweiten aber schon (Kunde kreditwürdig?). Hat die Bank einen Spielraum, kann sie für ihren Entscheid unterschiedliche Faktoren berücksichtigen und dies auf unterschiedliche Weise. Aus diesem Grund soll der zweite Fall von Art. 19 E-DSG erfasst sein: Gerade weil die Bank sich bei der Programmierung ihres Computers auf starre Regeln begrenzen muss und den Computer nicht so programmieren kann, dass er wie ein Mensch *alle* möglicherweise relevanten Faktoren in holistischer Weise berücksichtigen kann, soll die Überprüfung des Entscheids durch einen Menschen weiterhin vorbehalten sein. Besteht für den Entscheid hingegen kein Spielraum, kommt Art. 19 E-DSG selbst dann nicht zum Tragen, wenn der Computer falsch entscheidet bzw. falsch programmiert ist (also das Schloss trotz gültigem Code nicht öffnet). Die Komplexität des Entscheids kann jedoch entgegen dem Bundesrat nicht massgebend sein. Sonst wäre auch ein Spamfilter von Art. 19 E-DSG erfasst: Es ist ein hochkomplexer Prozess, E-Mails daraufhin zu beurteilen, ob es sich um unverlangte Werbung handelt oder nicht. Dieser Prozess steht in der Komplexität derjenigen einer Bonitätsbeurteilung in nichts nach. Der Unterschied besteht auch hier darin, dass im Falle des Spamfilters kein Spielraum besteht,[123] im Falle der Bonität schon.
- Der Entscheid muss für die betroffene Person mit einer **Rechtsfolge** verbunden sein oder aber sie **erheblich beeinträchtigen**. Hier weicht die Schweiz etwas von der EU-Regelung ab.

120 Botschaft (Fn. 2), S. 120.

121 Botschaft (Fn. 2), S. 120.

122 Es sei denn, diese Fällen würden automatisch ausgesteuert und von einem Menschen geprüft und freigegeben, oder aber ein Mensch hat die Kreditlimite bereits vorgängig auf einen höheren Betrag als Null festgelegt.

123 Worin sich die einzelnen Spamfilter unterscheiden ist der Anteil und die Auswahl der *false positives* und *false negatives*. Es ist aber jeweils klar, dass die betreffenden Treffer «false» sind.

Unter der DSGVO kann vertreten werden, dass die rechtliche Wirkung ein gewisses Gewicht aufweisen muss, weil in der Folge von einer «in ähnlicher Weise» erfolgenden erheblichen Beeinträchtigung die Rede ist. In der Schweiz ist das nicht der Fall: Jede Rechtsfolge genügt, sei es ein Vertragsabschluss, die Ausübung eines vertraglichen Rechts und theoretisch auch eine Erfüllungshandlung unter dem Vertrag (also z.B. die Lieferung der Ware); die Rechtsfolge ist der Untergang des Anspruchs auf Erfüllung. Was eine «erhebliche Beeinträchtigung» im Sinne von Art. 19 Abs. 1 E-DSG ist, definiert auch die Botschaft nicht abschliessend. Immerhin hält sie fest, dass eine blosse Belästigung nicht genügen soll.[124] Sie erwähnt als mögliches Beispiel eine nicht zugeteilte medizinische Leistung und unter gewissen Umständen auch der verweigerte Vertrag (in welchem Fall der automatisierte Entscheid also dazu führt, dass es gerade keine Rechtsfolge gibt).

- Allenfalls kann sich noch die Frage stellen, ob vom Geltungsbereich von Art. 19 E-DSG im Sinne einer teleologischen Auslegung auch jene automatisierten Einzelentscheide auszunehmen sind, in denen der Computer zu einer **Gesamtbetrachtung** aller Umstände analog derjenigen eines Menschen tatsächlich bereits in der Lage ist und eine Wiedererwägung des Entscheids durch einen Menschen daher nichts bringt. Ein Beispiel mag die (leider nicht mehr verfügbare) Anwendung «faces.ethz.ch» sein[125].

[Rz 103] Die Botschaft hält fest, dass es möglich ist, dass eine Person vor oder nach einem Entscheid bezüglich ihres Standpunkts angehört werden kann.[126] Das macht so keinen Sinn, denn wenn die Anhörung durch einen Menschen mit Entscheidbefugnis vor der Entscheidfällung erfolgt, liegt kein automatisierter Entscheid mehr vor. Wird das menschliche Gehör erst nach dem getroffenen Entscheid ein Thema, so stellt sich die Frage, wie lange das Unternehmen in der Lage sein muss, auf seinen Entscheid zurückzukommen. Bis dahin muss dieser zwar wirksam, aber in einer Schwebe bleiben, soll die Regelung sinnvoll bleiben. Der Entwurf sagt nichts dazu für den Privatbereich.[127] Eine Frist von einigen Tagen nach «Eröffnung» des Entscheids wird in aller Regel genügen. Eine Person kann auf eine Anhörung auch verzichten, etwa indem sie die sofortige Umsetzung eines durch den Entscheid abgeschlossenen Vertrags verlangt bzw. das Unternehmen kann dies verlangen, wenn von ihm verlangt wird, entsprechend des automatisierten Entscheids zu handeln. Dies bedarf keiner besonderen Form.

16. Auskunftsrecht: Missbrauch wird mit neuen Ansprüchen zunehmen

[Rz 104] Das Auskunftsrecht ist einerseits ein wichtiges Instrument einer betroffenen Person zur Durchsetzung des Datenschutzes, andererseits aber eines der am häufigsten missbrauchten Instrumente. Im Vordergrund steht vor allem die heute vorherrschende Nutzung des Auskunftsrechts zu datenschutzfremden Zwecken, wie z.B. die Beschaffung von Beweismitteln im Zivilprozess. Unverantwortliche Entscheide auch des Bundesgerichts haben diese **Missbräuche** (anders

124 Botschaft (Fn. 2), S. 121.

125 Bei dieser Computeranwendung der ETH Zürich beurteilte ein Computer durch künstliche Intelligenz die Attraktivität einer Person (vgl. z.B. https://motherboard.vice.com/de/article/pgkn4g/diese-kuenstliche-intelligenz-errechnet-wie-attraktiv-ihr-seid-634 und https://arxiv.org/abs/1510.07867).

126 Botschaft (Fn. 2), S. 122.

127 Im Bereich der Bundesorgane wird als Beispiel die Rechtsmittelfrist nach automatisiertem Erlass einer Verfügung erwähnt (Botschaft [Fn. 2], S. 122).

als im europäischen Ausland) leider geschützt.[128] Daher sind sie primär in der Schweiz ein Thema. In Rechtsstreitigkeiten gehört es heute zum Standard, dass versucht wird, von der Gegenseite mittels Auskunftsrecht die Edition relevanter Dokumente zu verlangen, auch wenn das Verfahren nichts mit dem Datenschutz zu tun hat. Die Botschaft anerkennt die Existenz dieser Missbräuche zwar mittlerweile[129], doch sieht der Entwurf unverständlicherweise keine Massnahmen zur Eindämmung vor.[130]

[Rz 105] War es bisher nur möglich, das Auskunftsrecht mit Bezug auf **Datensammlungen** geltend zu machen, fällt diese Einschränkung mit dem neuen Art. 23 E-DSG inzwischen weg. Von grosser praktischer Bedeutung ist sie ohnehin nicht: In den meisten Fällen wurde in der Praxis die Frage, ob überhaupt eine Datensammlung besteht, ignoriert.

[Rz 106] Inhaltlich soll das Auskunftsrecht deutlich erweitert werden. Auch hier wurde ein Swiss Finish mit potenziell erheblichen Folgen geschaffen: Neu müssen auf Verlangen nebst den bearbeiteten Daten nicht mehr nur abschliessend definierte Pflichtinformationen geliefert werden, sondern jede Information, die für eine betroffene Person erforderlich ist, um ihre Rechte nach DSG geltend zu machen.[131] In der EU sind die zu liefernden Angaben im Gegensatz dazu abschliessend definiert.[132] Bleibt dies im Entwurf, kann jede Person, über welche Daten bearbeitet werden, auf dem Weg des Auskunftsrechts neu zum Beispiel auch Einsicht in Verträge (z.B. mit Auftragsbearbeitern), Weisungen und beliebige andere Interna eines Unternehmens erhalten. Es wird sich immer argumentieren lassen, dass dies zur Beurteilung der Rechtmässigkeit und damit etwaiger persönlichkeitsrechtlicher Ansprüche erforderlich ist; in der bisher reichhaltigen Gerichtspraxis wurden solche Argumente, selbst wenn sie offenkundig vorgeschoben waren, regelmässig anerkannt. Gleichzeitig wird den Unternehmen in manchen Fällen verwehrt werden, sich auf ihre Geschäftsgeheimnisse oder andere eigene Interessen berufen zu können, selbst wenn diese überwiegen, weil die betroffenen Personendaten mit Dritten geteilt werden (siehe nachfolgende Ausführung zur Geltendmachung überwiegender eigener Interessen, Rz. 111 ff.).[133] Ob sich der Bundesrat der Konsequenzen seines Übereifers in der Ausgestaltung des Auskunftsrechts bewusst war, darf bezweifelt werden.

[Rz 107] Auch der Katalog der zu liefernden **Mindestangaben** wurde leicht erweitert: Neu muss auch über die Aufbewahrungsdauer informiert werden, über die Länder, in welche exportiert wird und auf welcher Grundlage, sowie über automatisierte Einzelentscheide und die Logik, auf

---

128 Vgl. etwa Urteil des Bundesgerichts 4A_506/2014 vom 3. Juli 2015 ; dazu http://swissblawg.ch/2015/07/4a5062014-4a5242014-rechtsmissbrauchlic.html m.w.H.

129 Botschaft (Fn. 2), S. 131.

130 Lösungsansätze gibt es diverse. Sie reichen von der Beschränkung auf Fälle, in denen nachgewiesen werden kann, dass ein Auskunftsersuchen primär aus Datenschutzgründen erfolgt und nicht zum Zwecke der Beweisausforschung (Frage des Institutsmissbrauchs) über Kostenschranken bis hin zu einer Klarstellung, dass die Hürden zur Annahme eines Missbrauchs deutlich zu senken sind. Einer der erfolgversprechendsten Ansätze erscheint jedoch, das Auskunftsrecht inhaltlich nicht einzuschränken, es aber formal so auszugestalten, dass es für die Beweisausforschung nicht mehr interessant ist. Dies könnte zum Beispiel dadurch geschehen, dass der Auskunftspflichtige wählen kann, dass er die Daten nicht mehr in Kopie dem Auskunftsersuchenden übergibt, sondern stattdessen einer dritten Stelle, die entweder die Verletzung des Datenschutzes stellvertretend prüft (denn nur dazu dient das Auskunftsrecht), wie es der EDÖB heute in gewissen Fällen tut, oder bei welcher der Auskunftsersuchende die Daten einsehen kann, aber sie eben nicht mehr zweckentfremdet verwenden kann, z.B. als Beweismittel in einem nicht datenschutzrechtlich motivierten Forderungsprozess, was heute den Regelfall darstellt.

131 Art. 23 Abs. 2 E-DSG.

132 Art. 15 Abs. 1 DSGVO.

133 Art. 24 Abs. 2 Bst. a E-DSG. Typische Fälle werden die Weitergabe von Daten an Aufsichtsbehörden oder Konzerngesellschaften sein.

welcher diese basieren.[134] Die Auskunft zur Logik erfordert keine detaillierten Angaben, jedoch wird sie Angaben zur Menge und Art der verwendeten Personendaten sowie zu deren Gewichtung enthalten müssen.[135] Es dürfte daher in der Schweiz nicht genügen, wenn darauf hingewiesen wird, dass z.B. die Kreditwürdigkeit einer Person aufgrund einer Wertung bisheriger Zahlungserfahrungen und Einträge im Betreibungsregister errechnet wird. Es müsste auch der Erhebungszeitraum (z.B. der letzten fünf Jahre) und gewisse Angaben zur Gewichtung angegeben werden (z.B. in welchen Fällen, in denen von einer fehlenden Kreditwürdigkeit ausgegangen wird). Diese Angaben müssen notabene nur im Falle eines Auskunftsersuchens offengelegt werden, nicht bereits im Rahmen der Informationspflicht nach Art. 17 E-DSG und wohl auch nicht, wenn eine Einwilligung in solche automatisierten Einzelentscheide eingeholt wird. Allerdings genügt es nicht, dass das Unternehmen seine Prozesse so steuert, dass Fälle negativer Entscheide vor deren Kundgabe einem Menschen zur Bestätigung vorgelegt werden. Dann liegen in diesen Fällen zwar keine automatisierten Einzelentscheide mehr vor, in den anderen Fällen bestehen sie aber weiterhin, auch wenn die Informations- und Anhörungspflicht nach Art. 19 Abs. 3 E-DSG entfällt. Angaben zu automatisierten Einzelentscheiden werden zudem nur dann erforderlich sein, wenn welche bestehen, die inhaltlich vom Auskunftsersuchen erfasst sind. Verlangt der Kunde einer Bank Einblick in sein Kundendossier, so muss ihm keine Übersicht aller automatisierten Einzelentscheide im Unternehmen offengelegt werden, und vernünftigerweise auch nicht all jener, die ihn möglicherweise im Laufe der Kundenbeziehung betreffen könnten. Nach dem Sinn und Zweck des Auskunftsrechts ergibt sich, dass über jene automatisierte Einzelentscheide Auskunft zu erteilen ist, für welche die angeforderten Daten herangezogen werden und die ohne weitere Information oder Rückfrage der betroffenen Person erfolgt sind oder normalerweise erfolgen bzw. erfolgen können. Denn das Auskunftsrecht muss nur aber immerhin jene Angaben liefern, mit denen eine Person jene Datenbearbeitungen überprüfen bzw. sich dagegen wehren kann, bei denen sie das sonst nicht könnte. Daher können von einer Auskunftserteilung jene Einzelentscheide ausgeklammert werden, über die sie ohnehin vorgängig zum gegebenen Zeitpunkt informiert würde und dann die Gelegenheit hätte, ihre Rechte wahrzunehmen. Wenn also eine Bank automatisierte Kreditentscheide trifft, braucht sie den nach seinem Kundendossier fragenden Kunden darüber nicht zu informieren, wenn der Kunde dann, wenn er einen Kreditantrag stellt, noch darüber informiert würde und Gelegenheit erhält, seine Rechte geltend zu machen und beispielsweise zu widersprechen oder nicht einzuwilligen, wenn nach seiner Einwilligung gefragt wird. Hingegen sind vom Auskunftsrecht wohl alle automatisierten Einzelentscheide erfasst, die unter Art. 19 Abs. 1 E-DSG fallen, also auch solche, auf die eine der beiden Ausnahmen gemäss Abs. 3 zutrifft. Wenn also ein Kunde wissen will, welche Daten und welche Logik dem auf ihn für eine automatisierte Kreditvergabe angewandten Einzelentscheid zugrunde lag, kann er dies auch dann verlangen, wenn seinem Begehren stattgegeben wurde.

[Rz 108] Wie heute müssen Auskünfte grundsätzlich **kostenlos** erteilt werden,[136] während der Bundesrat Ausnahmen vorsehen kann.[137] Ob er das Versprechen, der Tatsache Rechnung zu tragen, dass gewisse Auskunftsersuchen mit hohem Aufwand verbunden sind,[138] wirklich einhält,

134 Art. 23 Abs. 2 E-DSG.

135 Botschaft (Fn. 2), S. 132.

136 Art. 23 Abs. 1 E-DSG.

137 Art. 23 Abs. 6 E-DSG.

138 Botschaft (Fn. 2), S. 133.

wird sich zeigen. Bisher konnte selbst in Fällen, in denen ein einziges Auskunftsersuchen ein Unternehmen viele Tausende Franken kostet, nur gerade CHF 300 verlangt werden. Die EU sieht hier eine flexible Lösung vor, die unter anderem bei exzessiven Ersuchen greift.[139] Es wäre wünschenswert, wenn auch in der Schweiz den Unternehmen das Recht gegeben würde, eine angemessene Entschädigung zu verlangen, diese aber nicht betragsgemäss zu begrenzen. Im Streitfall wird ohnehin der Richter entscheiden müssen. Der Autor dieser Zeilen kennt Fälle, in denen die Beantwortung von Auskunftsersuchen weit über CHF 10'000 kosteten. Im Zusammenhang mit Auskunftsersuchen unter der DSGVO zeichnet sich ab, dass manche Unternehmen ein zweistufiges Vorgehen einführen werden: In einer ersten Stufe wird ein unspezifisches Auskunftsersuchen mit der Lieferung von gewissen Mindestinformationen beantwortet mit dem Hinweis, dass weitergehende Informationen nur geliefert werden, wenn genau spezifiziert wird, worum es dem Auskunftsuchenden konkret geht. Tut der Auskunftsersuchende nichts, kann das Auskunftsersuchen als exzessiv mit entsprechenden Kostenfolgen belegt werden. Bei Banken werden Auskunftsersuchen heute zum Beispiel regelmässig dazu benutzt, verlorengegangene Kontoauszüge «nachzubestellen».

[Rz 109] Anders als heute wird nicht mehr verlangt, dass die Auskunft **schriftlich** zu erfolgen hat. Neu ist nur noch erforderlich, dass die betroffene Person die Informationen gemäss Art. 23 Abs. 2 E-DSG erhält; auf welche Weise, ist nicht vorgeschrieben. Dies kann in elektronischer Form sein, was bisher nur in gegenseitigem Einvernehmen möglich war. Die neue Regelung kann grundsätzlich sogar so ausgelegt werden, dass der betroffenen Person lediglich Einblick in ihre Daten gewährt werden muss, geht es doch nur darum, dass die Person weiss, was für Daten wie bearbeitet werden. Das ist mit einer Einsichtnahme erfüllt. Es ist allerdings zu erwarten, dass die Gerichte in Anbetracht ihrer bisher einseitigen Entscheidpraxis zugunsten von Auskunftsuchenden dies nicht als hinreichend ansehen werden und argumentieren werden, die Person wird etwaige Beweise für ein datenschutzwidriges Verhalten in den Händen haben und mit ihrem Rechtsvertreter teilen können müssen. Damit lässt sich das Auskunftsrecht weiterhin zur Beweismittelbeschaffung missbrauchen.

[Rz 110] Dies gilt umso mehr, als dass seitens der **Einschränkungsgründe** des Auskunftsrechts sich im Wesentlichen nichts ändern soll. Zwar wird neu als Einschränkungsgrund eingeführt, dass das Auskunftsgesuch offensichtlich unbegründet oder querulatorisch ist.[140] In solchen Fällen konnte die Auskunft allerdings schon bisher ohne Weiteres als gegen den Grundsatz von Treu und Glauben verstossend verweigert werden. Gewonnen ist damit insbesondere zur Bekämpfung der heute vorherrschenden Missbräuche zur Beweismittelbeschaffung nichts, da sich Datenschutzgründe immer vorschieben lassen und die Auskunftsersuchen somit normalerweise nie «offensichtlich» unbegründet sind.

[Rz 111] Wesentlich wichtiger wäre es, eine uneingeschränkte Berufung auf **überwiegende private Interessen** zu ermöglichen. Diese soll nach Art. 24 Abs. 2 Bst. a E-DSG weiterhin nur möglich sein, wenn die Personendaten nicht Dritten bekanntgegeben werden. Mit «Dritten» sind zwar nicht auch Auftragsbearbeiter gemeint, sondern nur andere Verantwortliche. Bekanntgaben an solche sind in der Praxis allerdings häufig. Zu typischen Fällen zählen der Datenaustausch innerhalb eines Konzerns, da die verschiedenen juristischen Einheiten untereinander als Dritte gelten.

139 Art. 12 Abs. 5 Bst. a DSGVO.

140 Art. 24 Abs. 1 Bst. c DSGVO.

Ein anderes häufiges Beispiel ist die Auskunftserteilung an Behörden, die ebenfalls als Dritte gelten. Muss also ein Unternehmen zum Beispiel seiner Aufsichtsbehörde aus irgendeinem Grund vertrauliche geschäftliche Unterlagen offenlegen, kann sich das Unternehmen nicht mehr auf das Geschäftsgeheimnis berufen. Selbst wenn klar ist, dass das Interesse an der Geheimhaltung der Unterlagen überwiegt, ist auch ein Richter gezwungen, die ungeschwärzte Herausgabe der Unterlagen anzuordnen, sobald sie eine externe Person, die darin vorkommt (z.B. ein ehemaliger Mitarbeiter), verlangt.

[Rz 112] Zu welch stossenden Ergebnissen die Regelung des Bundesrats führt, zeigt auch ein anderes Beispiel: Lässt ein Unternehmen von einer Anwaltskanzlei ein Memorandum über die Erfolgschancen eines von einem ehemaligen Mitarbeiter oder Kunden angedrohten Prozesses erstellen, wird sie dieses im Prozess nie offenlegen müssen. Die Korrespondenz zwischen Anwalt und Klient ist geschützt. Anders beim Auskunftsrecht: Am Schutz der Anwaltskorrespondenz besteht zwar klar ein überwiegendes eigenes Interesse. Teilt das Unternehmen das Memorandum aber mit seiner Muttergesellschaft, weil diese wissen will, welchem Risiko die Tochtergesellschaft ausgesetzt ist, liegt in aller Regel eine Bekanntgabe an Dritte vor. Die Berufung auf den Schutz der Anwaltskorrespondenz ist nach Art. 24 Abs. 2 Bst. a E-DSG nicht mehr möglich, mit entsprechenden weitreichenden Folgen.

[Rz 113] In der EU sind Auskunftspflichtige wesentlich besser vor Missbräuchen geschützt:

- *Erstens* können in der EU gemäss Gerichtspraxis unter dem Titel des Auskunftsrechts keine Dokumente herausverlangt werden, sondern nur Personendaten als solche. Das wäre an sich auch in der Schweiz korrekterweise der Fall, aber die Gerichte bis hin zum Bundesgericht setzten sich bisher über diese Einschränkung konsequenterweise hinweg und behandelten das Auskunftsrecht so, als wäre es ein Anspruch auf Urkundenedition. Dies könnte in Zukunft sogar noch schlimmer werden, da Art. 23 E-DSG nicht mehr davon spricht, dass «Daten» geliefert werden müssen, sondern «Informationen», was so verstanden werden kann, dass es auch Dokumente umfasst, auch wenn dies dem Sinn und Zweck des DSG widersprechen würde. Dem könnte mit einer redaktionellen Anpassung, wodurch nur die Personendaten «als solche» verlangt werden können, entgegengewirkt werden.
- *Zweitens* ist in der EU klar, dass das Auskunftsrecht der Durchsetzung des Datenschutzes dienen soll, und nur diesem. Wer den Datenschutz zur Urkundenedition für einen bevorstehenden Prozess zweckentfremdet, stellt ein «offensichtlich unbegründetes» Auskunftsgesuch, auch wenn behauptet wird, dass damit auch Datenschutzgründe verfolgt werden.[141] Nun soll zwar künftig auch die Schweiz eine solche Regelung erhalten.[142] In der Schweiz ist die Ausgangslage jedoch eine andere: Auskunftsgesuche gelten hierzulande solange als nicht unbegründet, als dass sie auch Datenschutzgründen dienen, selbst wenn diese von untergeordneter Natur sind.[143]
- *Drittens* besteht in der EU ein Schutz von Geschäftsgeheimnissen, der Auskunftsansprüchen vorgeht. Er wird in der Richtlinie 2016/943 des Europäischen Parlaments und des Rates über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung neu

141 Art. 12 Abs. 5 DSGVO.

142 Art. 24 Abs. 1 Bst. c E-DSG.

143 BGE 138 II 425, E. 5.5 f.

einheitlich geregelt, die von den Mitgliedsstaaten bis Mitte 2018 in nationales Recht umzusetzen ist. Im DSG kann ein Auskunftspflichtiger eigene Geschäftsgeheimnisse nur im Rahmen überwiegender eigener Interessen geltend machen, was ihm aber verwehrt ist, wenn er sie mit anderen Eingeweihten (z.B. Konzerngesellschaften, Geschäftspartner) geteilt hat, was freilich sehr oft vorkommt. In Art. 23 Abs. 1 Bst. i DSGVO wird den Mitgliedsstaaten erlaubt, die Berücksichtigung weiterer überwiegender privater Interessen vorzusehen.

[Rz 114] Die vom Bundesrat vorgeschlagene Lösung führt somit zum zweiten Swiss Finish des Auskunftsrechts. Der Ausschluss der **überwiegenden eigenen Interessen** im Falle einer Bekanntgabe von Personendaten an Dritte gehört gestrichen. Sachlich war und ist er ohnehin durch nichts gerechtfertigt. Denn wenn es in einem konkreten Fall tatsächlich so ist, dass die Interessen des Auskunftspflichtigen jene des Auskunftsersuchenden *überwiegen*, dann ist es so und sollte berücksichtigt werden. Art. 27 Abs. 1 E-DSG kennt ebenfalls keinen Vorbehalt zugunsten von Personendaten, die Dritten bekanntgegeben werden; es besteht schlicht kein sachlicher Zusammenhang. Die Botschaft sagt ebenfalls nicht, warum dieser Vorbehalt im Gesetz verbleiben soll. Seine Streichung würde wenigstens etwas Handhabe gegen die Missbräuche des Auskunftsrechts bieten. Auch bei einer Streichung bleibt es letztlich dem Richter überlassen, die Interessen abzuwägen. Für sachgerechte Entscheide bleibt somit genügend Raum.

17. Sanktionen mit Systemwechsel: Strafbar bleibt der Einzelne

[Rz 115] Das Sanktionssystem des Datenschutzrechts hat schon in der DSGVO die grösste Aufmerksamkeit auf sich gezogen. Beim Vorentwurf war es nicht anders. Beim Entwurf war die Spannung gross: Wird ein Systemwechsel zu Administrativsanktionen wie in der EU vorgeschlagen? Es blieb jedoch beim Ansatz des Vorentwurfs: Die Durchsetzung des DSG erfolgt wie bisher auf drei Ebenen: Privatrecht, Strafrecht und Aufsichtsrecht.

[Rz 116] Über **privatrechtliche Klagen** können betroffene Personen ihre Ansprüche mit Hilfe des Zivilrichters durchsetzen. Gerichtskosten sollen hierfür künftig – anlog der Regelung für arbeitsrechtliche Streitigkeiten bis CHF 30'000 – keine mehr entstehen, ausser bei mut- oder böswilliger Prozessführung.[144] Der Bundesrat erhofft sich davon offenbar nicht nur einen leichteren Zugang zu ihrem Recht für betroffene Personen, sondern auch eine differenziertere Gerichtspraxis durch mehr Fälle und damit mehr Rechtssicherheit.[145] Parteientschädigungen fallen allerdings weiterhin an; sie werden regelmässig das grössere Kostenrisiko für eine klagende Partei sein.

[Rz 117] Materiell ändert sich an den zivilrechtlichen Ansprüchen nicht viel. Art. 28 E-DSG, der diese aufführt, aber im Wesentlichen auf Art. 28 ZGB verweist, wird redaktionell etwas geändert. Die einzige etwas aussergewöhnliche Bestimmung findet sich in Art. 28 Abs. 1 E-DSG mit Bezug auf das Berichtigungsrecht. Die Bestimmung konkretisiert die Ausnahmen, in denen keine Berichtigung verlangt werden kann. Das sind einzig deren zwei: Ein Gesetz verbietet die Änderung der Daten oder die Personendaten werden zu öffentlichen Archivzwecken bearbeitet. Auf beide werden sich private Datenbearbeiter kaum je berufen können. Überwiegende Eigen- oder Drittinteressen können *a priori* keine geltend gemacht werden. Wie weit die Gerichte hier gehen werden,

144 Art. 114 Bst. f ZPO.

145 Botschaft (Fn. 2), S. 191.

muss sich noch zeigen. Nach dem Wortlaut der Bestimmung kann selbst zur Korrektur von archivierten, nicht mehr aktiv benutzten Daten und Daten auf Sicherheitskopien verpflichtet werden, auch wenn dies mit einem massiven Aufwand verbunden ist. Das erscheint nicht sachgerecht; die DSGVO erlaubt mehr Einschränkungen. Allenfalls wird ein Richter in einem solchem Fall zum Ergebnis kommen, dass es der betroffenen Person am erforderlichen Rechtsschutzinteresse fehlt oder über den Begriff der «Richtigkeit» korrigierend eingreifen.

[Rz 118] Die **strafrechtliche Durchsetzung** wird gegenüber der heutigen Regelung stark ausgebaut, doch geht sie sehr viel weniger weit als noch im Vorentwurf. Im Wesentlichen baut die strafrechtliche Sanktionierung des Datenschutzes auf drei Pfeiler:

- **Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 54 E-DSG):** Diese Regelung stellt das unter Strafe, was im DSG schon bisher im Rahmen von Art. 34 DSG unter Strafe gestellt worden war, allerdings mit einem massiv erhöhten Bussenrahmen von bis zu CHF 250'000. Es ist die Verletzung der Informationspflicht (Art. 17, Art. 19 E-DSG) und Verletzung des Auskunftsrechts (Art. 23 E-DSG), wobei in letzterem Falle nach wie vor nur die falsche oder unvollständige Auskunft sanktioniert wird, nicht die offene Verweigerung der Auskunft. Insofern bringt die Norm nichts Neues; sie kam in der Vergangenheit kaum je zur Anwendung. Neu ist jedoch, dass insbesondere die Informationspflichten, auf die sie verweist, massiv ausgebaut wurden, so dass der Bestimmung nunmehr eine deutlich grössere Rolle zukommt und für Datenbearbeiter ein höheres Risiko besteht, erfasst zu werden. Da die Informationspflicht aufgrund ihrer Ausgestaltung in vielen Fällen nicht oder nicht vernünftig erfüllt werden kann, ist die pauschale Strafbarkeit ihrer Verletzung rechtspolitisch höchst problematisch. Wird Art. 17 f. E-DSG und die Strafbestimmung so umgesetzt wie geplant, wird sich jeder, der in der Schweiz Daten bearbeitet, früher oder später strafbar machen. Daran ändern auch die allgemeinen Bagatellregeln des Strafrechts nichts. Immerhin ist die Verletzung der Informations- und Auskunftspflichten nur auf Antrag strafbar; antragsberechtigt sind nur betroffene Personen als geschützte Personen. Der EDÖB hat zwar ein Anzeigerecht[146], aber kein Strafantragsrecht, wie es hier erforderlich wäre. Die Bestimmung sanktioniert ferner denjenigen, der dem EDÖB falsche Auskünfte erteilt oder sich weigert, an einer Untersuchung mitzuwirken. Ergänzt wird diese Strafdrohung durch Art. 57 E-DSG, welche die Missachtung einer Verfügung des EDÖB unter Strafe stellt. Zu denken ist zum Beispiel an eine Anordnung des EDÖB, eine konkrete Datenbearbeitung einzustellen oder nach seinen Vorgaben anzupassen.[147] Sie weicht insofern von Art. 292 StGB ab, als dass hier eine mit CHF 250'000 sehr viel höhere Busse (statt CHF 10'000[148]) vorgesehen ist; die europarechtlichen Vorgaben verlangen abschreckende Sanktionen. Die Busse bei Nichtbeachtung muss allerdings in der betreffenden Verfügung angedroht worden sein.
- **Verletzung der Sorgfaltspflichten (Art. 55 E-DSG):** Diese Bestimmung ist neu und erfasst drei Tatbestände aus dem materiellen Datenschutzrecht. Der Strafkatalog wurde gegenüber dem Vorentwurf massiv reduziert. Die Strafbarkeit der Verletzung diverser Meldepflichten wurde ganz gestrichen; so geht der Entwurf sogar weniger weit als das heutige Recht[149]. So bleibt das Unterlassen einer *Data Breach Notification* und einer Konsultation des EDÖB bei

146 Art. 59 Abs. 2 E-DSG.

147 Gestützt auf Art. 45 E-DSG.

148 Art. 106 StGB.

149 Welches eine Busse vorsieht: Art. 34 Abs. 2 Bst. a DSG.

Datenschutz-Folgenabschätzungen straflos (und das Unterlassen der Datenschutz-Folgenabschätzung und Führen eines Inventars selbst auch). Was an Tatbeständen geblieben ist, erscheint freilich reichlich zufällig ausgewählt: Bestraft werden kann mit bis zu CHF 250'000, wer (i) Personendaten entgegen den Bestimmungen über den Datenexport (Art. 13 f. E-DSG) ins Ausland bekanntgibt, (ii) eine Auftragsbearbeitung (Art. 8 E-DSG) nicht sauber regelt oder dabei Geheimhaltungspflichten verletzt oder sich nicht vergewissert, dass eine hinreichende Datensicherheit besteht, und (iii) wer die Vorgaben des Bundesrats zur Datensicherheit (Art. 7 Abs. 3 E-DSG) nicht befolgt. Letzterer Fall lässt sich immerhin damit erklären, dass der Bundesrat wohl versuchte, dem strafrechtlichen Bestimmtheitsgebot nachzukommen. Werden die Bestimmungen des Bundesrats zur Datensicherheit den Grad der Konkretisierung haben, der sich heute beispielsweise in Art. 9 VDSG findet, wäre damit aber nichts gewonnen. Sie sind nämlich letztlich genauso nichtssagend und Allgemeinplätze wie die Grundnorm von Art. 7 E-DSG. Die Strafbestimmung wird vor allem dazu führen, dass die verantwortlichen Personen mehr Aufwand für die Dokumentation ihrer Sicherheitsmassnahmen betreiben werden, um zu zeigen, dass sie die Anforderungen des Bundesrats erfüllen. Zu mehr Datensicherheit wird dies jedoch kaum beitragen, es sei denn, er würde konkrete Risikosituationen regeln. Gesetzgeberische Regelungen zur Datensicherheit beschränken sich daher normalerweise darauf, gewisse Schutzziele zu definieren und es dem Rechtsunterworfenen überlassen, das Risiko zu beurteilen und angemessen zu adressieren. Diese Strafnorm dürfte somit wenig materielle Wirkung haben, sondern primär die Bürokratie fördern. Dasselbe gilt auch für die Strafbarkeit im Zusammenhang mit der Auftragsbearbeitung. Warum der Bundesrat ausgerechnet in diesem Bereich ansetzt für seine Strafnormen, bleibt im Dunkeln. Auftragsbearbeitungen sind im praktischen Datenschutzalltag normalerweise kein Problem bzw. von ihnen geht normalerweise kein wirkliches Risiko für die betroffenen Personen aus. Auch hier wird die Strafnorm primär Bürokratie in Form von zusätzlicher Dokumentation zur Folge haben. Die Strafbarkeit der widerrechtlichen Bekanntgabe von Personendaten ins Ausland hingegen erscheint sinnvoll: In diesem Bereich wurde das DSG in der Vergangenheit regelmässig verletzt, weil Verletzungen keine oder nur selten Rechtsfolgen hatten, ausser ein (theoretisches) Strafbarkeitsrisiko bei unterlassener Meldung an den EDÖB nach Art. 6 Abs. 3 DSG, die nun in vielen Fällen gar nicht mehr nötig ist. Unternehmen werden im internationalen Datenaustausch sehr viel genauer auf ihre Praxis achten müssen, was zum Beispiel auch den konzerninternen Datenaustausch betrifft, der heute noch mancherorts nicht rechtskonform organisiert ist. Das betrifft dann sowohl grenzüberschreitende Bekanntgaben im Konzern wie auch konzerninterne Auftragsbearbeitungen (beides kann mit *Intra-Group Data Transfer Agreements* in der Regel rasch und einfach gelöst werden). Auch erfordert eine Strafbarkeit einen Strafantrag. Der EDÖB kann somit keine Strafuntersuchung in Gang setzen, sollte er eine Rechtswidrigkeit feststellen oder vermuten.

- **Verletzung der beruflichen Schweigepflicht (Art. 56 E-DSG):** Diese Strafnorm führt durch die Hintertür eine Strafbarkeit grundlegender Datenschutz- bzw. Vertraulichkeitsverstösse ein. Es gab sie in reduziertem Umfang schon bisher (Art. 35 DSG), doch spielte sie in der Praxis kaum eine Rolle, vermutlich weil sie erstens relativ unbekannt ist und zweitens auf besonders schützenswerte Daten und Persönlichkeitsprofile beschränkt war. Letzteres fällt nun weg. Art. 56 E-DSG schützt alle geheimen Personendaten anderer, die eine Person aufgrund ihres Berufs braucht und erfahren hat. Eine vertragliche Geheimhaltungspflicht, wie sie Art. 162 StGB erfordert, braucht es also nicht. Auch müssen die Personendaten kein Geschäftsgeheimnis darstellen. Es genügt gemäss dem allgemeinen Geheimnisbegriff, dass (i) die Tatsa-

che, von welchen die Personendaten handeln, nicht allgemein bekannt oder zugänglich sind, (ii) die betroffene Person ein schützenswertes Interesse hat und will, dass dies so bleibt.[150] Richtigerweise wird auch gefordert, dass dieser Geheimhaltungswille zum Ausdruck kommt. Dennoch ist der Anwendungsbereich der Regel enorm weit: Jeder kann von einer solchen Geheimhaltungspflicht betroffen sein, ob Autoverkäufer, Ladenangestellte in einer Bäckerei oder die Person am Ticketschalter im Kino: Sie alle müssen künftig mit Strafverfolgung rechnen, wenn sie ausplaudern, was ihnen ein Kunde an nicht öffentlichen Informationen im beruflichen Zusammenhang anvertraut hat, solange es nicht gerade irrelevanter, unproblematischer Smalltalk ist. Diese Regelung ist nicht unbedingt falsch, hat aber eine enorme Tragweite, die wohl nicht bedacht wurde; die meisten Personen, die diesem neuen, generellen Berufsgeheimnis unterworfenen sein werden, werden sich dessen nicht bewusst sein. Als Tathandlung erfasst sein wird jede Weitergabe an unbefugte Empfänger, d.h. eine Person, die vom Geheimnis, gemessen am berechtigten Geheimhaltungsinteresse und -willen, keine Kenntnis haben soll und nicht schon hat. Allerdings wird die bloss zweckwidrige Weitergabe an einen an sich befugten Empfänger nicht erfasst sein. Nicht erfasst ist selbstverständlich auch die Weitergabe anonymisierter Daten oder pseudonymisierter Personendaten, da sie für den Empfänger und Dritte keine Personendaten mehr darstellen, solange diese nicht über einen Re-Identifikationscode verfügen. Anders als beim klassischen Berufsgeheimnis (Art. 321 StGB) gibt es im Rahmen von Art. 56 E-DSG keine Möglichkeit der Entbindung durch eine Aufsichtsbehörde. Die Strafdrohung ist mit CHF 250'000 allerdings deutlich geringer.

[Rz 119] Neu eingeführt wird ferner eine Bestimmung zum Identitätsdiebstahl. Diese findet sich allerdings nicht im DSG, sondern im neuen Art. 179^{decies} StGB. Erfasst werden sollen allerdings nur Fälle von einer gewissen Schwere.[151]

[Rz 120] Weiterhin straflos bleibt die ungerechtfertigte **Verletzung der Bearbeitungsgrundsätze**, was in Anbetracht des Bestimmtheitsgebots des Strafrechts auch richtig ist. Sollten dereinst Verwaltungsstrafen eingeführt werden, so wird sich der Bundesrat wohl überlegen müssen, ob er den Katalog der Tatbestände ausweitet; in der EU sind auch Verletzungen der Bearbeitungsgrundsätze massiv sanktioniert. Insgesamt erscheinen die Strafbestimmungen des Entwurfs somit vergleichsweise milde. Dazu trägt auch bei, dass alle Verstösse anders noch als im Vorentwurf nur bei **vorsätzlicher Begehung** strafbar sind; allerdings genügt bereits ein Eventualvorsatz, d.h. es genügt, dass die Verwirklichung des Tatbestands zwar nicht beabsichtigt ist, die Person sie aber für möglich hält und in Kauf nimmt.[152] Wer also den Export von Personendaten anordnet und weiss, dass hierbei gewisse Regelungen zu beachten sind, ihm aber egal ist, ob sie eingehalten sind oder nicht und er sich daher nicht darum kümmert, kann grundsätzlich bestraft werden. Wer hingegen entsprechenden Rechtsrat einholt und sich um eine Einhaltung der Regelungen bemüht, kann auch dann nicht bestraft werden, wenn sich herausstellen sollte, dass der Rechtsrat falsch war. Kommt der Rechtsrat (wie so oft) zum Ergebnis, dass die Situation nicht eindeutig ist, die Rechtmässigkeit des Exports sich aber mit guten Gründen vertreten lässt, und kann die Person zeigen, dass sie an diese Rechtmässigkeit glaubte, wird sie straffrei bleiben, selbst wenn sie falsch lag und möglicherweise fahrlässig handelte.

150 Botschaft (Fn. 2), S. 168.

151 Botschaft (Fn. 2), S. 195.

152 Art. 12 Abs. 2 StGB.

[Rz 121] Der Entwurf des Bundesrates ist insofern deutlich schärfer als die DSGVO, als dass die Sanktionierung sich **gegen natürliche Personen**, nicht gegen das Unternehmen als solches richtet, wie dies in der EU der Fall ist. Da die Sanktionen strafrechtlicher Natur sind, muss damit gerechnet werden, dass sie weder versichert werden können, noch vom Unternehmen für den Gebüssten bezahlt werden dürfen, da dies als eine strafbare Verfolgungsbegünstigung qualifiziert werden könnte.[153] Die strafrechtliche Natur führt auch dazu, dass weitere Massnahmen wie die Einziehung von Vermögenswerten möglich ist, und zwar auch bei Dritten (sprich: beim Unternehmen selbst).[154] Der Entwurf sieht aber keine finanziellen Verwaltungssanktionen vor, wie sie etwa das Kartell- oder Fernmeldegesetz (KG; SR 251, FMG; SR 784.10) vorsieht, die das Unternehmen selbst treffen würden. Der Grund dafür ist nachvollziehbar: Die Schweiz ist nach den europäischen Vorgaben verpflichtet, abschreckende Sanktionen einzuführen. Wenn jedoch Sanktionen mit Strafcharakter ausgesprochen werden sollen, sind auch entsprechende strafprozessuale Garantien in den betreffenden Verfahren vorzusehen. Solche hat die Schweiz in ihrem Verwaltungsverfahrensrecht noch nicht, und deren Schaffung ist angesichts des Zeitdrucks, mit welchem die Schweiz das DSG revidieren muss, nicht vernünftig möglich.[155] Auch stellen sich weitere, grundsätzliche Fragen im Zusammenhang mit der Sanktionierung von Unternehmen, die noch nicht gelöst sind.[156] Der Entscheid des Bundesrats, auf Verwaltungssanktionen einstweilen zu verzichten, ist daher nachvollziehbar, auch wenn es in der Sache im Falle von Datenschutzverletzungen mehr Sinn macht, die verantwortlichen Unternehmen als die für sie handelnden Einzelpersonen zu sanktionieren.

[Rz 122] Der Bundesrat wird in der Botschaft nicht müde zu betonen, dass die Strafsanktionen primär die **Leitungspersonen** von Unternehmen treffen werden.[157] Dies verkennt jedoch die Realitäten. Es trifft zwar in der Tat zu, dass im Schweizer Recht die Verletzung von straf- und verwaltungsrechtlichen Pflichten durch Unternehmen den für sie handelnden Organen zugerechnet wird.[158] Dies sieht auch der Entwurf so vor.[159] Sie ist jedoch nicht auf diese beschränkt, jedenfalls solange die Pflichtverletzung auch durch natürliche Personen begangen werden kann. Die Anstiftung und Gehilfenschaft zur Verletzung der Art. 54–56 E-DSG wird zwar nicht erfasst, weil es sich «nur» um Übertretungen handelt.[160] Doch bei genauerer Betrachtung öffnet sich das Feld. So betreffen die Strafbestimmungen von Art. 55 und 56 E-DSG datenschutzrechtliche Pflichten, die nicht nur den Verantwortlichen treffen (welcher in der Regel das Unternehmen ist), sondern jede an der Datenbearbeitung mitwirkende Person. Doch auch dort, wo die strafbewehrte Pflicht nur dem Verantwortlichen auferlegt ist, wie etwa bei der Informations- oder Auskunftspflicht, ist es ohne Weiteres möglich und auch üblich, dass die Sicherstellung deren Einhaltung an untere Chargen delegiert ist. Diese werden, wenn sie mit entsprechenden Befugnissen ausgestattet

153 Art. 305 StGB; allerdings ist darauf hinzuweisen, dass diese Frage im Falle der Bezahlung einer Geldbusse durch einen Dritten in der Lehre umstritten ist (gegen das Vorliegen einer Begünstigung: Vera Delnon/Bernhard Rüdy, Basler Kommentar, Strafgesetzbuch II, 3. Auflage, Art. 305 StGB, N 20, m.w.H.).

154 Art. 70 StGB.

155 Botschaft (Fn. 2), S. 165.

156 Ebd.

157 Botschaft (Fn. 2), S. 165.

158 Art. 29 StGB, Art. 6 des Bundesgesetzes über das Verwaltungsstrafrecht vom 22. März 1974 (VStrR; SR 313.0).

159 Art. 58 Abs. 1 E-DSG.

160 Art. 333 StGB i.V.m. Art. 105 StGB.

sind, zu Leitungspersonen.[161] Zu denken ist etwa an den betrieblichen Datenschutzbeauftragten, der sich selbständig um die Beantwortung von Auskunftsersuchen kümmert. Zwar sieht Art. 58 Abs. 2 E-DSG vor, dass in geringfügigeren Fällen (Busse bis CHF 50'000) darauf verzichtet werden kann, die strafrechtlich verantwortlichen Einzelpersonen zu büssen und stattdessen auf das Unternehmen zurückzugreifen. Diese Ausnahme ist jedoch nicht zwingend. Zudem setzt sie voraus, dass Untersuchungsmassnahmen zur Ermittlung der verantwortlichen Person erforderlich sind, die unverhältnismässig wären. In vielen Fällen werden sich die verantwortlichen Personen jedoch rasch feststellen lassen bzw. bereits feststehen.

[Rz 123] Zu beachten ist in diesem Zusammenhang, dass die **Strafuntersuchung** nicht vom EDÖB geführt wird, sondern von den Kantonen. Das ist insofern spannend, als diese über keinerlei Erfahrung in diesem Bereich verfügen. Es ist daher zu erwarten, dass diese sich in Fällen, in welchen der EDÖB bereits tätig wurde und Ermittlungen geführt hat, sich weitgehend auf ihn abstützen werden. Das wird dadurch noch weiter begünstigt, dass er in der Rolle eines Privatklägers an entsprechenden Verfahren mitwirken kann.[162] Letzteres wird er zwar aufgrund seiner knappen Ressourcen wohl zu vermeiden versuchen. Allerdings ist die Regelung aus demselben Grund problematisch, aus dem der Bundesrat keine Verwaltungssanktionen einführt, nämlich das Fehlen der nötigen strafprozessualen Verfahrensgarantien im Verwaltungsverfahren. Somit ist es ohne Weiteres denkbar oder sogar wahrscheinlich, dass die Strafbehörden eine Angelegenheit nicht eigenständig und unabhängig beurteilen werden, wenn der EDÖB diese bereits untersucht und beurteilt hat. Sie werden seine Schlussfolgerungen im autonomen Nachvollzug als ihre eigenen übernehmen, strafprozessuale Garantien hin oder her.

[Rz 124] Der dritte und wohl wichtigste Pfeiler in der Durchsetzung des Datenschutzes stellen die neu geschaffenen **verwaltungsrechtlichen Kompetenzen des EDÖB** dar. Er konnte schon bisher mögliche Datenschutzverletzungen untersuchen, jedenfalls wenn sie Exporte oder eine gewisse Zahl von Personen betrafen. Auch konnte er gegen Verstösse vergleichsweise wirksam vorgehen. Zwar durfte er lediglich Empfehlungen aussprechen, hatte jedoch bei deren Nichtbefolgung ein entsprechendes Klagerecht.[163] Dies genügt den europarechtlichen Vorgaben allerdings nicht mehr. Der EDÖB wird neu dem Verwaltungsverfahren unterstellt (Art. 46 E-DSG), erhält die Befugnis, eine entsprechende verwaltungsrechtliche Untersuchung von Datenschutzverstössen durchzuführen (Art. 43 f. E-DSG) und Anordnungen zu treffen, um diese zu verhindern oder aus der Welt zu schaffen (Art. 45 E-DSG), einschliesslich vorsorglicher Massnahmen (Art. 44 Abs. 2 E-DSG). Ergänzt wird dies um entsprechende Bestimmungen der nationalen und internationalen Amtshilfe (Art. 48 ff. E-DSG).

[Rz 125] Anders als heute, wo der EDÖB im Wesentlichen als «Rosinenpicker» agieren kann, ist er künftig verpflichtet, Meldungen über mögliche Datenschutzverstösse nachzugehen. Die Verletzung des DSG wird quasi zum verwaltungsrechtlichen **Offizialdelikt**.[164] Er kann zwar von der Eröffnung einer Untersuchung absehen, wenn die Verletzung des Datenschutzes von geringfügiger Bedeutung ist,[165] doch erfordert der Entscheid darüber mindestens eine gewisse Vorbefassung mit der Sache. Erfährt er also zum Beispiel im Rahmen der Beratung von Missständen in

161 Art. 29 Abs. 1 Bst. c und d StGB.

162 Art. 59 Abs. 2 E-DSG.

163 Art. 29 DSG.

164 Art. 43 Abs. 1 E-DSG.

165 Art. 43 Abs. 2 E-DSG.

einem Unternehmen, oder liest er davon in der Zeitung, so wird er tätig werden müssen. Es wird sich zeigen, wie ernst er diese Vorgabe nimmt, denn sie hat das Potenzial, seinen Betrieb massiv zu überlasten. Personell, das ist schon heute klar, wird der EDÖB nicht hinreichend dotiert sein. Wird zusätzlich berücksichtigt, dass die Formalisierung seines Verfahrens als eigentliches Verwaltungsverfahren schon für sich einen gewissen Zusatzaufwand mit sich bringt, ist es somit ohne Weiteres möglich, dass der EDÖB selbst bei zehn zusätzlichen Stellen (die als Bedarf ermittelt wurden) im Ergebnis unter dem revidierten Recht weniger für den Datenschutz tun kann als heute. Es würde dem Datenschutz mit anderen Worten nach der hier vertretenen Ansicht wesentlich mehr dienen, die heutigen Kompetenzen zu belassen und dem EDÖB stattdessen sehr viel mehr Ressourcen zur Verfügung zu stellen. Leider hat die Schweiz diese Option nicht. Über die ihm zugeteilten personellen Ressourcen entscheidet offenbar die Bundesverwaltung und nicht das Parlament, und es stellt sich die Frage, wie gross ihr Interesse an einer Stärkung jener Behörde ist, deren wesentliche Aufgabe auch die Überwachung der Bundesverwaltung ist.

[Rz 126] Selbstverständlich müssen von einer Untersuchung betroffene Personen in der im **Verwaltungsverfahren** üblichen Weise mitwirken;[166] auch die Beschlagnahme von Unterlagen vor Ort ist möglich, allerdings wird der EDÖB zunächst um Mitwirkung ersuchen müssen.[167] Hierbei ist zu beachten, dass der EDÖB zwar unter dem Amtsgeheimnis steht,[168] die von ihm beschafften Unterlagen nach Abschluss eines Verfahrens aber grundsätzlich über das Öffentlichkeitsgesetz (BGÖ; SR 152.3) auch von Dritten einsehbar sind, wenngleich unter dem (in der Praxis nicht weitreichenden) Vorbehalt von Geschäftsgeheimnissen. Doch auch schon während der Untersuchung bleibt eine Untersuchung nicht geheim: Der EDÖB ist verpflichtet, jedenfalls den Anzeigeerstattern über die von ihm unternommenen Schritte und das Ergebnis seiner Untersuchung zu informieren,[169] auch wenn nur die Person, gegen die sich die Untersuchung richtet, Verfahrenspartei ist (nicht also etwaige von einer Datenbearbeitung betroffene Personen) und daher gegen Verfügungen des EDÖB nur ihr Rechtsmittel zur Verfügung stehen.[170] Das Informationsrecht des Anzeigeerstatters ist insofern systemwidrig und sollte gestrichen werden; es ist auch in der Sache nicht erforderlich, sondern lädt im Gegensatz zu Missbräuchen ein.

[Rz 127] Bussen kann der EDÖB keine ausfällen, aber seine **Interventionsmöglichkeiten** sind umfassend und daher für sich schon abschreckend: Er kann verfügen, dass eine Bearbeitung von Personendaten ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird oder Personendaten ganz oder teilweise gelöscht werden, wenn Datenschutzvorschriften verletzt sind.[171] Dies kann ein Unternehmen, das auf die Bearbeitung von Personendaten angewiesen ist, wesentlich härter treffen als eine Bussgeldzahlung. Immerhin kann der EDÖB auch blosse Verwarnungen aussprechen, wenn das betreffende Unternehmen schon während der Untersuchung die für den Datenschutz erforderlichen Massnahmen trifft;[172] es ist damit zu rechnen, dass der EDÖB schon aus Gründen der Effizienz darauf hinwirken wird, dass Unternehmen dies tun und er daher nicht den Aufwand hat, entsprechende Anordnungen zu treffen.

166 Art. 43 Abs. 3 E-DSG.

167 Art. 44 Abs. 1 E-DSG.

168 Art. 22 des Bundespersonalgesetzes vom 24. März 2000 (BPG; SR 172.220.1).

169 Art. 43 Abs. 4 E-DSG.

170 Art. 46 Abs. 2 E-DSG.

171 Art. 45 Abs. 1 E-DSG.

172 Art. 45 Abs. 4 E-DSG.

[Rz 128] Der EDÖB kann auch die Durchführung flankierender Massnahmen anordnen, wie etwa eine Datenschutz-Folgenabschätzung, die Vornahme von Meldungen von Verletzungen der Datensicherheit (d.h. die Einführung eines entsprechenden Prozesses) oder den Abschluss eines Datenexportvertrags.[173] Trotz entsprechender Kritik in der Vernehmlassung belassen wurde seine Kompetenz, die Bekanntgabe von Personendaten ins Ausland zu untersagen, selbst wenn sie die Exportbestimmungen von Art. 13 f. E-DSG nicht verletzt, sondern sie «nur» gegen eine andere Bestimmung des Schweizer Rechts verstösst.[174] Eine eigenständige Bedeutung dürfte diese Regel allerdings selten haben, da jede solche Bekanntgabe immer auch eine Verletzung von Art. 5 Abs. 1 E-DSG bedeutet (Grundsatz der Rechtsmässigkeit der Datenbearbeitung). Zu denken ist an Fälle von Geheimhaltungsvorschriften (z.B. Bankgeheimnis, Art. 273 StGB) und an Art. 271 StGB.

[Rz 129] Selbstverständlich sind Verfügungen des EDÖB aufgrund von Datenschutzverletzungen kostenpflichtig. **Gebühren** kann der EDÖB allerdings auch in diversen anderen Fällen verlangen, so namentlich bei den diversen Melde-, Genehmigungs- und Konsultationspflichten und bei der Beratung von Privaten.[175] Es wird am Bundesrat liegen, die Details vorzugeben. Dass die Beratung einer Person, die den Datenschutz einhalten will oder ihn bei sich verletzt sieht, kostenpflichtig sein soll, für Klagen gegen eben eine solche Datenschutzverletzung jedoch keine Gerichtsgebühren erhoben werden dürfen, steht in einem gewissen Widerspruch zueinander. Ohnehin könnten die neuen Gebühren, die der EDÖB verlangen muss, noch für einigen Gesprächsstoff sorgen. So gehen die Vorstellungen in der Bundesverwaltung, wie viel der EDÖB für seine Risikoeinschätzungen von ihm vorgelegten Projekten verlangen kann, in teils astronomische Höhen.

18. Übergangsbestimmungen: Zwei Jahre Zeit

[Rz 130] Der Vorentwurf hatte noch keine Übergangsbestimmungen, die eine solche Bezeichnung verdienten. Das hat sich mit dem Entwurf geändert. Generell gilt nun eine Übergangsfrist von zwei Jahren, die allerdings differenziert angewendet wird.

[Rz 131] Diese Übergangsfrist gilt nach Art. 63 E-DSG in jedem Fall für die ausgeweitete Informationspflicht (Art. 17 E-DSG), für die Regeln betr. automatisierte Einzelentscheide (Art. 19 E-DSG), für die Pflicht zur Vornahme einer Datenschutz-Folgeabschätzung (Art. 20 E-DSG) und für die Vorgaben von *Privacy by Design* und *Privacy by Default* (Art. 6 E-DSG). Darüber hinaus wird danach unterschieden, ob eine Datenbearbeitung vor Inkrafttreten des revidierten DSG bereits «begonnen» hatte oder noch nicht. Hat sie bereits begonnen, so gilt auch für sie eine Übergangsfrist von zwei Jahren (Art. 64 Abs. 2 und 3 E-DSG). Ist sie zu diesem Zeitpunkt wiederum «abgeschlossen», kommt das neue Recht mit Ausnahme des Auskunftsrechts nicht mehr zur Anwendung (Art. 64 Abs. 1 E-DSG).

[Rz 132] Was die Begriffe wie «begonnen» oder «abgeschlossen» bedeuten, definiert Gesetz und Botschaft nicht. Sie sind entsprechend auszulegen:

---

173 Art. 45 Abs. 3 E-DSG.

174 Art. 45 Abs. 2 E-DSG.

175 Art. 53 E-DSG.

- **Abgeschlossene Datenbearbeitungen:** Da auch die Aufbewahrung bzw. Speicherung von Daten ein Bearbeiten darstellt, kann eine abgeschlossene Bearbeitung begriffslogisch nicht existieren. Daher muss die Bestimmung durch eine geltungserhaltende Reduktion ausgelegt werden. Eine Datenbearbeitung ist somit dann «abgeschlossen», wenn sich diese nach dem gewöhnlichen Gang der Dinge auf eine Aufbewahrung bzw. Speicherung beschränkt. Archivierte Daten oder Daten auf Datensicherungen sind ein solches Beispiel. Auf die Daten wird nur noch ausnahmsweise zurückgegriffen, z.B. aufgrund eines Datenverlusts, eines Rechtsstreits oder – wie Art. 64 E-DSG selbst erwähnt – aufgrund eines Auskunftsersuchens, dessen Beantwortung ebenfalls eine Datenbearbeitung darstellt. Gemeinsam ist allen Fällen, dass die Bearbeitung einen Ausnahmecharakter aufweist. Der Begriff der «Datenbearbeitung» ist allerdings selbst nicht klar. Weil der Verantwortliche in gewissen Grenzen selbst bestimmen kann, was einer bestimmten Datenbearbeitung zugerechnet wird und was nicht (z.B. im Rahmen der Inventarpflicht nach Art. 11 E-DSG), scheint es vernünftig, dass der Begriff der «abgeschlossenen» Datenbearbeitung für die Zwecke von Art. 64 Abs. 1 E-DSG sich auch auf eine Untermenge einer Datenbearbeitung beziehen kann, die ebenso Daten betrifft, deren Bearbeitung noch nicht abgeschlossen ist im obigen Sinne. Wird die Buchhaltung als eine einzige Datenbearbeitung verstanden, so stellen Daten der abgeschlossenen Finanzjahre jenen Teil dar, der «abgeschlossen» ist und auf welchen Art. 64 Abs. 1 E-DSG anzuwenden ist, während die Buchungsdaten des laufenden Jahres als nicht abgeschlossen gelten (und für sie Art. 64 Abs. 2 E-DSG gilt, weil die Datenbearbeitung schon «begonnen» wurde). Im Falle von Vertragsdaten wird deren Bearbeitung in der Regel dann als abgeschlossen im Sinne von Art. 64 Abs. 1 E-DSG gelten, wenn der Vertrag beidseitig erfüllt ist und sie daher (einstweilen) nicht mehr benötigt werden; die Verjährung von etwaigen Ansprüchen braucht allerdings nicht abgewartet zu werden. Werden die Daten jedoch noch zur Kundenprofilbildung verwendet (z.B. in einem CRM), so ist deren Bearbeitung nach wie vor nicht abgeschlossen. Unklar ist allerdings, ob im Falle einer «Reaktivierung» von archivierten Daten diese nach wie vor von der Ausnahmeregelung von Art. 64 Abs. 1 E-DSG profitieren können, oder deren neuerliche Bearbeitung alle Vorgaben des E-DSG erfüllen muss. Die Zweckbestimmung von Art. 64 Abs. 1 E-DSG spricht jedenfalls für ersteres, da ihre Beschaffung im Vertrauen erfolgte, dass die nunmehr beabsichtigte Nutzung den Vorgaben (nur) des bisherigen Rechts genügen musste; allerdings wird dies in der Praxis in Bezug auf die Bearbeitungsgrundsätze und etwaige Rechtfertigungsgründe in wenigen Fällen einen Unterschied ausmachen.
- **Begonnene und fortgeführte Datenbearbeitungen:** Eine Datenbearbeitung hat spätestens dann «begonnen», wenn es zu einer Bearbeitung von Personendaten gekommen ist. Da es sich hier um eine Übergangsregelung handelt, die bereits unter altem Recht getroffene Massnahmen schützen will, und der Beginn der tatsächlichen Bearbeitung von Personendaten zufällig sein kann, sollte eine Datenbearbeitung bereits dann begonnen haben, wenn eine erste Vorkehrung zur Bearbeitung vorgenommen wurde: Abgestellt wird in Art 64 E-DSG nicht darauf, ob mit der Bearbeitung von Personendaten begonnen wurde, sondern ob die Datenbearbeitung begonnen wurde. Das ist nicht dasselbe. Der Begriff der Datenbearbeitung umfasst auch die zur Bearbeitung gehörenden Vorkehrungen, wie z.B. der Online-Fragebogen, die Einwilligung, die Instruktion des Personals oder das Aufsetzen der betreffenden Systeme. Ob eine Datenbearbeitung mit dem Treffen solcher Vorkehrungen schon begonnen hat, also z.B. der Programmierung des Fragebogens oder dem Entwurf einer Einwilligungserklärung, wird womöglich umstritten sein. Nach der hier vertretenen Ansicht macht eine zu strenge Auslegung keinen Sinn: Es geht beim Inkrafttreten des revidierten DSG um einen einmaligen

Vorgang, bei welchem es nicht darauf ankommen kann, ob einige Datenbearbeitungen mehr oder weniger von der Übergangsfrist von Art. 64 E-DSG ausgenommen sind. Zudem wird das Inkrafttreten ohnehin sehr kurzfristig stattfinden und damit genügend Herausforderungen bieten. Das DSG selbst zieht in Art. 6 Abs. 1 E-DSG eine Grenze zwischen diesen technischen und organisatorischen Vorkehrungen einer Datenbearbeitung und deren Planung. Diese Abgrenzung erscheint sinnvoll: Eine Datenbearbeitung hat somit dann «begonnen», wenn mit dem ersten, auf die Planung folgenden Schritt zu ihrer konkreten Umsetzung begonnen wird. Das passt auch vom Zweck der Regelung: Spätestens zu diesem Zeitpunkt müssen die für die Datenbearbeitung geltenden Rahmenbedingungen feststehen.

Wie «breit» eine Datenbearbeitung inhaltlich definiert wird, hängt letztlich vom Verantwortlichen ab; er wird dies auch in seinem Inventar reflektieren. Insbesondere stellt sich die Frage, ob Art. 64 Abs. 2 E-DSG auch solche Datenbearbeitungen erfasst, deren Zweck nach dem Inkrafttreten des revidierten DSG verändert bzw. erweitert wurde. Aus dem Umstand, dass Art. 64 Abs. 2 E-DSG anders als Art. 64 Abs. 3 E-DSG keinen Vorbehalt einer Zweckänderung macht, kann geschlossen werden, dass auch in ihrem Zweck erweiterte Datenbearbeitungen von der zweijährigen Frist profitieren, solange die Einheit der Datenbearbeitung gewahrt wird, d.h. vertreten werden kann, dass es um dieselbe Datenbearbeitung geht. Wenn die Botschaft zu Art. 64 Abs. 2 E-DSG festhält, dass die davon erfassten Bearbeitungen während zwei Jahren «ohne weitere Anpassungen fortgeführt» werden,[176] so bezieht sich das «ohne weitere Anpassungen» jedenfalls auf Anpassungen zwecks Erfüllung der schärferen Anforderungen des revidierten DSG. Immerhin kann das «fortgeführt» (oder «fortdauern» im Gesetzestext) dahingehend interpretiert werden, dass die Bearbeitung sich in ihren datenschutzrechtlichen Parametern nach dem Inkrafttreten nicht wesentlich geändert haben darf, weil es sonst um mehr als eine reine Fortführung gehen würde (Beispiel einer nicht wesentlich geänderten Datenbearbeitung: Kundendaten, die von einer Gesellschaft bisher einzig für die Vertragsabwicklung und eigene Marketingzwecke benutzt wurden, werden neu auch anderen Konzerngesellschaften für deren Marketingaktivitäten zur Verfügung gestellt).

Wieviel nach dem Inkrafttreten des revidierten DSG an einer Datenbearbeitung geändert werden darf, damit sie noch von der zweijährigen Übergangsfrist profitieren kann, ist vor diesem Hintergrund nicht wirklich klar. Es besteht jedoch Argumentationsspielraum. Nach der hier vertretenen Ansicht profitiert eine Datenbearbeitung in jedem Fall dann von der Übergangsfrist von zwei Jahren, wenn ein Bearbeitungszweck erst nach Inkrafttreten des revidierten DSG hinzutritt, dieser aber nach Art. 4 Abs. 3 DSG schon vorher verfolgt werden durfte. Hat sich ein Unternehmen für die Bearbeitung seiner Kundendaten in der Datenschutzerklärung die Zwecke A, B und C ausbedungen und kommt die Verfolgung von Zweck C erst unter dem neuen DSG zum Tragen, so greift die Übergangsfrist trotzdem. Die Datenbearbeitung wurde auch für den Zweck C begonnen, da erste Daten hierfür bereits beschafft wurden, auch wenn die weitere Bearbeitung noch nicht erfolgt ist. Unternehmen werden selten alle Daten einer bestimmten Datenbearbeitung jeweils immer für alle Zwecke bearbeiten, für welche sie erhoben wurden. Ein Unternehmen hat möglicherweise angekündigt, dass es die Daten seiner Kunden für bestimmte Marketingaktivitäten nutzen wird, dies aber zum

176 Botschaft (Fn. 2), S. 173.

Zeitpunkt des Inkrafttretens des revidierten DSG noch nicht getan hat. Auch das Hinzutreten neuer Daten ändert an der Geltung von Art. 64 Abs. 2 E-DSG nichts. Selbstverständlich sollte der Verantwortliche auch im Rahmen des Inventars seiner Datenbearbeitungen auf entsprechende Kongruenz achten. Zu beachten ist auch, dass eine Zweckerweiterung selbst unter bisherigem Recht oft nicht ohne zusätzliche Information möglich ist.

[Rz 133] Art. 64 Abs. 3 E-DSG wiederum soll offenbar klarstellen, dass für eine vor dem Inkrafttreten des DSG begonnene Datenbearbeitung insbesondere die **Datenschutz-Folgeabschätzung** (Art. 20 und 21 E-DSG) nicht nachgeholt werden muss, nur weil das DSG geändert wurde (anders jedoch unter der DSGVO[177]). Dass Art. 6 Abs. 1 E-DSG (*Privacy by Design*) nicht nachgeholt werden muss, soweit er sich auf eine bereits abgeschlossene Planungsphase bezieht, ergibt sich wiederum aus der Natur der Sache. Freilich ist das auch bei Art. 20 Abs. 1 E-DSG so: Die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung verlangt, dass eine solche «vorgängig» durchgeführt wird. Rückwirkend kann die Bestimmung gar nicht erfüllt werden. Der Bearbeitungszweck ist jedenfalls dann unverändert, wen er vor dem Inkrafttreten des revidierten DSG bereits verfolgt wurde (wenn auch nur mit einem Teil des Datenbestands der Datenbearbeitung) oder nach Art. 4 Abs. 3 DSG hätte verfolgt werden dürfen. Weniger klar ist, ob das Kriterium der Beschaffung «neuer Daten», die Beschaffung neuer *Datensätze* oder aber neuer *Datenkategorien* meint. Beides kommt grundsätzlich in Frage. Die Spezialregelung von Art. 64 Abs. 3 E-DSG wird vermutlich dahingehend interpretiert werden, dass Unternehmen für eine Datenbearbeitung, der laufend neue Daten zugeführt werden, innerhalb von zwei Jahren für die Zeit nach Ablauf der Übergangsfrist eine Datenschutz-Folgeabschätzung mit etwaiger Meldung vorgenommen haben müssen. Kommt es allerdings zum Ergebnis, dass sich die Datenbearbeitung nicht vertreten lässt, wird sie nach zwei Jahren wohl auch dann eingestellt werden müssen, wenn die zwischenzeitlich neu beschafften Daten wieder aufgegeben würden. Weniger weitgehende Interpretationen sind allerdings auch möglich, denn die Ausnahmeregelung von Art. 64 Abs. 3 E-DSG ist nicht wirklich ausgereift. Auch hier besteht Argumentationsspielraum.

[Rz 134] Art. 64 Abs. 4 E-DSG gilt im Umkehrschluss für jene Datenbearbeitungen, die nach dem Inkrafttreten des revidierten DSG überhaupt erst begonnen werden, sowie für jene Bearbeitungszwecke, die nicht schon nach Art. 4 Abs. 3 DSG vor dem Inkrafttreten verfolgt werden durften. Werden die Bearbeitungszwecke nach dem Inkrafttreten zum Beispiel mittels neuer AGB erweitert, so sind bezüglich der Datenbearbeitung zu diesen neuen Zwecken die Bestimmungen des revidierten DSG zu beachten. Dasselbe gilt aber auch für Bearbeitungszwecke, die bisher nicht verfolgt wurden, nach Art. 4 Abs. 3 DSG auch nicht gestattet gewesen wären, aber nach Art. 27 Abs. 2 E-DSG gerechtfertigt werden können. Dies könnte z.B. eine neue, nicht personenbezogene Auswertung von Kundendaten sein, welche diesfalls die neuen, schärferen Bestimmungen für solche Bearbeitungen zu erfüllen hat.

[Rz 135] Stellt sich die Frage, wann das **revidierte DSG in Kraft** treten wird. Der Bundesrat legt dem Parlament nahe, das Gesetzespaket so zu verabschieden, dass es bereits auf Spätsommer/Herbst 2018 in Kraft treten kann. Bis dahin müssen die Regeln betreffend Schengen umgesetzt sein. Für die Bestimmungen zu privaten Datenbearbeitungen bestünde an sich mehr Zeit, aber die Vorlage soll nach dem Willen des Bundesrats als Paket verabschiedet werden. An den

177 Leitlinie der Artikel-29-Datenschutzgruppe zu Datenschutz-Folgenabschätzungen vom 4. Oktober 2017 (WP248, Rev. 01) (http://ec.europa.eu/newsroom/document.cfm?doc_id=47711), S. 13 f.

Verordnungen will der Bundesrat immerhin bereits ab Frühjahr 2018 arbeiten. Werden der bestehende Bereinigungsbedarf der Vorlage und Faktoren wie die Referendumsfrist berücksichtigt, wird mit einem Inkrafttreten allgemein aber erst für 2019 gerechnet.

19. Schlussbemerkungen

[Rz 136] Der Entwurf für ein totalrevidiertes DSG des Bundesrates ist gegenüber dem Vorentwurf deutlich verbessert worden und grundsätzlich stimmig in Anbetracht der europarechtlichen Vorgaben. Noch weist er allerdings einige gewichtige Mängel und vor allem unerwartet viele Swiss Finishes auf, die das Parlament jetzt bereinigen sollte (eine Darstellung findet sich **hier**).[178] In einigen Fällen dürfte dies geschehen, in anderen wird sich die Materie vermutlich als zu komplex erweisen, um zu diesem Zeitpunkt die nötigen Korrekturen noch durchzuführen. Es wird dann vom Pragmatismus der Aufsichtsbehörde, der Literatur und in einigen Jahren auch der Gerichte abhängen, diese auf dem Weg der Auslegung nachzuholen.

[Rz 137] Mit einer Vielzahl von aufsichts-, zivil- und strafrechtlichen Fällen ist allerdings nicht zu rechnen, insbesondere nicht mit vielen Bussen. Strafbestimmungen gab es schon heute, und sie kamen so gut wie nie zum Einsatz. Die Aufsichtsbehörde hat ebenfalls klargemacht, dass Zwangsmassnahmen nicht ihr primäres Instrument zur Durchsetzung des Datenschutzes sein werden. Der EDÖB wird weiterhin wie bisher primär auf andere Mittel zurückgreifen – namentlich das Gespräch und das «*naming and shaming*» durch den Gang an die Öffentlichkeit – bevor er sich selbst den Aufwand eines verwaltungsrechtlichen Verfahrens antut. Die Kantone werden ebenfalls keinen besonders grossen Willen verspüren, im Datenschutz hohe Fallzahlen präsentieren zu können.

[Rz 138] Den europarechtlichen Anforderungen wird die Schweiz objektiv betrachtet trotzdem genügen, so wie sie es auch heute tut. Dazu ist es nicht erforderlich, die DSGVO auch ausserhalb des Schengen-Bereichs zu übernehmen. Es wäre ihr damit auch nicht gedient, obwohl dies hie und da propagiert wird. Zwar gibt es eine Reihe von Unternehmen, welche sowohl unter die DSGVO als auch unter das DSG fallen, und sich daher von vornherein nur an der DSGVO ausrichten. Für sie spielt das DSG keine Rolle, solange es weniger weit geht als die DSGVO. Es gibt aber auch zahlreiche Betriebe in allen Grössen, die sich nicht an der DSGVO ausrichten werden, weil sie nicht oder nur in marginalen Bereichen Anwendung findet. Muss sich ein Unternehmen für das Tracking von Benutzern seiner Website der DSGVO unterordnen, bedeutet dies noch lange nicht, dass es dies auch mit dem restlichen Betrieb tun muss und vernünftigerweise sollte.

[Rz 139] Das Schweizer DSG hat daher nach wie vor eine eigenständige und wichtige Bedeutung. Daher ist es auch wichtig, dass die Räte sich für eine vernünftige Übernahme der europarechtlichen Vorgaben einsetzen. Die Revision des DSG wird so oder so zu einem deutlichen Zusatzaufwand für Unternehmen, insbesondere auch kleinere und mittlere Unternehmen führen, und hier gilt es unnötige Bürokratie auf jeden Fall zu vermeiden. Schon jetzt zeichnet sich ab, dass von der Revision vor allem die Berater und Anwälte profitieren werden.[179]

---

178 Vgl. auch die Zusammenfassung bei David Vasella, Zum Entwurf des DSG vom 15. September 2017, walderwyss rechtsanwälte (http://datenrecht.ch/wp-content/uploads/Kritikpunkte-beim-Entwurf-des-DSG.pdf).

179 Vgl. David Rosenthal, Eine Mogelpackung, in: Neue Zürcher Zeitung, 3. Mai 2017 (https://www.nzz.ch/meinung/revision-des-datenschutzgesetzes-eine-mogelpackung-ld.1289879).

David Rosenthal, lic. iur., Konsulent, Homburger AG, Zürich, Lehrbeauftragter ETH Zürich und Universität Basel.